

Systems-Theoretic Safety Analyses Extended for Coordination

by

KIP EDWARD JOHNSON
LT COL, UNITED STATES AIR FORCE

B.S. Aeronautical Engineering, United States Air Force Academy, 2000
S.M. Aeronauts and Astronautics, Massachusetts Institute of Technology, 2002
M.S. Flight Test Engineering, United States Air Force Test Pilot School, 2009

Submitted to the Department of Aeronautics and Astronautics
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2017

© 2017 Massachusetts Institute of Technology. All rights reserved.

Signature of Author _____

Department of Aeronautics and Astronautics
September 7, 2016

Certified by _____

Nancy G. Leveson, Ph.D.
Professor of Aeronautics and Astronautics
Thesis Committee Chair

Certified by _____

Sheila E. Widnall, Ph.D.
Institute Professor and Professor of Aeronautics and Astronautics

Certified by _____

John M. Flach, Ph.D.
Professor of Psychology, Wright State University

Certified by _____

Roland E. Weibel, PhD.
Technical Staff, Lincoln Laboratory

Accepted by _____

Paulo C. Lozano, Ph.D.
Associate Professor of Aeronautics and Astronautics
Chair, Graduate Program Committee

[Page intentionally left blank]

DISCLAIMER

This material is based upon work supported by the Department of the Air Force under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the Department of the Air Force, Department of Defense, or the US Government.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

[Page intentionally left blank]

Systems-Theoretic Safety Analyses Extended for Coordination

by

Kip Edward Johnson, Lt Col, USAF

Submitted to the Department of Aeronautics and Astronautics
on Sep 7, 2016 in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Aeronautics and Astronautics

ABSTRACT

When interdependent conditions exist among decision units, safety results in part from coordination. Safety analysis methods should correspondingly address coordination. However, state-of-the-art safety analysis methods have limited guidance for analytical inquiry into coordination between interdependent decision systems. This thesis presents theoretical and applied research to address the knowledge gap by extending STAMP (Systems-Theoretic Accident Model and Processes)-based analysis methods STPA (System-Theoretic Process Analysis) and CAST (Causal Analysis based on STAMP).

This thesis contributes to knowledge by introducing: 1) a coordination framework for use in analysis, 2) STPA-Coordination and CAST-Coordination, which extend STPA and CAST to analyze coordination, and 3) flawed coordination analysis guidance for use in the extensions. The coordination framework provides explanatory power for observation of and analysis of coordination in sociotechnical systems. The coordination framework includes perspectives for use in the evaluation of coordination, which are used to operationalize the framework for analysis. STPA-Coordination extends STPA with additional steps for analysis of how coordination can lead to unsafe controls (i.e. hazards). In part, STPA-Coordination uses analysis guidance introduced in this thesis that consists of four unique flawed coordination cases and nine coordination elements. CAST-Coordination extends CAST with additional steps to investigate accident causation influences from flawed coordination.

Two case studies evaluate the utility of extensions, flawed coordination guidance, and the framework. One case study investigates the application of STPA-Coordination to a current and significant sociotechnical system challenge—unmanned aircraft systems integration into military and civil flight operations. Results are compared to official functional hazard analysis and requirements results. The comparison shows that STPA-Coordination provides additional insights into identifying hazardous coordination scenarios and recommendations.

Another case study applies CAST-Coordination to investigate a Patriot missile friendly fire (2003) during Operation Iraqi Freedom, which is a relevant concern today. CAST-Coordination is successfully applied to the friendly-fire coordination problem. When compared to official government accident investigation reports, CAST-Coordination shows benefits in identifying accident influences and generating recommendations to address the coordination and safety problem.

Both case study quantitative and qualitative results are promising and suggest STPA- and CAST-Coordination and the coordination framework are useful.

Thesis Supervisor: Nancy Leveson

Title: Professor of Aeronautics and Astronautics

[Page intentionally left blank]

ACKNOWLEDGMENTS

The PhD Journey

Professor Nancy Leveson took me under her wing on this PhD journey from the beginning. As my advisor and committee chair, she not only guided my research, but also nurtured my ability to conduct original research and to communicate ideas and results more articulately. Professor Leveson, a special thank you for all of your time and energy put into this safety and coordination PhD work and in developing my research abilities. I am honored to have been a part of your Engineering a Safer World movement!

The PhD committee consisted of top professionals in their field. My research benefitted immensely from their on-point feedback, knowledge, and intellectual curiosity. I am grateful for their time, energy, and guidance. Professor Sheila Widnall, thank you for your key support and research guidance. Professor John Flach, your expertise in the social sciences and probing questions are an essential part of my work—thank you. Dr. Roland Weibel, for your thorough guidance, your time listening and giving feedback to research ideas, and for the opportunity to be part of UAS integration safety efforts—thank you.

In addition to the formal committee, many others were involved. Professor Leia Stirling participated during the proposal and defense and was a thesis reader; I benefitted from her feedback and ideas throughout. Prof Stirling, thank you. Dr. John Thomas is a devoted mentor for us all in the lab and was a significant influence on my journey. Your precision guidance and insights kept me on track. Dr. Thomas, thank you for offering your time and professional feedback. Professor Cody Fleming, thank you for the discussions and guidance while in the lab and for being a reader and defense member at the end. I wish you all rewarding academic careers.

I was fortunate to be part of the Systems Engineering Lab (SERL) and MIT Lincoln Lab. Maj Matt Rabe (Ph.D.), Lt Col Brandon Abel, John Vivilecchia and Dr. Ed Lyvers—thank you for mixing research with fun time. Col William Young (Ph.D.), Lt Col (ret) Wes Olson (Ph.D.), Dr. Carlos Lahoz, Maj Dan Montes (Ph.D.), Maj Diogo Castilho—thank you for the research discussions. I thank all the other past and present members that created an intellectually inspiring environment to conduct research.

The PhD Opportunity

The PhD opportunity was possible from the assistance of many. I must thank the Air Force and USAF Test Pilot School for this amazing opportunity to pursue higher education. MIT Lincoln Lab enabled the opportunity through their Military Fellowship program; Col (ret) John Kuconis deserves a big thank you for leading this program. Dr. James Kuchar, Col (ret) Charles Robinson, Col (ret) T. Mike Luallen, Lt Col (ret) Mark Giddings, Col Steven Ross (Ph.D.), Lt Col (ret) Steve Jacobson—thank you for your support.

The Moral Support

Tiffany, you are the strength of our family. Thank you for your love and support, all while earning your JD. My daughters, thank you for your love and hugs that melt my heart. My family was the balance to the rigors of the PhD journey. Mom and Dad on both sides of the family, Tiffany and I are so grateful for your love and unwavering support in our academic endeavors—thank you.

[Page intentionally left blank]

TABLE OF CONTENTS

DISCLAIMER.....	3
ABSTRACT	5
ACKNOWLEDGMENTS.....	7
TABLE OF CONTENTS	9
LIST OF FIGURES.....	11
LIST OF TABLES	13
1 INTRODUCTION	15
1.1 Motivation.....	15
1.2 Overview of Safety and Coordination.....	16
1.3 Research Approach	18
1.4 Thesis Outline	19
2 BACKGROUND	21
2.1 Traditional Safety Analysis Methods and Limitations.....	21
2.2 Systems-Theoretic Accident Model and Processes (STAMP).....	26
2.3 Coordination	31
2.4 Safety and Coordination.....	42
2.5 Summary and Research Gaps	45
3 A COORDINATION FRAMEWORK.....	47
3.1 Decision Systems	47
3.2 Decomposing Coordination	49
3.3 Fundamental Coordination Relationships.....	54
3.4 Perspectives on Coordination Related to System Outcomes	57
3.5 Summary, a Coordination Framework.....	62
4 EXTENDING STPA for COORDINATION	63
4.1 STPA-Coordination	63
4.2 Identifying UCAs from Flawed Coordination Cases	65
4.3 Flawed Coordination Guidance Using Coordination Elements	68
4.4 Theoretical Application: Causal Analysis Using Flawed Coordination Guidance	72
4.5 Summary, Extending STPA for Coordination	81
5 STPA-COORDINATION CASE STUDY: UAS COLLISION AVOIDANCE.....	83

5.1	Case Study Background.....	83
5.2	Systems Engineering Baseline	84
5.3	Safety Control Structure.....	85
5.4	STPA-Coordination for UAS Collision Avoidance.....	86
5.5	STPA-Coordination Results Comparison with Previous Work.....	130
5.6	A Process Comparison for Safety Analysis of UAS Integration	138
5.7	Summary, STPA-Coordination Case Study.....	141
6	CAST-COORDINATION CASE STUDY. PATRIOT FRIENDLY FIRE SHOOT DOWN..	143
6.1	CAST-Coordination.....	143
6.2	Systems Engineering Baseline.....	145
6.3	The Safety Control Structure	145
6.4	Proximate Events	148
6.5	CAST-Coordination Applied.....	149
6.6	CAST-Coordination Results Comparison with Official Accident Reports	172
6.7	Summary, CAST-Coordination for Accident Investigation.....	179
7	CONCLUSIONS.....	181
7.1	Contributions to Knowledge	181
7.2	Limitations and Future Work.....	184
	LIST OF DEFINITIONS AND ACRONYMS.....	187
	BIBLIOGRAPHY	191
	APPENDIX A. Flawed Coordination Guidance and Examples.....	201
	APPENDIX B. RTCA SC-228 Draft STPA on UAS Integration Report	211
	APPENDIX C. STPA-Coordination Frequency Analysis.....	243
	APPENDIX D. Coding of and Comparison with DO-344 FHA and Requirements Analysis	257
	APPENDIX E. CAST-Coordination Case Study Background.....	273
	APPENDIX F. Coding Results, CAST-Coordination Case Study	283

LIST OF FIGURES

Figure 1. Launching the F-16 “Viper.”	15
Figure 2. Doctors Without Borders Friendly Fire Incident, Kunduz, Afghanistan 2015.	16
Figure 3. Risk Assessment Matrix.....	22
Figure 4. HFACS List of Personnel Factors.	26
Figure 5. STAMP Control Model	28
Figure 6. Coordination in Systems.....	39
Figure 7. Control Feedback Loop Guidance, Unsafe Control Action Causal Analysis	44
Figure 8. Decision System	48
Figure 9. Component Coordination Within Decision System	48
Figure 10. Between Decision System Coordination, (a) Vertical and (b) Lateral	48
Figure 11. Coordination Elements	53
Figure 12. Fundamental Coordination Relationships in Sociotechnical Systems	55
Figure 13. Internal and External Evaluation of Coordination.....	58
Figure 14. Coordination and Time.....	60
Figure 15. Coordination Strategy Late Scenarios	61
Figure 16. Causal Analysis Diagrams for Coordination.....	65
Figure 17. Flawed Coordination Cases.....	66
Figure 18. STPA Step 2 Using Flawed Coordination Guidance	72
Figure 19. Vertical Coordination by Control, Relationship ‘A’	73
Figure 20. Lateral Coordination Between Decision Systems, Relationship ‘B’	75
Figure 21. Lateral Coordination Between Decision Systems, Relationship ‘C’	78
Figure 22. Within Decision System Coordination, Relationship ‘D’	79
Figure 23. Unmanned Aircraft Systems Concept	83
Figure 24. Unmanned Aircraft Collision Avoidance Safety Control Structure.....	85
Figure 25. Coordination Relationships for Collision Avoidance.....	89
Figure 26. UAS Separation Boundaries.....	105
Figure 27. STPA-Coordination Hazardous Scenario Count.....	128
Figure 28. STPA-Coordination Recommendation Count for Safe Coordination	130
Figure 29. FAA Safety Risk Management Analysis Phases.....	139
Figure 30. Patriot Missile System Launch	143

Figure 31. Air Defense System Safety Control Structure.....	146
Figure 32. Lateral Coordination, Patriot and Aircrew	150
Figure 33. Component Commander Lateral Coordination	158
Figure 34. Air Component Commander, Within Decision System Coordination	166
Figure 35. Land Component Vertical Coordination	168
Figure 36. Lateral Supporting Coordination, Below Component Command	169
Figure 37. A Systems Approach to Safety with STPA-Coordination and CAST-Coordination	183
Figure 38. DO-344 FHA Decomposition.....	257
Figure 39. Joint Command Relationships.....	274
Figure 40. Air/Missile Defense Command and Control Structure	276
Figure 41. Air Defense Artillery Brigade Organization	277
Figure 42. Joint Air Force and Army Theater Air Control Systems.....	278

LIST OF TABLES

Table 1. Coordination Definitions	32
Table 2. Interdependencies and Coordination Methods (Malone & Crowston 1990; Malone & Crowston 1994).....	34
Table 3. Interdependency and Coordination Strategy Pairs.....	35
Table 4. Coordination Components	35
Table 5. Coordination Processes.....	36
Table 6. Coordination Conflicts and Causal Factors (March & Simon 1958).....	37
Table 7. Conditions for Successful Coordination (Okhuysen & Bechky 2009).....	37
Table 8. Organizational Uncertainty (Thompson 1967).....	41
Table 9. Coordination and Uncertainty.....	41
Table 10. Fundamental Coordination Relationship Matrix	54
Table 11. Extended STPA.....	63
Table 12. STPA-Coordination	64
Table 13. Unique Flawed Coordination Cases	66
Table 14. Flawed Coordination Cases	67
Table 15. Flawed Coordination Causal Analysis Matrix.....	68
Table 16. Flawed Coordination Guidance for Unsafe Control Action Causal Analysis	69
Table 17. Analysis Symbols and Nomenclature	72
Table 18. Causal Analysis Guidance, Fundamental Coordination Relationship A, Case 2	74
Table 19. Discrete vs. Continuous Control Action Descriptions.....	76
Table 20. Causal Analysis Guidance, Fundamental Coordination Relationship ‘B’, Case 2.....	76
Table 21. Causal Analysis Guidance, Fundamental Coordination Relationship ‘B’, Case 3.....	77
Table 22. Causal Analysis Guidance, Fundamental Coordination Relationship C, Case 2.....	78
Table 23. Causal Analysis Guidance, Fundamental Coordination Relationship ‘D’, Case 2.....	80
Table 24. Decision System Roles and Responsibilities	86
Table 25. Unsafe Control Actions, UAS Decision System	87
Table 26. STPA-Coordination, UAS Decision System Lateral Coordination.....	90
Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination.....	112
Table 28. Collision Avoidance Coordination Strategy Priority Matrix	124
Table 29. STPA-Coordination Hazardous Scenario Count	127

Table 30. DAA-Related Hazardous Coordination Scenario Count	128
Table 31. STPA-Coordination, Recommendation Count for Safe Coordination	129
Table 32. Hazardous Coordination Scenarios, Comparison with DO-344 FHA	132
Table 33. A Qualitative Comparison with DO-344 FHA Coordination Scenarios	133
Table 34. Coordination Requirements, Comparison with DO-344 Functional Requirements...	136
Table 35. Extended STPA Comparison with the FAA Safety Risk Management.....	140
Table 36. CAST-Coordination Steps	144
Table 37. Joint Operations Decision System Roles and Responsibilities.....	146
Table 38. Timeline, Patriot Shoot Down of GR-4	149
Table 39. Flawed Coordination Influences, Patriot and Aircrew Lateral Coordination.....	152
Table 40. Flawed Coordination Influences, Component Commander Lateral Coordination.....	161
Table 41. Recommendations for Supporting Coordination	170
Table 42. Qualitative Comparison with USCENTCOM Accident Investigation Report	173
Table 43. Qualitative Comparison to UK Ministry of Defense Accident Investigation Report.	175
Table 44. Comparison to CAST-Coordination Accident Influences	177
Table 45. Comparison to CAST-Coordination Recommendations	178
Table 46. Operational Unsafe Control Actions (STPA Step 1).....	219
Table 47. STPA-Coordination Lateral Coordination, Count Data	243
Table 48. Coding STPA-Coordination Vertical Coordination, Count Data	251
Table 49. FHA Coding and Comparison Results.....	258
Table 50. FHA Frequency Analysis of Coordination Hazards	267
Table 51. Coding the UAS Functional Requirements	270
Table 52. CAST-Coordination Frequency Analysis.....	283
Table 53. USCENTCOM Coordination-Related Contributing Factors to the Patriot Incidents.	287
Table 54. USCENTCOM Coordination Behavior Recommendations	288
Table 55. UK MOD Coordination-Related Contributing Factors to the Patriot Incident.....	289
Table 56. UK MOD Coordination Recommendations on the Patriot Incident.....	290

1 INTRODUCTION

This thesis presents the theoretical and applied research results investigating the relationship between coordination of multiple interdependent decision units and safety in sociotechnical systems. The thesis introduces: 1) a coordination framework, 2) extensions to state-of-the-art systems-theoretic safety analyses, and 3) flawed coordination analysis guidance. The extensions and flawed coordination guidance are applied to two case studies. Case study results suggest benefits over traditional safety analysis approaches in the analysis and design of safe system coordination.

This chapter provides the research motivation, an overview of safety and the research problem, the research approach, and an overview of the thesis.

1.1 Motivation

Shown in Figure 1 is an F-16 “Viper” fighter aircraft during engine start-up and launch procedures. When launching an F-16, the pilot, crew chief (front center), and additional maintenance crewmembers are used. The pilot and maintenance crew acting independently cannot safely launch an aircraft. Rather, the pilot and maintenance members are *dependent* on each other not to harm personnel while preparing the aircraft for flight operations. To ensure *safety* during launch procedures, *coordination* in space and time between every decision maker is required.



Unfortunately, flawed coordination can lead to loss of life and examples are plenty in patient care, aviation, and in military operations for example. In patient care, a study suggested that the lack of team coordination was responsible for over 40% of emergency department errors (Risser et al. 1999). In civilian and military flight operations, coordination is crucial for safety. Coordination is needed within a cockpit among aircrew members, between aircrew and Air Traffic Control (ATC), and in other cases between aircrew of different aircraft (e.g. formation flight). Internal cockpit coordination is often called crew resource management (CRM), which is often cited as a contributing factor to aviation mishaps (Helmreich 1997).

Military operations are also rife with examples of unsafe coordination. In 2003 during the start of Operation Iraqi Freedom there were three friendly-fire incidents involving Patriot missile systems and friendly coalition aircraft all within a two-week period. One of the incidents included a shoot down of a British GR-4 Tornado aircraft. In this incident, the Patriot firing unit was operating independently and with degraded communications. The Patriot system erroneously classified the Tornado as a hostile anti-radiation missile and real-time coordination efforts with the GR-4 were inadequate. The results of flawed

coordination were two friendly aircraft destroyed, three coalition aircrew killed, and a Patriot radar system attacked by friendly aircrew that luckily only damaged equipment. (US Central Command 2004)

Another friendly fire incident occurred in Afghanistan in October 2015. The crew of an AC-130 gunship unintentionally engaged a Doctors Without Borders hospital in Kunduz, Afghanistan for a period of approximately 30 minutes in the early morning hours. The coordination between stakeholders involved in the engagement, including the engagement authority and the aircrew was inadequate for the given conditions. US Central Command (2016) concluded that “poor communication, coordination, and situational awareness” were contributing factors that lead to the wrong target identified and engaged (p. 3). Figure 2 is a glimpse into the charred remains of hospital buildings resulting from the friendly fire. The human toll of this fratricide incident, influenced by flawed coordination, was a reported 42 deaths and many wounded (US Central Command 2016).



Figure 2. Doctors Without Borders Friendly Fire Incident, Kunduz, Afghanistan 2015.
Image from (US Central Command 2015), p. 70. Image in public domain.

The motivation of this research is to improve state-of-the-art safety analysis and design methods to prevent accidents due in part to flawed coordination.

1.2 Overview of Safety and Coordination

For sociotechnical systems, coordination between decision units can be beneficial and even necessary to achieve safety. It seems appropriate to begin the dissertation with the definitions used for coordination and safety as each word embodies concepts rich in meaning:

Coordination is the management of and the processes needed to integrate interdependent entities.

This thesis takes the rather simplistic definition of coordination as the focal point for rigorous investigation into safety and coordination. Safety is the system goal of particular interest, defined as:

Safety. The freedom from conditions which cause accidents (US Department of Defense 2012).

Accidents can be defined as an unplanned event that leads to a loss, such as loss of life or a loss of a mission.

1.2.1 Traditional Safety Analysis Methods

Traditional safety analysis methods were developed during the 1950-60s to handle predominantly electromechanical safety problems. Safety efforts largely include identification of hazards and operationalization of safety through characterization of risk and failures (or its corollary reliability). Common quantitative and qualitative safety analysis methods include: reliability analysis (e.g. Fault Tree Analysis, Event Tree Analysis, and Failure Mode and Effects Analysis), HAZOP (Hazard and Operability Study), modeling and simulation, accident analysis, use of checklists, and ad-hoc brainstorming sessions (Federal Aviation Administration 2014c; Leveson 1995; US Department of Defense 2012).

Traditional safety is largely based on a model of accident causation that asserts accidents result from a linear chain of failure events—Domino Theory (Heinrich 1931) and the Swiss Cheese model (Reason 1990) are examples. Safety conceptualized as a failure problem may have been adequate for electromechanical systems. Accidents, however, occur from more than electromechanical failure events and linear failure chains. Accidents also occur from flawed design requirements, non-linear or indirect interactions and behaviors, human errors and software errors to name a few (Leveson 2012).

For example, a linear failure chain paradigm suggests that aircraft mid-air collisions occur from failure of air traffic control (ATC) to separate aircraft, followed by failure of a collision avoidance system to separate aircraft, and last failure of pilots to accomplish see-and-avoid procedures. However, these failure events may be dependent and non-linear. An accident can occur when the interactions between collision avoidance systems and aircrew are inadequately designed, or when the rules inadequately specify roles and responsibilities between ATC and aircrew under collision scenarios.

If we are to build tomorrow's sociotechnical systems for safety, perhaps an alternative approach is needed to capture the rich source of accident causation beyond failures observed in today's complex, human- and software-intensive sociotechnical systems.

1.2.2 A Systems-Theoretic Approach to Safety

Systems theory provides an alternative paradigm for safety (Leveson 2004; Rasmussen 1997b). A systems-theoretic approach to safety embodies two primary concepts (Checkland 1981): 1) system goals emerge from subsystem interactions and are not a property of any one subsystem alone (Bertalanffy 1968) and 2) communication and control are necessary for goal-directed systems (Ashby 1956). STAMP (Systems-Theoretic Accident Model and Processes) is a system-theoretic model of accident causation that asserts accidents occur as a result of inadequate control and top-down enforcement of system safety constraints (Leveson 2004).

Derived from STAMP, STPA (System-Theoretic Process Analysis) is a systems theoretic analysis method that applies to emergent system properties, such as safety and security. The emphasis of STPA is analysis of control behavior by a decision unit (or "controller"). STPA begins with identification of unsafe control actions that can lead to system hazards and then seeking to understand why those unsafe control actions may occur, or causal analysis. One of STPA's benefits is the use of the well-established control theoretic feedback model to assist in problem formulation and for analytical guidance.

There are four conditions needed for feedback control, which include (Ashby 1956; Conant & Ashby 1970):

- 1) Goal condition. Control must have a goal or overarching guidance.
- 2) Controllability. A controller must be able to influence a process outcome by control actions.
- 3) Observability. A controller must be able to observe or somehow ascertain the system state.
- 4) Process models. A controller must have a model of system relationships.

Put another way, the control model describes how a controller makes decisions (i.e. the algorithm). Higher-level inputs (e.g. goals and constraints) and observed information inputs (i.e. feedback or feedforward) and process models guide the decisions.

As a metaphor for sociotechnical system interactions, the control-theoretic model has broad applicability and the application of STPA has been shown useful in many domains. In addition to control, communications among decision units has long been a hallmark in system theory. Control and communications are inextricably linked and this thesis is interested in the communications problem among interdependent decision units as it relates to the analysis and design of safe systems.

1.2.3 Research Problem

Problem: The concept of coordination has limited operationalization for use in traditional and systems-theoretic safety analysis methods, from safety engineering methods through accident investigation.

1.3 Research Approach

Proposition: To address system safety in complex work domains, analysis and design must in part address coordination between multiple interdependent decision units.

Overall Objective: Develop extensions to state-of-the-art systems-theoretic safety analyses that accommodate and guide examination and design of coordination between multiple interdependent decision units.

To address the overall objective, there were four iterative research phases. A mixed methods research design was used, applying both qualitative and quantitative research methods.

1. Develop a coordination framework. The framework provides the explanatory power for observation and analysis of coordination in sociotechnical systems. The framework is the bridge between the theoretical literature and safety engineering applications as demonstrated in this thesis.
2. Develop STPA-Coordination. The extension to STPA is derived from the coordination framework and it uses analysis guidance refined through informal feedback and case study analysis.

3. Develop CAST-Coordination. The extension to CAST is derived from the coordination framework in a similar approach to developing STPA-Coordination in phase 2.
4. Case study analysis. Integral to development of the coordination framework and analysis extensions was their application to two real-world case studies. The case study included a quantitative and qualitative comparison of results to: 1) official hazard and accident analyses of the same problem and 2) accepted analysis processes. The case studies were hypothesized to demonstrate utility of the coordination framework and analysis extensions. If successful, the case studies would support an argument *towards* validation—that the coordination framework, analysis extensions and guidance are useful, credible, and provide beneficial insights over state-of-the-art analysis of coordination for safety in complex work domains.

1.4 Thesis Outline

The thesis chapter descriptions are as follows, roughly following the research approach:

Chapter 2. Background. Safety concepts and analysis methods, coordination concepts, and coordination related to safety analysis methods are reviewed in seminal and recent literature. The common thread in Chapter 2 is to highlight the limited integration of coordination behavior in state-of-the-art safety analysis methods.

Chapter 3. A Coordination Framework. This chapter introduces a framework to provide explanatory power and common understanding useful for the observation of and analysis of coordination observed in sociotechnical systems. The framework includes perspectives to evaluate coordination with respect to an outcome, which is needed to operationalize the framework for hazard and accident analysis methods introduced in Chapters 4 and 6 respectively.

Chapter 4. Extending STPA for Coordination. STPA-Coordination is introduced, which extends STPA with additional steps to analyze how coordination can lead to hazards (i.e. unsafe control actions). The chapter operationalizes the coordination framework to develop flawed coordination guidance to be used with STPA-Coordination, which includes a set of four flawed coordination cases. STPA-Coordination is then applied to a theoretical set of fundamental coordination relationships.

Chapter 5. STPA-Coordination Case Study. STPA-Coordination is applied to unmanned aircraft system (UAS) integration safety problem. STPA-Coordination results are compared to RTCA (a US civil aviation standards development organization) safety efforts on the same problem and to current Federal Aviation Administration (FAA) safety analysis processes.

Chapter 6. CAST-Coordination Case Study. CAST-Coordination is introduced, which is an extension to CAST. Then CAST-Coordination is demonstrated on a Patriot missile system friendly fire incident during Operation Iraqi Freedom (2003). CAST-Coordination results are compared to three official government reports.

Chapter 7. Conclusions.

[Page intentionally left blank]

2 BACKGROUND

The background section reviews the literature related to safety engineering, concepts in coordination, and the integration of coordination with safety engineering. Traditional and system-theoretic analysis methods are reviewed. Seminal works through recent contributions in organizational and coordination theory are reviewed to provide a background for a coordination framework introduced next in Chapter 3. Last, the integration of coordination in safety analysis methods is reviewed and the knowledge gap addressed by this research is highlighted.

2.1 Traditional Safety Analysis Methods and Limitations

Safety analysis is a broad term encompassing many efforts. The more common safety efforts include: 1) reliability and accident rate predictions, 2) identification of hazards and risk, and 3) accident analysis. Accident rate predictions attempt to quantify system safety by reliability and simulation methods. Hazard and risk analyses attempt to identify and assess hazards for elimination, minimization, or acceptance. Accident analysis is used to determine accident causation and is often associated with human error.

2.1.1 Reliability and Failure Chains

Safety is often operationalized as a reliability problem. Reliability analysis methods were developed during the 1950s and 1960s to assess systems such as missile launch systems (Eckberg 1963) and nuclear reactor systems (Keller & Modarres 2005; US Nuclear Regulatory Commission 1975). Common reliability analysis methods include the fault tree, event tree, and failure modes and effects analysis (FMEA). These analysis methods identify components or events that can fail¹ and some order the failures into “trees” where failure nodes can branch into more failure nodes.

Safety treated as a reliability problem is based on a model of accident causation most commonly known as Domino Theory (Heinrich 1931) and the Swiss-Cheese Model (Reason 1990). Under these accident models, accidents occur from a linear and cascading chain of failure events. A concern with the linear failure chain accident models is that accidents can occur when the sociotechnical components are working reliably and from non-linear interactions. Operationalizing safety as a reliability problem omits accident causation beyond the failure paradigm, to include flawed design requirements, flawed coordination, decisions, and actions and non-linear interactions.

A concern with reliability analysis methods is the common assumptions that failure events are independent and stochastic in nature. The assumptions are useful for analysis, but perhaps inadequate for representing true sociotechnical system dynamics that exhibit dependency and deliberate behaviors in response to context. Another concern is the lack of data and ambiguous system architectures, especially during early system design when a system may not even exist. When it is claimed that predictions are

¹ Failure in reliability analysis methods is often conceptualized as more than physical component failures, such as human error and functions not working.

generally wrong (de Neufville & Scholtes 2011), the concern with lack of relevant data for reliability analysis methods to predict accident and failure rates becomes pronounced. Even if there was accurate data and linear failure chain models, high reliability is not necessary nor sufficient for safe systems (Leveson 2012). Safety is more than a reliability problem; safety must also account for hazardous functions (or behaviors), interactions, and non-linear system dynamics that may lead to accidents.

In decades past, use of reliability analysis methods may have sufficed for electromechanical systems they were developed to analyze. However, characterizing safety as a linear failure event chain problem has limited applicability to the software and human intensive *sociotechnical* systems of today. In addition to failures, linear and non-linear behaviors, and their interactions with each other and the environment can cause accidents.

A new paradigm is needed to address accident causation beyond linear failure event chains, discussed in section 2.2 below.

2.1.2 Risk

Safety is also operationalized through the concept of risk. Risk describes hazards as a combined consideration of event probability and severity. Risk is characterized by levels, usually increasing from low to high. Figure 3 is a representative risk matrix taken from the MIL STD 882E (2012). Hazard severity can be defined by losses, such as loss of humans, financials, or mission goals. Hazard probability of occurrence can be characterized qualitatively or quantitatively.

RISK ASSESSMENT MATRIX				
SEVERITY \ PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Figure 3. Risk Assessment Matrix.

Reprinted from (US Department of Defense 2012), p. 12. Figure in public domain.

In general, risk assessment can influence decisions regarding hazards and resource allocation to address them throughout a system's lifecycle. There are limitations, however. Categorizations in the risk matrix — severity, probability, and risk level—are arbitrarily assigned. For example, the FAA considers probability Level E “extremely improbable” as likelihood less than 1E-9 (Federal Aviation Administration 2014c), while the DOD considers the equivalent level “improbable” as likelihood less than 1E-6 (US Department of Defense 2012). It is also difficult to assess how hazards relate to each other. For example, if there are similar hazards both assessed “serious,” should the hazard risk be “high”? Further, determining the probability of occurrence may be difficult and left to subjective judgment.

2.1.3 Safety Design Efforts

de Weck et al. observe that while safety has a long history in engineering, safety has “...not enjoyed the same focus as other engineering properties that are more easily tested in a laboratory or field setting” (De Weck et al. 2012) p. 2. When safety is conceived as a failure property and operationalized by reliability analyses, safety has a limited role in the design of system functions and their interactions. In the systems engineering literature, safety efforts are often described as efforts parallel to system design rather than part of defining the system functions and interactions (Blanchard 2006; SAE Aerospace 2010).

Common safety efforts during system design include hazard analysis and modeling and simulation.

2.1.3.1 Hazard Analysis

This thesis adopts the hazard definition used in STAMP (Leveson 2012):

Hazard: “A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)” (p. 184).

A hazard is related to accidents by the following (Leveson 2012):

Hazard + {Worst Case Environmental Conditions} → **Accident (loss)** (p. 185)

Hazards and failures are often used interchangeably in the literature and in safety analysis efforts. In this thesis, an identified failure may lead to a hazard; the terms should not be confused.

Often one of the first hazard analysis efforts in concept development and early design are the preliminary hazard list (PHL) and the preliminary hazard analysis (PHA) (Vincoli 2006). The PHL and PHA are early attempts to identify hazards, assess scope of safety effort, and assess design alternatives. The Failure Modes and Effects Analysis is a common method used to conduct a PHL and PHA. The PHL and PHA are not specific techniques, just labels to identify when in the system phase analysis occurs.

Hazard analysis throughout design and post-design uses any number of methods discussed previously with reliability and risk analysis. In addition, hazard analysis often includes the use of checklists and ad-hoc brainstorming with designated experts. Reference (Leveson 1995) and (Vincoli 2006) for a review of safety analysis methods and techniques.

2.1.3.2 Modeling and Simulation

Modeling and simulation are used for safety efforts in predicting accident rates and are common in the air transportation system domain (Harkleroad et al. 2013). MIT Lincoln Laboratory has worked extensively with TCAS and modeling airspace encounters for safety purposes. For example, fault trees and fast-time Monte Carlo simulations were used to assess TCAS and determine system safety (Kuchar & Drumm 2007). Kochenderfer et al. used Bayesian networks to model airspace encounters and predict accident rates (Mykel J. Kochenderfer et al. 2010).

The use of probability theory in modeling and simulation is beneficial in several ways. Monte-Carlo simulations by definition are good for describing system behavior due to stochastic events. One can run an algorithm against many random scenarios as in the TCAS examples to quantify the probability of rare events such as mid-air collisions. Models and simulation are also useful for trend and sensitivity analyses, and therefore for relative comparisons between alternative designs (Sheridan 2002).

There are concerns, however, with modeling and simulation efforts used for safety. First, there may be a lack of useful data and known system architecture to not only feed the models, but to develop the models in the first place. For example, unmanned aircraft systems (UAS) integration into the National Airspace System (NAS) is a system in design phase without relevant data (US Government Accountability Office 2013) or system architecture to develop the necessary models for simulation. Another concern is the stochastic characterization used, which can calculate a probability of an event with some statistical significance. However, designing the deliberate functions and interactions needed for preventing hazards may be a challenge with stochastic representations.

Modeling and simulation has many potential benefits and uses. However, safety results from a complex web of linear and non-linear interactions, interactions that may be difficult to model and that stochastic representations may hide. Safety requires the deliberate design of system functions and interactions themselves, not just stochastic characterizations. While the allure of quantitative modeling and analysis for such complex properties as safety is powerful and prevalent (Sheridan 2002), safety and engineering safe systems should not be characterized by numbers alone.

2.1.4 Accident Analysis and Human Error

“It is commonly accepted that the contribution of human factors to accidents is between 70 – 90% across a variety of domains” (Hollnagel & Woods 2005) p. 7.

Safety efforts in early design phases are most effective in terms of economics and technical performance (Fleming 2015), while least effective are safety efforts post-accident. However, accident investigations provide an opportunity to find and re-design inadequate aspects of a system. Considering human error is generally cited as responsible for 70-90% of accidents, it is understandable why classification of human error attracts much attention in the safety and human factors literature (Scarborough et al. 2005). Classic human error taxonomies include Rasmussen’s skill-rule-knowledge based errors (Rasmussen 1982; Rasmussen 1983) and Reason’s discussion on active failures (Reason 1990).

Rasmussen's human error framework is based on three levels of human behaviors. Skill-based behaviors are sensory-motor based behaviors. Rule-based behaviors are an abstraction level higher and represent pre-planned decision about actions. At the highest abstraction are knowledge-based behaviors, which consider goal-directed decisions made when rules inadequately address the current scenario.

Rasmussen's human error taxonomy attributes coordination to a skill-based human error problem: "[Skill-based] Errors are related to variability of force, space or time coordination" (Rasmussen 1982) p. 316. Rasmussen's conception of coordination as related to human actions is similar to Bernstein's perspective in motor coordination theory (Bernstein 1967). Rule-based human behavior is based in coordination rules for subroutines and errors may occur related to these coordination rules. Coordination in Rasmussen's human error taxonomy was conceived as an *individual* behavior. The focus of this thesis is in the coordination (i.e. interactions) among decision units, not individual behavior.

Reason's error taxonomy distinguishes between active failure and latent conditions. Active human errors are "the unsafe acts committed by people who are in direct contact with the...system" (Reason 2000) p. 769. Active errors are further refined into intentional or unintentional. Unintended actions are due to slips (physical) or lapses (cognitive) for example. Intentional human errors are due to mistakes or violations. Reason (1990) labeled slips, lapses, and mistakes as "basic error types." Along with active failures, there are "latent conditions" that exist within the system itself caused by decisions related to organizational design or policy for examples (Reason 2000). Latent conditions along with active failures may lead to accidents.

Rasmussen and Reason provided conceptual frameworks to describe human error, but little was done to operationalize them for use in safety analysis (Weigmann & Shappell 1997). Shappell and Weigmann (2000) argue "...a comprehensive framework for identifying and analyzing human error continues to elude safety professionals and theorists alike" (p. 1). In response to limited human factors guidance in accident analysis, Shappell and Weigmann developed the Human Factors Analysis and Classification System (HFACS) for accident investigation in US Naval aviation (Shappell & Weigmann 2000). HFACS has since been applied to aviation in general and to other domains, e.g. shipping incidents (Celik & Cebi 2009) and mining incidents (Lenné et al. 2012).

HFACS focuses on the operator perspective, but also accounts for environmental, supervision, and organizational factors (US Department of Defense 2005). HFACS is a framework for accident analysis based on Reason's Swiss Cheese Model and concepts of active failures (e.g. operator control actions) and latent conditions (e.g. organizational concerns). The reader is referred to (US Department of Defense 2015) for a more thorough and recent description of HFACS as used by the US Department of Defense (DOD).

HFACS includes a "preconditions" level that primes human behavior and is a potential error source for the human "action" error level. The preconditions level consists of three factors including "personnel factors," which is further decomposed into "Coordination/Communication/Planning" as shown in Figure 4. The DOD HFACS (2005) defines the precondition level as:

Coordination / communication /planning are factors in a mishap where interactions among individuals, crews, and teams involved with the preparation and execution of a mission that resulted in human error or an unsafe situation (p. 9).

Updated DOD HFACS guidance (2015) replaces the terms “Coordination/Communication/Planning” with “teamwork,” yet keeps the definition and guidance similar. However, the relationships between coordination, communication, and planning factors are ambiguous with little guidance provided beyond the guidewords.

A focus on human error is not without scrutiny (Dekker 2006; Rasmussen 1997b). Accident causation with a focus on human error may too often fall into the trap known as “hindsight bias” (Fischhoff 1975). Hindsight bias is the tendency to simplify causation after the fact. Hindsight bias in accident causation tends to turn complex and dynamic interactions into simple and linear causation where the human can more easily be blamed. One challenge with the human error focus is to overcome hindsight bias and ask why the decision or action may have seemed reasonable under the circumstances (Dekker 2006).

Emphasizing human error tends to place the blame on the human, but some argue it is the human-system interaction in context to blame. That is, human behavior is influenced by the context in which it occurs. While one can design training to influence how well humans interact with a given system (Annett & Duncan 1967), the human factor must be accounted for in system design. The significance in the difference between blaming human error and human interaction is that engineers can design solutions to the human-system interactions that accommodate the human factor.

The analysis and design of *systems* requires a more holistic paradigm that treats humans as part of the system (Hollnagel & Woods 1983), which goes beyond a focus on human error often associated with accident investigations.

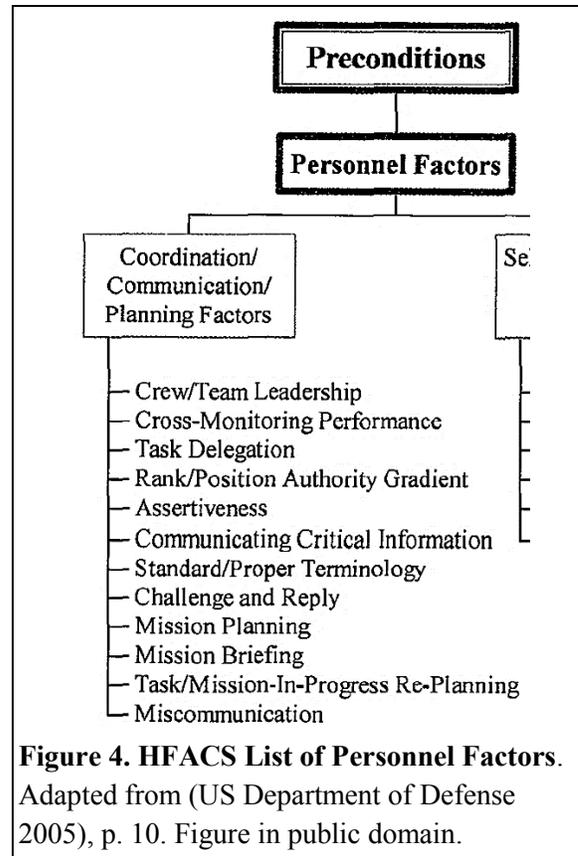


Figure 4. HFACS List of Personnel Factors. Adapted from (US Department of Defense 2005), p. 10. Figure in public domain.

2.2 Systems-Theoretic Accident Model and Processes (STAMP)

“Modern technology and society have become so complex that the traditional branches of technology are no longer sufficient; approaches of a holistic or systems, and generalist and interdisciplinary, nature became necessary” (Bertalanffy 1972) p. 420.

2.2.1 Systems Thinking

Systems theory provides a set of concepts that articulate how problems can and should be viewed from a holistic systems perspective. Systems theory acknowledges that there are system properties and behaviors that cannot be observed at a decomposed level or by summing the components as in classic scientific reductionism. Systems-thinking is an approach to problem solving that uses two system-theoretic conceptual pairs: 1) systems have emergence and hierarchy and 2) systems need communication and control (Checkland 1981).

The first conceptual pair of a systems approach is that of emergence and hierarchy. Every system has hierarchy and behaviors that emerge from subsystem interactions (Bertalanffy 1968). Emergence is a key concept related to the adage the whole is greater than the sum of its parts. For examples, the aircraft property of range or endurance is not a property of the wing or the engine alone; rather, these properties emerge and only have meaning at the aircraft level. The second conceptual pairing—communications and control—draws from Cybernetics and represents the “anti-entropic” behaviors that allow open systems to organize and remain stable (Ashby 1956; Wiener 1956). These behaviors are observed everywhere, from biological systems to human social systems.

Another aspect to systems thinking is that systems are social constructs. That is, the researcher decides the boundary of a system and the perspectives chosen for analysis. Results of analysis are based on the chosen system constructs and do not represent an absolute reality.

2.2.2 STAMP (Leveson 2004)

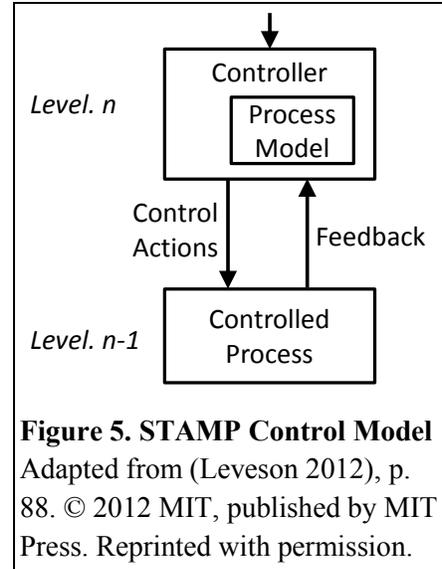
Systems theory provides an alternative paradigm for modelling safety and accident causation (Leveson 2004; Rasmussen 1997b). Leveson introduced STAMP (Systems-Theoretic Accident Model and Processes) to the safety community over a decade ago, which is the first new accident causation model based in systems theory (Leveson 2004). STAMP conceptualizes safety as a system property, which is a property that *emerges* from subsystem interactions and is a property that must be *controlled*. Accidents causation according to STAMP occurs from inadequate controls, and accidents are prevented by the top-down enforcement of system safety constraints.

STAMP is a departure from linear failure chain accident models first introduced during the 1930s. There are three primary concepts that define STAMP: safety constraints, hierarchical control structures, and process models (Leveson 2012). System safety constraints are derived from the system level accidents and hazards. The hierarchical control structure is the functional representation of the system responsible for enforcing the system safety constraints on the physical process. The control structure can include levels as high as required for analysis, such as government organizations. The process models are a controller’s representation of the controlled process and its relationships to the environment.

STAMP uses a control model to operationalize safety, which requires a goal, controllability condition, observability condition, and system model (Ashby 1956; Leveson 2012). Shown in Figure 5 are the basic STAMP concepts. The safety constraints are given with a system and are an input to the level n controller. The controller is responsible for enforcing the safety constraints on subsystems, level n-1 (its goal). Control actions require process models to determine the appropriate control actions. Completing the loop, feedback updates a controller’s process models (observability condition).

In STAMP, safety emerges from the hierarchical control of subsystems and processes. Accidents result from one or more of the following (Leveson 2012) p. 92:

1. The safety constraints were not enforced by the controller.
 - a. The control actions necessary to enforce the associated safety constraint at each level of the sociotechnical control structure for the system were not provided.
 - b. The necessary control actions were provided but at the wrong time (too early or too late) or stopped too soon.
 - c. Unsafe control actions were provided that caused a violation of the safety constraints.
2. Appropriate control actions were provided but not followed.



The unsafe controls provide the framework for the new systems theoretic hazard analysis method STPA (System-Theoretic Process Analysis).

2.2.3 System-Theoretic Process Analysis (STPA)

STPA is a hazard analysis method based on STAMP and is part of a top-down systems engineering approach. As part of the systems engineering approach, the system accidents and hazards are defined. From the hazards, the systems safety constraints can be derived. It is the safety constraints that controllers are responsible for enforcing. Next, a system model is developed, called a safety control structure. With the systems engineering baseline accomplished, STPA is used to analyze each controller identified in the control structure.

STPA begins with the identification of unsafe control actions (UCAs), or actions that can lead to system hazards. Based on STAMP, STPA assesses four general unsafe control actions (Leveson 2012) p. 217:

1. A control action required for safety is not provided or is not followed.
2. An unsafe control action is provided that leads to a hazard.
3. A potentially safe control action is provided too late, too early, or out of sequence.
4. A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action).

STPA then identifies scenarios that can lead to the unsafe control actions, which have traceability to the system hazards. The control theoretic feedback model guides causal analysis of the relationship between controllers and controlled processes. These two steps are labeled as STPA step 1 (identify UCAs) and

step 2 (UCA causal analysis). Reference *Engineering a Safer World* (Leveson 2012) and *An STPA Primer* (Leveson 2013) for additional information on STPA and its application to hazard analysis.

STPA improves on current ad-hoc hazard scenario identification with a structured top-down systems engineering approach that uses hierarchical system and feedback control models for guidance (Leveson 2012). The output of STPA is the identification of unsafe control actions and set of hazardous scenarios that can lead to the unsafe controls. Given the hazardous scenarios, one can develop a set of qualitative safety constraints for system control behaviors.

STPA has been successfully applied to nearly every domain since its inception, and has been shown to identify hazardous scenarios not captured using traditional safety analysis methods. As a measure of usefulness and validity, STPA and its applications are published numerous times in peer-reviewed publications. STPA has been used in: air transportation systems, e.g. (Fleming et al. 2013); pharmaceutical systems, e.g. (Leveson et al. 2012); automotive systems, e.g. (Stringfellow et al. 2010) and (Placke 2014); medical devices, e.g. (Antoine 2013); and US Air Force flight test and evaluation, e.g. (Montes 2016). STPA may also be applicable to other system emergent properties such as security, e.g. (Young & Leveson 2014).

In addition to wide application, researchers have extended STPA in efforts to improve analysis guidance. Thomas developed a formal (mathematical) approach for identifying unsafe control actions (Thomas 2013). The formal approach requires the problem space to be decomposed into a discrete problem space, such as: control actions, environmental factors, process states, and scenarios. Given decomposition, the Thomas method will determine the unsafe control scenarios formally. The approach is perhaps more suited for more constrained problems because defining a discrete problem space is a challenge when many degrees of freedom in control and nearly limitless environmental scenarios exist (Flach 2012).

Another development in STPA is analysis guidance for human controllers (Montes 2016; Thornberry 2014). Thornberry integrates human factors principles of workplace ecology and action affordance into the causal factor hazard analysis of human controllers. The workplace ecological approach asserts that the human should be analyzed within the constraints of the work domain (Flach et al. 1998; Vicente & Rasmussen 1992). Affordances are the perceived possibilities for action or “the opportunities in the ecology” (Flach & Voorhorst 2016) p. 54. Thornberry (2014) introduces “*flawed detection and interpretation of feedback* and the *inappropriate affordance of action*” causality categories (p. 2, emphasis in original). Montes (2016) expands Thornberry’s causal analysis work to include additional process model guidance and socio-organizational influences on unsafe control actions.

While STPA has been used widely and extensions have been developed, there remains limited STPA guidance related to coordination behavior of multiple decision units. STPA extended for coordination is one of the research opportunities this thesis addresses.

2.2.4 Control-Theoretic Safety Design

A control theoretic approach to safety may be used concurrently during system design stages (Harkleroad et al. 2013; Leveson 2012). Fleming developed STECA (Systems-Theoretic Early Concept Analysis), which is a formal analysis method using the control theoretic feedback model to evaluate the plain text language in written documents (Fleming 2015; Fleming & Leveson 2015). STECA is demonstrated on a

ConOps for in-trail procedures in his dissertation, comparing the ConOps plain text language against a mathematical model describing the four conditions needed for control. Fleming suggests STECA could be used to influence early design decisions for safety.

2.2.5 STPA Comparison to Reliability Analyses

At a fundamental level, more than failure conditions can cause accidents, such as flawed individual and group behaviors, and flawed interactions. These flawed behaviors and interactions may actually be designed into a system. That is, accidents can occur when the system is operating correctly, but the context is different from anticipated (e.g. weather not accounted for) or the system behaves not as intended (e.g. automation changes mode unexpectedly, but as programmed).

Traditional reliability analysis methods are based in the chain-of-failure events accident causation model. As such, reliability analysis methods nearly exclusively address accidents caused by failure conditions, which handles only part of the problem. In contrast, STPA is based in STAMP and identifies hazardous scenarios that can lead to unsafe control actions. STPA treats failure conditions as one of many hazardous scenarios that can cause unsafe control behavior.

While failure conditions can lead to accidents, direct causality cannot be inferred from failure conditions. For example, if an F-16 fighter jet engine does not start during engine start up procedures, safety is not necessarily a concern. If the same incident occurs in flight, however, the single engine F-16 failure may lead to an accident. Traditional reliability methods are perhaps not efficient for this reason. Efforts are expended characterizing failure conditions that may or may not affect safety. In contrast, STPA is a worst-case analysis based in systems engineering. The systems engineering process is conducted top-down, starting with identification of the accidents and system level hazards. STPA is then used to identify scenarios that can lead directly to the hazards. STPA can be considered more efficient than traditional analysis methods in that efforts identify *only* hazardous scenarios that can lead directly to accidents, scenarios that involve both failure and flawed behavioral conditions.

Analysis is ultimately conducted to influence decisions. Reliability analysis methods are used to assess failure conditions and determine accident rates. Reliability analysis methods also assist in determining minimum reliability requirements, which assumes meeting a numerical threshold makes the system safe. STPA in contrast is not a quantitative method at all, either reliability or risk-based. STPA is a functional or behavioral analysis method. What is implied is that safety is in the system behaviors and interactions, regardless of predicted likelihoods that could be assessed.

Safety efforts using reliability analysis also assume that safety is a component property. In other words, if a component meets a minimum reliability threshold then it is safe. Perfectly reliable components, however, with functions and interactions designed incorrectly can lead to accidents. For example, the cruise control that correctly attempts to counter reduction in velocity when driving through a water puddle may lead to hydroplaning, which could send the car and those inside into a ditch or worse. The cruise control was reliable, but its design was unsafe. STAMP recognizes that safety is an emergent property that does not have meaning at the component level.

Reliability analysis often relies on three primary event assumptions: stochastic events, independent events, and linear failure events. First, the assumption that component or event failures are stochastic may

be reasonable for failure behavior of electromechanical systems the methods were developed to address. However, goal-directed behavior in sociotechnical systems is generally intentional and designed rather than stochastic. Humans (and software) may not be included in reliability analysis methods; if they are, a commonly accepted practice is to characterize humans stochastically (Bell & Swain 1983). Efforts to stochastically characterize goal-directed behaviors are of limited value for deciding what those behaviors and their interactions should be to achieve safe outcomes. In contrast, the use of STPA can derive functional design requirements for system behaviors and interactions that lead to safe outcomes.

The second common assumption is that failure events are independent even though events are clearly not independent. This is done perhaps because it makes the mathematics of reliability analysis tractable. An early Boeing fault tree manual proclaims, “The qualification ‘independent’ is imposed not only because of the resulting simplification but also because the Boolean version of the fault tree contains only events that may be regarded as independent...” (Eckberg 1963) p. 79. STPA addresses dependent interactions that occur or should occur in dynamics systems, which is in contrast to the mathematical reason to assume independence.

Last, the stochastic and independent events are assumed to fail in linear chains per the underlying accident causation model (e.g. Domino Theory, Swiss cheese model, or defense in depth). The linearity also assists in reliability calculations. However, accidents occur from linear *and* non-linear behaviors and interactions. In contrast, STPA addresses linear and non-linear interactions and hazardous scenarios without using a quantitative analysis to linearize accident causality.

Like modeling and simulation efforts, reliability analysis methods are data driven. Likelihood of failure conditions must be quantified. Data are needed to characterize the failure event, which may be difficult to gather even if a reasonable failure measure could be articulated. For systems in the design phases with novel technology or concept of operations, such as UAS integration into flight operations, the data simply do not exist. STPA uses current system architecture and functions for analysis. In design, STPA can use anticipated architecture(s) and functions and its results can influence architectural and behavioral design considerations without quantitative data.

STPA addresses several limitations in the operationalization of safety using reliability analysis methods. STAMP, which STPA is derived from, is a true paradigm change for safety.

2.3 Coordination

“Coordination (and the communication it implies) is central to the very existence of organizations” (Kleinbaum et al. 2009) p. 1.

The concept of coordination is rich in meaning and this section provides a set of perspectives and constructs from the literature that are used in the following chapters to develop a coordination framework and to analyze coordination. Defining coordination is first and then coordination in the context of systems is reviewed.

2.3.1 Coordination Defined

The concept of coordination is a primary emphasis in management and organizational literature (March & Simon 1958; Thompson 1967). Coordination is also found in physiology (Bernstein 1967), computer science (Cataldo et al. 2006), psychology, and systems theory to name a few (Malone & Crowston 1990). Malone and Crowston suggest and make efforts to develop a new interdisciplinary theory of coordination (Malone & Crowston 1994). Table 1 highlights selected definitions from different fields, using seminal and current literature.

Table 1. Coordination Definitions

Field	Coordination Definition
Kinesiology (Bernstein 1967)	“ <i>The co-ordination of a movement is the process of mastering redundant degrees of freedom of the moving organ, in other words its conversion to a controllable system. More briefly, co-ordination is the organization of control of the motor apparatus</i> ” (p. 128, emphasis in original).
Automation (Watson & Holmes 2009)	“Coordination involves managing the interaction of processes... Examples of coordination functions are monitoring and assessing performance” (p. 1607).
Cybernetics (Ashby 1981)	“Co-ordination is essentially a holistic phenomenon, discernible only over the whole” (p. 128).
Organizational Theory (Argote 1982)	“Coordination involves fitting together the activities of organization members, and the need for it arises from the interdependent nature of the activities that organization members perform” (p. 423).
Organization Science (Jarzabkowski et al. 2012)	“...concerned with the alignment of interdependent organizational activities to accomplish collective organizational tasks...” (p. 908).
Coordination Theory (Malone & Crowston 1994)	“Coordination is managing dependencies between activities” (p. 90).
Management Science (Faraj & Xiao 2006)	“At its core, coordination is about the integration of organizational work under conditions of task interdependence and uncertainty” (p. 1156). “...a temporally unfolding and contextualized process of input regulation and interaction articulation to realize a collective performance” (p. 1157).
Management Science (Okhuysen & Bechky 2009)	“Coordination, the process of interaction that integrates a collective set of interdependent tasks, is a central purpose of organizations” (p. 463).
Management Science (Gulati et al. 2012)	They define a “coordination perspective” (p. 537): “...we define coordination as <i>the deliberate and orderly alignment or adjustment of partners’ actions to achieve jointly determined goals</i> . We regard coordination as an outcome that can be characterized by

Field	Coordination Definition
	<p>efficiency... [and] by effectiveness” (emphasis in original).</p> <p>“Coordination typically involves the specification and operation of information-sharing, decision-making, and feedback mechanisms in the relationship to unify and bring order to partners’ efforts, and to combine partners’ resources in productive ways. In short: coordination seeks to ensure that partners’ efforts ‘click’ and yield the desired outcomes with minimal process losses.”</p>

This thesis defines coordination as:

Coordination is the management of and the processes needed to integrate interdependent entities.

In particular, this research is concerned with coordination of multiple interdependent decision units. It is the interdependency that distinguishes coordination from similar concepts alluded to by the terms cooperation and collaboration. Cooperation and collaboration are potentially mutually beneficial interactions, but are not necessarily interdependent interactions.

The definition of coordination is central perspective in this thesis, but a conceptually richer understanding is required to be useful for analysis. The next subsections expand upon the definition and address the following questions:

1. What are interdependencies and how can one manage them?
2. What components and processes comprise coordination?
3. How can coordination be effective in integrating interdependent decision units?

2.3.1.1 *Interdependence and Coordination Strategy*

“Need for joint decision-making in an organization arises through two central problems in organizational decision-making: resource allocation and scheduling. The greater the *mutual dependence on a limited resource* (5.19), the greater the felt need for joint decision-making with respect to that resource [5.15: 5.19]. The greater the *interdependence of timing of activities* (5.20), the greater the felt need for joint decision-making with respect to scheduling [5.15:5.20].” (March & Simon 1958) p. 122 (emphasis in original).

In this thesis, coordination is the behavior to address interdependent conditions between two or more decision units. What are interdependencies and what manages them?

According to Thompson (1967), sociotechnical systems exhibit three primary interdependencies, which he labels pooled, sequential, and reciprocal interdependence. First, under pooled interdependency decision units and subsystem components must meet their responsibilities for a system to be successful. Pooled interdependency is perhaps the most basic form and is an inherent part of any organizational and

system structure. In other words, pooled interdependency is what transforms independent decision units and components into a goal-directed system. Second, sequential interdependence occurs when temporal order is necessary for successful outcomes. Last, Thompson (1967) describes reciprocal interdependence as the direct input-output dependence of each decision unit with another: “each unit involved is penetrated by the other” (p. 55).

Thompson classifies three coordination strategies that correlate with the three interdependencies. Standardization is used for pooled interdependency. Examples of standardization include rules and establishing the system structure. As a minimal requirement, systems should have some form of standardization (Flach et al. 2013). A fundamental concern for coordination by standardization is the balance between control and flexibility to achieve system goals (Grote et al. 2009). Coordination by planning helps ensure successful outcomes in sequential interdependency scenarios. Last is mutual adjustment. Mutual adjustment is direct coordination with another decision unit and is the most costly in terms of “communication and decision efforts” (Thompson 1967) p. 64.

Malone and Crowston (1990, 1994) describe four general interdependencies: shared resources, prerequisite constraints, simultaneity constraints, and task-subtask. Shared resource and simultaneity constraints are unique from the categories in (Thompson 1967). Simultaneity describes an interdependency that requires actions accomplished at the same time. Simultaneity is a special case of what (March & Simon 1958) recognize as a temporal dependency. Task-subtask describes the interdependency when tasks (and sub-tasks) are united by a common goal.

The coordination strategies associated with the four interdependencies are listed in Table 2. The strategies are self-explanatory except those related to task-subtask interdependency, which are “goal selection” and “task decomposition.” The premise is that a goal is selected and then a strategy is developed to achieve the goal. An aviation example is a formation of fighter aircraft has a goal to avoid mid-air collisions. To achieve this goal, the fighter formation establishes a strategy to offset each other by altitude.

Table 2. Interdependencies and Coordination Methods (Malone & Crowston 1990; Malone & Crowston 1994)

Interdependency	Coordination Method
Shared Resource	<ul style="list-style-type: none"> • Managerial decisions • Priority scheme • Competition/Bidding
Prerequisite Constraints	<ul style="list-style-type: none"> • Sequencing • Notification
Simultaneity Constraints	<ul style="list-style-type: none"> • Scheduling • Synchronization
Task/subtask	<ul style="list-style-type: none"> • Goal selection • Task decomposition

In summary, there are at least five interdependency and coordination strategy pairs, listed by rows in Table 3. The first column is the concept pair identifier. The second and third columns identify interdependencies in the literature as cited; interdependencies listed in the same row are deemed similar. For example, Pair 1 shows pooled and task/subtask interdependency (columns two and three) matched with goal selection, task decomposition, and standardization coordination strategies (column four).

Table 3. Interdependency and Coordination Strategy Pairs

Pair	Interdependency		Coordination Strategy
	<i>Thompson (1967)</i>	<i>Malone & Crowston (90, 94)</i>	<i>*Thompson; **Malone and Crowston</i>
1	Pooled	Task/subtask	<ul style="list-style-type: none"> • Goal selection** • Task decomposition** • Standardization*
2	Sequential	Prerequisite constraints	<ul style="list-style-type: none"> • Planning*
3		Simultaneity constraints	<ul style="list-style-type: none"> • Scheduling** • Synchronization**
4	Reciprocal		<ul style="list-style-type: none"> • Mutual adjustment*
5		Shared resources	<ul style="list-style-type: none"> • Managerial decisions** • Priority scheme** • Competition/bidding**

Where there is interdependency, there should be a coordination strategy. The conceptual pair is the fundamental construct in the analysis of coordination for system safety; addressing problems with interdependent decision units without coordination may lead to hazardous scenarios.

2.3.1.2 Components and Processes of Coordination

What elements make up coordination? Malone and Crowston address this question in their work on coordination theory and decompose coordination into core components and processes, shown in the following Table 4 and Table 5 (Malone & Crowston 1990). The two perspectives on coordination decomposition provide a means to evaluate coordination scenarios, which may be useful in a systems approach to safety.

Table 4. Coordination Components

Coordination Component	Description
Goals	Must have mutually agreeable goals
Activities	The mechanism to accomplish goals, a strategy
Actors	Must have actors to accomplish activities

Interdependencies	The requisite need for coordination
-------------------	-------------------------------------

Table 5. Coordination Processes

Coordination Process	Description
Group decision-making	Coordination requires group decision-making to identify goals, develop strategy, and choose among activity alternatives.
Communication	The communication process establishes a common language and the protocols necessary for sending and receiving information.
Observation of common objects	More than observation, coordination benefits from observation of common objects. Objects may be electro-physical in nature depending on the application. Observation of common objects assists in other aspects of coordination.

Coordination is comprised of components and processes that enable the behavior. These perspectives are used later for analysis.

2.3.1.3 Conditions for Coordination

How should coordination be accomplished? Coordination components and enabling processes are not sufficient for coordination efforts; certain conditions are needed for coordination to be effective and integrate interdependent decision units.

Organizational theory provides insights into coordination using a perspective of avoiding conflict:

The conditions necessary for intergroup conflict in addition to the general absence of individual conflict can be summarized in terms of three variables. The existence of a positive *felt need for joint decision-making* (5.15) and of either a *difference in goals* (5.16) or a *difference in perceptions* of reality (5.17) or both among the participants in the organization are necessary conditions for *intergroup conflict* (5.18) [5.18:5.15, 5.16, 5.17]. Thus, we argue that there are three major factors influencing intergroup conflict and that they do not enter into the scheme in a strictly additive fashion, although shifts in any of the three will generally have positive effects on the amount of potential conflict. (March & Simon 1958) p. 121 (emphasis in original).

Compatible goals and compatible perceptions of the true state are needed to avoid conflict in joint decision-making and have successful coordination. March and Simon describe factors that may cause divergence in goals and perceptions, listed in Table 6. Successful coordination is in part related to shared goals and share decision perspectives and the two are correlated: “The greater the differentiation of individual goals, the greater the differentiation of individual perception” and vice versa (March & Simon 1958) p. 127.

Table 6. Coordination Conflicts and Causal Factors (March & Simon 1958)

Coordination Conflict	Causal Factors
Goal divergence (p. 125)	Influences on commonality of individual goals within the organization
	Clarity and consistency of the reward structure and therefore, the reinforcement system
	Compatibility of individual rewards
Individual perception divergence (p. 127)	Independent information sources
	Channeling of information-processing
	Informal information sharing (e.g. geographically separated units may have less opportunity)

(Okhuysen & Bechky 2009) analyzed coordination and organization theory and suggested a framework for *how* coordination should occur. What they identified were three “integrating conditions for coordination”: accountability, predictability, and common understanding. Table 7 summarizes the three integrating conditions.

Table 7. Conditions for Successful Coordination (Okhuysen & Bechky 2009)

Coordination Integrating Conditions	Description
Accountability	<ul style="list-style-type: none"> • Roles and responsibilities assigned • Reliance on trust • Ability to observe others and update
Predictability	<ul style="list-style-type: none"> • Able to anticipate • Being familiar with task and performance
Common understanding Note. The human factors literature associates common understanding with a “shared mental model” (Stout et al. 1999)	<ul style="list-style-type: none"> • A shared perspective on the global task • Understanding of strategy and actions • Understanding of other interdependent decision units • Understanding of holistic system

The conditions for coordination appear reasonable and incorporate concepts previously highlighted in this literature review. For example, March and Simon’s goal and perception divergence listed in Table 6 are incorporated into the coordination conditions *common understanding*. Along with the coordination strategy, the integrating conditions address the management of interdependent conditions.

2.3.1.4 Summary, Coordination Defined

This thesis defines coordination as the management of and processes needed to integrate interdependent entities. “Management of” includes a coordination goal and strategy, and the integrating conditions (i.e. accountability, common understanding, and predictability). The “processes needed” include communications, group decision-making, and observation of common objects.

2.3.2 Coordination in Systems

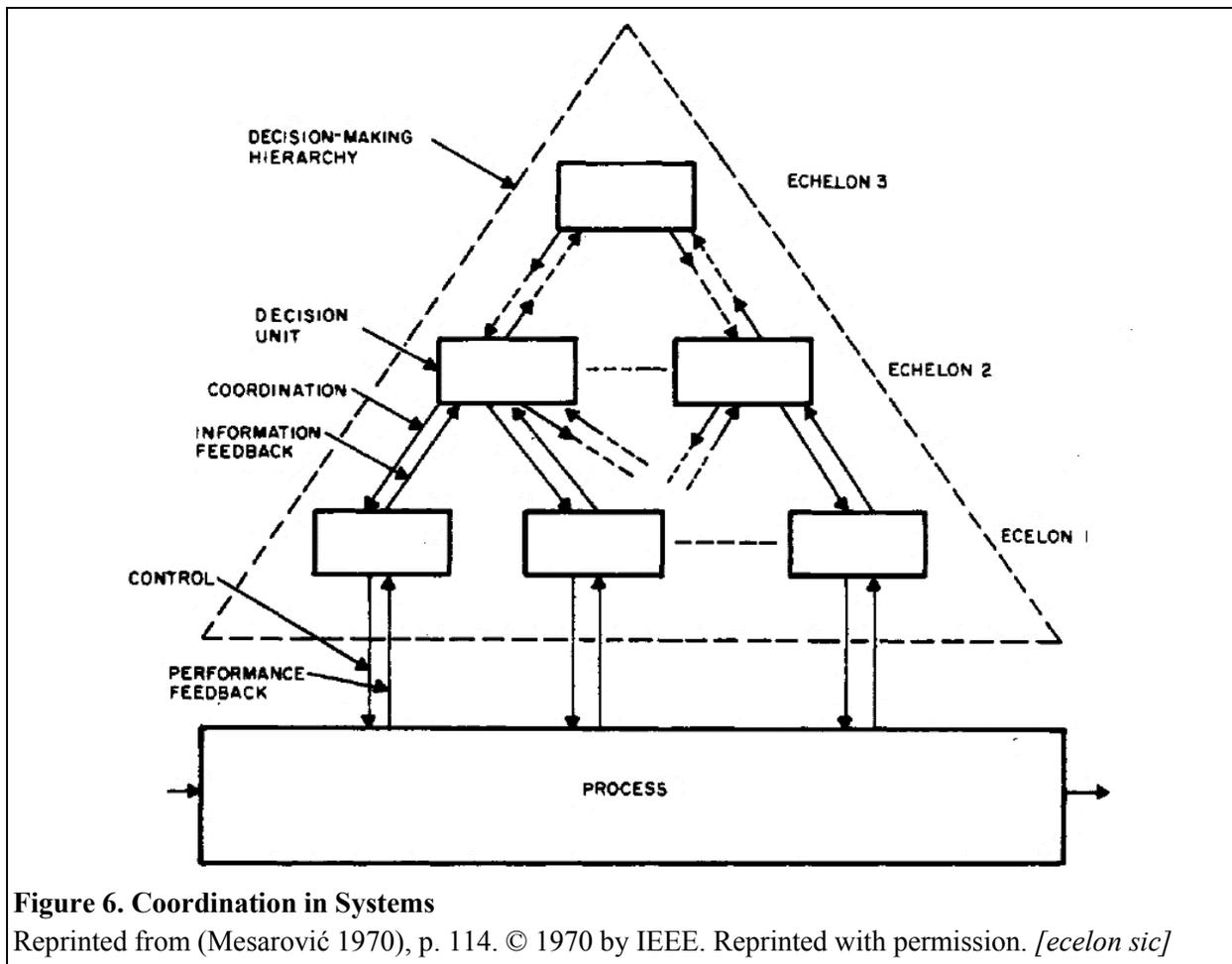
This section describes coordination concepts from a systems perspective. First, coordination is discussed relative to other goal-directed behaviors observed in sociotechnical systems. Next, the use of coordination to address degrees of freedom afforded an interdependency condition is discussed. Last, the concept of uncertainty is addressed relative to the coordination problem. The concepts in this section provide additional insights for the analysis of coordination.

2.3.2.1 Coordination, Decisions, and Actions

Coordination is a goal-directed behavior observed in sociotechnical systems. Figure 6 shows a hierarchical representation of a sociotechnical system, where the physical process is identified at the bottom of the hierarchy. The labeled “decision units” comprise the top portion of the sociotechnical system or “decision-making hierarchy.” The figure labels “coordination” as the interaction between decision units and “control” action from a decision unit to the physical process.

As conceived by Mesarović et al. (1970), the interaction among decision units throughout the decision-making hierarchy is coordination. Control action behavior is an interaction with the physical process by the lowest level decision units only. Decision units have the responsibility to make goal-directed decisions.

In addition to hierarchical systems, coordination can be found between decision units in any organizational structure. For example, Sage and Cuppan discuss “Federation of Systems,” which is an organization characterized by operational and managerial independence of systems (Sage & Cuppan 2001). In other words, there is little central control in federations. However, the “participation of the coalition of partners is based upon collaboration and coordination to meet the needs of the **federation**” (p. 327, emphasis in original).



The focus of coordination in this thesis is between decision units in sociotechnical systems. Coordination is a behavior related to decisions and actions in part by the desire to achieve system goals.

2.3.2.2 Coordination and Degrees of Freedom

“Behavior in the organization is not determined in advance and once for all by a detailed blueprint and schedule. Even if it is highly routinized, the routine has the character of a strategy rather than a fixed program” (March & Simon 1958) p. 26.

“...higher level [decision] units condition but do not completely control the goal-seeking activities of the lower-level unit. The lower level decision units have to be given some freedom of action to select their own decision variables...” (Mesarović et al. 1970) p. 50.

The concept of degrees of freedom, or alternatives afforded to the goal-directed behaviors, is important for coordination when interdependent conditions exist between decision units. At the system level, goals take the infinite degrees of freedom in the universe and define the system boundaries. Constraints on

system outcomes further define an envelope of acceptable behaviors and actions, which each decision unit must operate within (Rasmussen 1997a). Even with system constraints, there are usually many degrees of freedom left for decision units to manage, or to coordinate. Degrees of freedom have different implications for coordination based on whether it is vertical or lateral coordination.

In the vertical dimension, there is *coordination by control*. An example of coordination by control is in the organizational sense between hierarchical decision units (March & Simon 1958; Mesarović 1970). Another example of coordination by control are rules and regulations (Weichbrodt 2015). The vertical dimension refines and may further restrict degrees of freedom in each successive lower level in the hierarchy. With each successive level, the decision units get closer to the real-time process and are able to coordinate by control with more timely feedback. It is the last decision units that act upon a physical process within the degrees of freedom afforded and out outcome emerges; if designed correctly, this outcome falls within the system constraints and meets the system goals.

Coordination relationships exist in the lateral dimension as well. Degrees of freedom are given by the hierarchical structure above. Coordination by interdependent decision units may help achieve beneficial outcomes. Bernstein noted that the more degrees of freedom the more “complex and delicate” the coordination must be (Bernstein 1967) p. 105. The corollary to this statement is that (motor) coordination is the “mastering” of degrees of freedom (Bernstein 1967). Applied to lateral coordination, peer interdependent decision units should address given degrees of freedom, otherwise they may not achieve desired or even acceptable system outcomes.

Coordination manages degrees of freedom in sociotechnical systems in the vertical and lateral sense.

2.3.2.3 Coordination and Uncertainty

“Uncertainty appears as the fundamental problem for complex organizations, and coping with uncertainty, as the essence of the administrative process” (Thompson 1967) p. 159.

Uncertainty is an influential concept in the discussion of coordination and is relevant to systems and organizations alike (Ashby 1958; March & Simon 1958; Mindell 2000; Wiener 1956). The challenge is what to do about uncertainty. One paradigm assumes uncertainty away or minimizes uncertainty. In doing so, problem solving follows a normative and prescriptive approach. In this mechanistic view, coordination that is highly prescriptive and limiting on degrees of freedom is perhaps efficient; these scenarios may be ideal for automation.

Prescriptions in the face of uncertainty may only work in static and simple scenarios, which is not representative of sociotechnical systems. An alternative paradigm acknowledges uncertainty and recommends that coordination strategy be able to handle system internal and external uncertainty. Rather than prescription, uncertainty requires flexible coordination that can adapt when the uncertainty was realized with an unplanned scenario (Grote et al. 2009).

Systems and organization theory embrace uncertainty for they address the real world; failing to acknowledge uncertainty is not a successful strategy. Thompson describes three uncertainty types organizations face internally and externally, shown in Table 8; certainty in goals or purpose is assumed.

Table 8. Organizational Uncertainty (Thompson 1967)

Uncertainty	Description and Responses
External – Generalized uncertainty	Generalized external uncertainty is related to culture and the existence of an organization. It is the highest and “worst” uncertainty abstraction that must be resolved “first” by understanding cause/effect relationships of the organization and culture (p. 160).
External – Contingency	Once generalized uncertainty is addressed, an organization can move to contingency (or environmental) uncertainty. Responses may include negotiations, buffering, or coordination mechanisms able to “match” environmental uncertainty. This concept is similar to Ashby’s Law of Requisite Variety in cybernetics (Ashby 1958).
Internal – Interdependence of components	An organization seeks to minimize internal uncertainty through coordination.

In real systems, the mechanistic and uncertainty paradigms may coexist with various portions of the system under high and low uncertainty (Flach 2012; Thompson 1967). Having both prescription and flexibility are discussed in the literature under different labels of “loose coupling” (Weick 1976), “resilience” (Hollnagel et al. 2006), and “situated action” (Suchman 1987) for example. Rather than an all or none approach, a balanced coordination approach to handling uncertainty is advocated (Grote 2004). Using Thompson’s coordination descriptors, a balanced approach uses standardization, sequential and mutual adjustment coordination strategies to achieve system goals.

Table 9 provides a perspective on coordination methods as defined by (Thompson 1967) and its relationship to uncertainty as discussed by (Grote et al. 2009). There are four uncertainty categories when decomposed by 1) low and high uncertainty and 2) system (i.e. internal) and environmental (i.e. contingency) uncertainty, shown in Table 9. The decomposition should be conceived as a spectrum of uncertainty rather than as discrete categories.

Table 9. Coordination and Uncertainty

	Environment: low uncertainty	Environment: high uncertainty
System: low uncertainty	(i) static, simple, routine scenarios <ul style="list-style-type: none"> • ideal, normative models, closed system • coordination by standardization (i.e. control) • remove degrees of freedom 	(ii) naturalistic and competitive environments <ul style="list-style-type: none"> • e.g. financial industry • coordination by standardization, plan, mutual adjustment • coordination to balance control and flexibility
System: high uncertainty	(iii) emergent system in stable environment <ul style="list-style-type: none"> • e.g. start-up in established industry • coordination by standardization, plan, mutual adjustment 	(iv) complex sociotechnical systems, open systems <ul style="list-style-type: none"> • e.g. Space transportation, United Nations

	<ul style="list-style-type: none"> • coordination to balance control and flexibility 	<ul style="list-style-type: none"> • coordination by plan and mutual adjustment (i.e. flexibility)
--	---	---

At one end of the spectrum, Table 9(i) there is low uncertainty in both environment and the system. A system in this quadrant is characterized by one or more of: static, simple, routine, or highly constrained. Coordination for condition (i) may be achieved by standardization methods that are less flexible and more prescriptive in nature. Examples include physical barriers or guides for decision units to follow, such as the Panama City Canal lock system and car traffic roundabouts.

At the other end of the spectrum, Table 9(iv) describes systems and environments with high uncertainty, which is more representative of sociotechnical systems. These systems are complex and uncertain for many reasons, one being the degrees of freedom inherent or demanded from a system (Flach 2012). To handle the uncertainty, coordination that enables flexible responses such as planning and mutual adjustment is needed. The use of standardization coordination may still be beneficial for low uncertainty aspects of the system. An example of flexible coordination is ATC interacting with pilots to accommodate non-routine tasks and uncertain environments (e.g. thunderstorms) in a timely manner.

Quadrants (ii) and (iii) represent a mix of high and low uncertainty. A balanced approach is perhaps beneficial for these conditions: coordination by control to handle the routine aspects and flexible coordination to handle uncertainty.

The acknowledgement of uncertainty has several implications what coordination strategy to use. First, coordination by control methods such as standardization cannot be the sole means of coordination in sociotechnical systems. Predetermination of detailed action behaviors may neither be feasible nor be desired. Stated another way, rules are not always the answer (Dekker 2003; Leplat 1998; Weichbrodt 2015) and automation is not always the answer (Flach 2012; Flach 2016; Sheridan 2002). Second, coordination that enables flexibility in actions is required to address uncertainty faced internal and external to systems.

2.4 Safety and Coordination

Coordination has limited exposure in the safety literature and prior work. Traditional safety analysis methods largely address failures (e.g. FMEA and fault trees) and deviations from a normative model (e.g. HAZOP). Traditional analysis methods have a component focus and in many cases assume independence of events, which is not conducive for analysis of coordination behavior. General discussion on coordination and safety, and a focused investigation of systems theoretic safety analyses are presented in this section.

2.4.1 General Safety Concepts and Coordination

Resilience engineering is a set of concepts around the ideas of: flexibility and adaptability; detection of migration toward unsafe boundaries; anticipation and response to disturbances; and sustained motivation

to improve (Sheridan 2008). Resilience engineering espouses concepts related to coordination (Hollnagel et al. 2006). However, resilience engineering is more of a philosophy of safety than an analysis technique and has proved difficult to operationalize for use (Sheridan 2008).

Leplat discusses two coordination “dysfunctions” that may lead to accidents (Leplat 1987). The first dysfunction is “Boundary areas as zones of insecurity” (p. 183). The boundary area is discussed pertaining to boundaries of responsibilities that affected the physical process. The example given was floor cleaning not accomplished because one organization believed the other was responsible. The second dysfunction includes “Zones of overlapping as zones of insecurity” (p. 184). Overlapping zones are where multiple agents act on the same process. The example provided is overlapping rules for the same construction site. Leplat identifies one of several coordination relationships that can occur in sociotechnical systems—multi-agents and single process—to be discussed in the next chapter.

2.4.2 Systems Theoretic Safety Analyses and Coordination

2.4.2.1 STPA and Coordination

(Stringfellow 2010) provides analysis guidance for coordination related to STPA, which identifies trust, communication, and communication protocols as areas for evaluating coordination (p. 94):

1. Be motivated by,[sic] trust, and understand controller commands.
2. Be able to communicate information (give feedback) to the controllers about any problems or concerns that arise with the directive and be able to articulate an alternative option, if available.
3. Be able to freely communicate safety concerns up the command and control structure (e.g. without fear of retribution, concern that communication is 'unimportant', or concern that the boss will be upset).
4. Know the protocol for communicating with the controller: for example, sensors may need to know whether it is the responsibility of the controllers to ask sensors for information, or whether it is the sensor's responsibility to filter and relay relevant information to the controller.

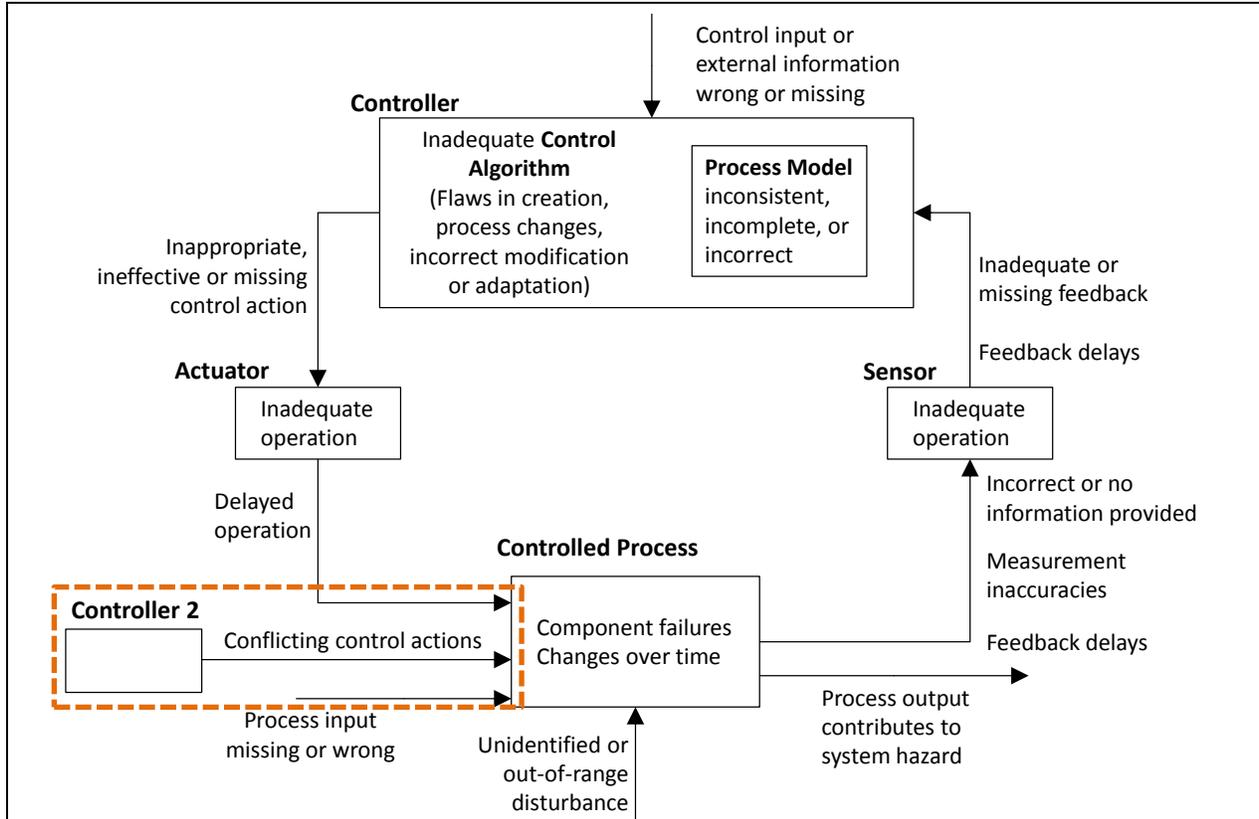
Stringfellow’s guidance is for vertical coordination (i.e. control-theoretic) involving humans. She also acknowledges, but did not pursue, team coordination as a concept related to STPA: “A causal factors taxonomy that is specially designed to focus on teams is left for future work” (Stringfellow 2010) p. 107. Team coordination *future work* is in part addressed by this thesis as lateral coordination.

In STPA, coordination is a potential cause for unsafe controls and is briefly discussed in STPA step 2 causal analysis guidance:

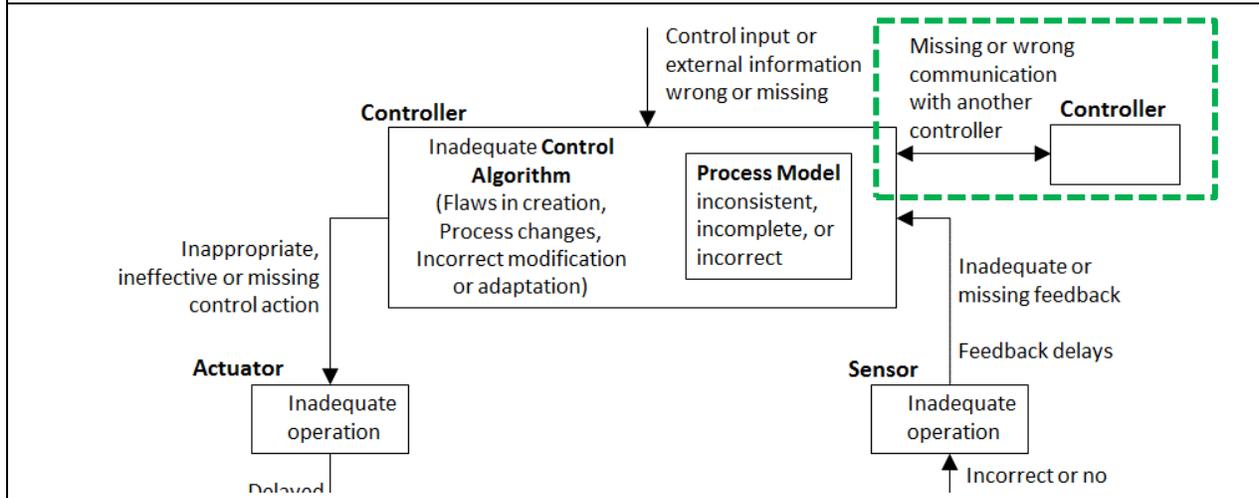
- Unsafe control caused by “inadequate” coordination between decision-makers (Leveson 2004; Stringfellow 2010; Stringfellow et al. 2010).

- “For multiple controllers of the same component or safety constraint, identify conflicts and potential coordination problems” (Leveson 2012) p. 213.

STPA literature provides a feedback control model in diagram form with guidewords to assist in the safety problem conception and analysis, which is reproduced in Figure 7.



(a) Adapted from (Leveson 2012), p. 93. © 2012 by MIT, published by MIT Press. Reprinted with permission.



(b) Adapted from (Leveson 2015), p. 28. © 2015 by Elsevier. Reprinted with permission.

Figure 7. Control Feedback Loop Guidance, Unsafe Control Action Causal Analysis

In Figure 7(a), coordination of multiple controllers on a single process is shown in the lower left hand corner and labeled “conflicting control actions” (Leveson 2012); this is the same coordination relationship identified by Leplat (1987). In a more recent publication, the causal analysis guidance diagram was updated to include “communication with another controller” shown in the upper right corner of Figure 7(b) (Leveson 2015).

How STPA conceives of and addresses coordination has evolved. However, there remains limited guidance beyond acknowledgment of an interaction with a single process or another controller.

2.4.2.2 CAST and Coordination

CAST (Causal Analysis based on STAMP) is an accident investigation method based on STAMP. CAST is structured with nine general steps to be accomplished, not necessarily in this particular order (Leveson 2012):

- 1-2. Systems engineering baseline. Identify accidents, hazards, safety constraints.
3. Document the safety control structure, including roles and responsibilities.
4. Identify proximate events.
5. Identify unsafe controls, failures, and interactions at the physical system level.
6. Identify why higher levels allowed or contributed to the accident. Document the context for decisions.
7. “Examine overall coordination and communication contributors to the loss” (p. 351).
8. Determine if migration towards unsafe behaviors was a factor.
9. “Generate recommendations” (p. 351).

Accident investigation using CAST recognizes that accidents occur from unsafe interactions throughout a sociotechnical system. The idea of a root cause is dismissed in a systems approach. While coordination is acknowledged, CAST analysis guidance for coordination is limited to the step 7 quote above.

2.5 Summary and Research Gaps

“...designing engineering systems involves significant extensions to the traditional design process applied to less complex systems” (de Weck et al. 2011) p. 124.

This chapter reviewed the literature related to safety and coordination. This thesis is concerned with coordination among interdependent decision units. Interdependency may come from organizational, temporal, reciprocal, and shared resource conditions for example. To manage these interdependencies, different strategies were identified from standardization to more dynamic (or mutual adjustment)

strategies. Successful management of coordination is assisted by “integrating” conditions of accountability, common understanding, and predictability. The processes needed for coordination include group communications, group decision-making, and observation of common objects.

Traditional safety analysis methods primarily use a chain-of-failure events model for accident causation, such as the Swiss Cheese model. Analysis methods derived from this accident causation model use failure and reliability measures to operationalize safety. While perhaps adequate for the analysis of electromechanical systems, a concern with traditional analysis methods is that they capture only a subset of potential accident scenarios in complex, human- and software-intensive systems. Another concern more directly related to this thesis is that there is limited to no integration of coordination in traditional safety analysis methods.

STAMP is a systems-theoretic accident model that characterizes accident causation due to flawed functions and interactions, both linear and non-linear, in addition to failures. The implication is that design and requirements errors may lead to accidents. Based on STAMP, STPA and CAST use a systems-theoretic and top-down systems engineering approach to analyze systems. STPA identifies unsafe control actions that may lead to hazardous outcomes, and scenarios that may cause the unsafe control to occur. CAST investigates accident causation from a holistic systems perspective, asserting that accidents do not occur from a root cause. In part, CAST identifies inadequate controls and coordination as accident influences. While coordination is acknowledged, limited guidance exists for analysis of coordination in both STPA and CAST.

The literature and knowledge gaps can be summarized as:

State-of-the-art safety analysis methods have limited conceptual depth and analytical guidance to evaluate coordination behavior between multiple interdependent decision units.

To begin addressing the identified knowledge gap, a coordination framework should be developed to increase explanatory power for the observation and analysis of coordination in sociotechnical systems. One such coordination framework is introduced next.

3 A COORDINATION FRAMEWORK

This chapter introduces a coordination framework. The coordination framework is the link between theory and engineering application, and is the foundation for STPA and CAST extensions and flawed coordination analysis guidance introduced in the following chapters.

The coordination framework consists of four conceptual points that provide common understanding and explanatory power for the observation and analysis of coordination and safety in complex work domains. The first point is a decision functional model that describes observed group coordination, and individual decision and action behaviors in sociotechnical systems. The second is coordination decomposed into a components, processes and conditions. The third is set of fundamental coordination relationships in sociotechnical systems. The last point provides perspectives on the evaluation of coordination that are used to operationalize the coordination framework for analysis.

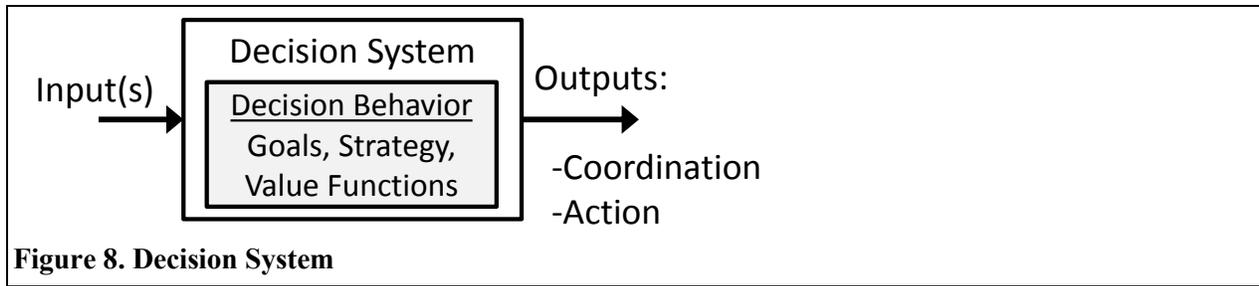
3.1 Decision Systems

This section introduces a *decision system* (DS) for analysis of coordination. The decision system is a functional model that relates the decision function to coordination and actions as discussed by Mesarović et al. in the BACKGROUND. The purpose of the decision system is to provide explanatory power for observed coordination behaviors and provide a common language for use in analysis of coordination.

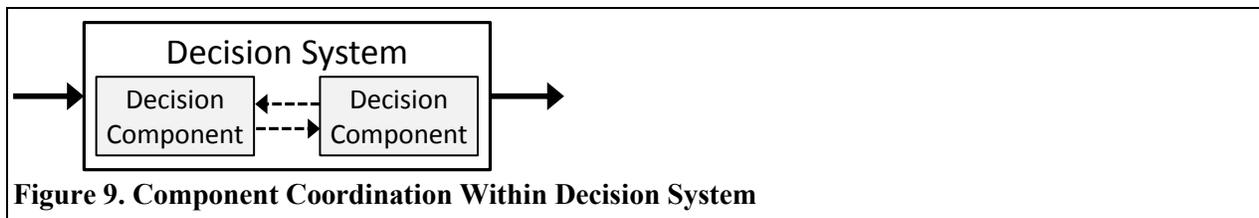
Up to this point in the thesis, the use of the word decision *unit* has been deliberate in order to discuss a general decision-making entity. Early systems theorists also used the term as shown in Figure 6. For systems theoretic analysis, a decision unit can be described by its functionality as a decision system. The decision system makes decisions and outputs one or both of coordination and action signals for another decision system or physical process. Decision system inputs are the information needed to make decisions.

The decision system black box makes decisions related to the common behavior output. The decisions of interest for safety are labeled “dynamic” decisions by (Brehmer 1992), which need the following:

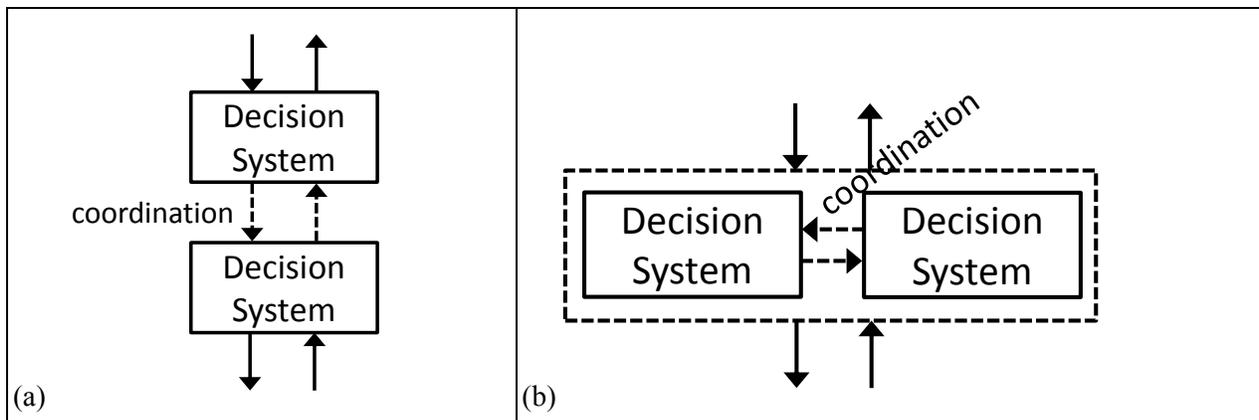
- Goals. Decisions need goals (Ashby 1956). Goals provide overarching guidance and a basis for determining what is beneficial and desired for sociotechnical systems.
- Strategy. The means to accomplish goals.
- Value functions. A way to evaluate decision alternatives, often faced with multiple competing goals and strategies (Flach 2015). Value functions (also called cost functions or payoff matrices) may be simple goal rankings and priorities, or may be more sophisticated mathematical algorithms. Value functions apply to both humans and automation. Note this thesis does not develop a decision framework or force the use of any decision theory for analysis.



With a functional model, analysis can distinguish between function and form. The form the decision system may take includes one or more decision-making *components*, which can be humans and automation. Decision components should coordinate decisions and actions for their common decision system output; this is called *within decision system* coordination, represented in Figure 9.



Coordination is also observed *between decision systems*, represented in Figure 10. Figure 10(a) shows vertical coordination between decision systems. Vertical coordination implies hierarchy and uses coordination by control methods, which can vary by degrees of freedom afforded to lower-level decision system behaviors. The other interaction between decision systems is lateral coordination, shown in Figure 10(b). Lateral coordination is a peer interaction where control is not implied. Examples of lateral coordination are observed in teams, ad-hoc organizations, and heterarchies in general.



The decision system concept provides descriptive power for coordination in sociotechnical systems and includes two conceptual relationship pairs: 1) within and between decision system coordination and 2) vertical and lateral coordination.

3.2 Decomposing Coordination

The concept of coordination is often oversimplified. This simplification is insufficient for analysis and design of sociotechnical systems with multiple interdependent decision systems. This section introduces a set of coordination elements that together describe what coordination is and how it should be accomplished, which was inspired from the organizational and coordination literature addressed in section 2.3 above.

3.2.1 Coordination Elements

Coordination can be decomposed into three categories. First are coordination components that describe the basic building blocks for coordination behavior. Second are processes that enable the basic components to engage in coordination behavior. Last, there are enabling conditions that describe how to carry out coordination. The three coordination categories are further refined into nine *coordination elements*, which address the “what” and “how” of coordination. The coordination elements are labeled numerically 1-9 for standardization in this thesis; the numbers do not indicate a priority scheme.

3.2.1.1 Coordination Components

The components represent the building blocks of coordination behavior in sociotechnical systems. The components address what is coordination and are inspired primarily by (Malone & Crowston 1990).

(1) Coordination Goals

Perhaps at the most fundamental level, coordination needs a goal. The coordination goal is also the minimum interdependency that unifies decision systems in a system (or organization). Without coordination goals, there are independent agents seeking to satisfy different and possibly competing system or individual goals. Some concerns include goal prioritization and goal divergence with time.

(2) Coordination Strategy

In sociotechnical systems, a coordination strategy is the planned set of behaviors among two or more decision systems or decision components. As discussed in the BACKGROUND, a coordination strategy can take on several forms including standardization or more real-time mutual adjustment strategy. The coordination strategy is goal-driven and must ultimately address behaviors that interact with the physical layer processes. This thesis uses the coordination strategy as the common thread for analysis of coordination behavior, with other coordination elements in support of developing and carrying out the strategy.

The coordination strategy must be adequate for the system and environment. Standardization may be adequate for coordination in simple, routine, and relatively static systems and environments. Strategy can be inadequate when its flexibility does not match the scenario variety. In systems theory, this concept is captured by Ashby’s Law of Requisite Variety that eloquently states “...*only variety in R can force down the variety due to D*; **variety can destroy variety**” (emphasis in original) where R is a regulator and D represents disturbances (Ashby 1956) p. 207. For example, standards that restrict action behaviors will have challenges when changes and the unexpected occur and standard actions no longer apply.

Another concern for coordination strategy is establishing one too late to influence an outcome. When it is too late, decision systems act independently. Too early is a competing concern, especially in uncertain and dynamic systems and environments that may necessitate a coordination strategy update to remain relevant.

Coordination strategy can be an output of coordination behavior. Coordination strategy may also be an input from higher-level decision systems that serve to guide and constrain behaviors. The use of and interaction with coordination strategy depends on where the focus of inquiry is in the system. The coordination strategy may apply to the physical process coordination (e.g. how multiple aircraft navigate through the National Airspace) or it may apply to coordination among the decision-making hierarchy (e.g. budgets, laws and regulations).

(3) Decision Systems

Coordination requires decision systems, the last basic coordination component. Some concerns for analysis and design of coordination is identifying the needed decision systems and ensuring adequate decision system capability to address the interdependent conditions using coordination. Decision systems are comprised of humans and automation decision components.

3.2.1.2 Coordination Enabling Processes

The processes that enable coordination include group decision-making, communications, and observation of common objects. The enabling process elements integrate the coordination components and provide the environment to engage in coordination behavior. The coordination processes are also inspired primarily by (Malone & Crowston 1990).

(4) Communications

Communications describe the capabilities and protocols needed to relay information within and between decision systems. In the safety literature, the term “communications” was often lumped into one description of “coordination and communication” such as shown in HFACs Figure 4 with limited to no further distinction between the concepts; the terms are perhaps used interchangeably. In this framework, communications and coordination are at different abstraction levels with communications a sub-process of the overall coordination behavior.

(5) Group Decision-Making

Group decision-making (DM) describes the processes within or between decision systems to determine alternatives, evaluate them, and make decisions. Group DM is different from the responsibility to make a final decision, which is discussed next in enabling conditions. Regardless of which decision system (or decision component depending on the abstraction) has decision responsibility, group DM processes enable the interaction for a decision to be made. Group DM addresses the physical or virtual environments, the protocols, the barriers, the conceptual frameworks, and value functions to name a few. Group decisions may occur

Group DM may not apply to the description of every coordination interaction, however. For example, coordination by standards may assign pre-planned actions of lower level decision systems where group

DM is not required or not addressed. Even if coordination by standards does not address group DM, developing the standards in the first place or updating them may require group DM.

Analysis of coordination should investigate where group DM is missing or inadequate among decision systems, which may lead to unacceptable outcomes (e.g. a hazard).

(6) Observation of Common Objects

With multiple decision systems, observation of common objects is beneficial and perhaps necessary depending on the context. In all phases of coordination, from strategy planning to strategy execution achieving an acceptable outcome relies on observation or knowledge of common objects. In addition to the content of observation, this coordination element is impacted by observation protocols. For example, decision systems may observe the same object at different times or using different data filters. In such cases, coordination behavior may be negatively affected even though the same object is being observed.

3.2.1.3 Coordination Enabling Conditions

The enabling conditions relate to the coordination strategy and describe *how* to accomplish coordination. The enabling conditions are primarily inspired by (Okhuysen & Bechky 2009) work in coordination theory that describes “integrating” conditions of accountability, predictability, and common understanding.

(7) Authority, Responsibility, Accountability.

Accountability is closely related to authority and responsibility within the management literature. Kerzner distinguishes between authority, responsibility, and accountability (ARA) as follows (Kerzner 2009):

- “Authority is the power granted to individuals (possibly by their position) so that they can make final decisions” (p. 94).
- “Responsibility is the obligation incurred by individuals in their roles in the formal organization to comprehensively perform assignments” (p. 94).
- “Accountability is being answerable for the satisfactory completion of a specific assignment. (Accountability = authority + responsibility)” (p. 95).

Authority and responsibility apply to decision system goal-directed behaviors—coordination, decision, and actions—that are assigned to decision systems. There should be responsibility assigned for development through execution of coordination and matching authority.

Accountability is an integrating condition for interdependent decision systems in coordination, and it goes beyond the management definition above. In coordination, accountability is concerned with dynamic efforts to have knowledge about other interdependent decision systems and if they are carrying out a coordination strategy as intended.

One of the more fundamental concerns with accountability is the ability to influence another decision system’s decisions, or coordinability. Coordinability is concept discussed by (Mesarović et al. 1970) in relation to hierarchical systems. Coordinability as defined by Mesarović et al. (1970) has been explicitly

related to “accident causation and prevention” (Cowlagi & Saleh 2013). Coordinability is not a hierarchical concern alone, however; it applies to both vertical and lateral, and within and between decision system coordination. Both humans and automation must be coordinable to achieve goals when interdependent conditions exist. Lack of coordinability, such as automation that makes decisions independent of other decision systems, may lead to unacceptable outcomes.

A concept intimately related to accountability and coordination is trust and confidence (Okhuysen & Bechky 2009). (McEvily et al. 2003) suggest that trust affects “...the interaction patterns and processes that enable and constrain the coordination of work among individuals” (p. 94). Lee and See also recognize the importance of trust in human and automation interactions (Lee & See 2004). Without confidence in other interdependent decision systems, coordination can suffer.

Accountability is concerned with observation and feedback from interdependent decision systems. Accountability is applicable to coordination strategy including its development, implementation, compliance with, and execution. Accountability is also concerned with coordination evaluation and update efforts. For example, there should be mechanisms to inform decision systems when strategy implementation begins when visual confirmation is infeasible. What is needed for and how to achieve accountability in coordination should be addressed by analysis.

In summary, successful coordination within and between decision systems needs authority, responsibility, and accountability.

(8) Common Understanding

Common understanding is “...a shared perspective on the whole task and how individuals’ work fits within the whole” (Okhuysen & Bechky 2009) p. 488. Coordination requires that decision systems have a common understanding of the problem and solution—an understanding of who, what, where, when, why and how. Some of the information aspects fundamental to common understanding and coordination are: 1) that interdependent conditions exist, and 2) what decision systems are affected and should be in coordination.

Common understanding of *why* coordination is needed at local and system levels may assist and influence decision systems to engage in coordination behavior and follow through with necessary actions. Ensuring enough common understanding may be a challenge in hierarchical coordination interactions. For example, common understanding of why managers make decisions or why a problem needs particular decision systems can influence compliance by lower-level decision systems. Without knowing why, a decision system may delay, alter, or perhaps ignore a coordination strategy from higher-level decision systems.

Common understanding, however, does not mean the same understanding. Often in organizations and hierarchical structures, the same understanding may not be feasible or desired. For example, military operation not provide soldiers and airmen all information on why a mission is being carried out due to operational concerns, information security concerns, etc. There may also not be enough time to fully explain why a certain strategy was invoked to involved decision systems. In fighter aircraft operations, for example, pilots may direct actions for immediate execution and explain why after the fact. While common understanding may not mean the same understanding for why coordination occurs, other perspectives of who, what, where, when and how should be the same.

Common understanding enables successful coordination outcomes. What is needed for and how to achieve common understanding should be addressed in analysis of coordination efforts.

(9) Predictability

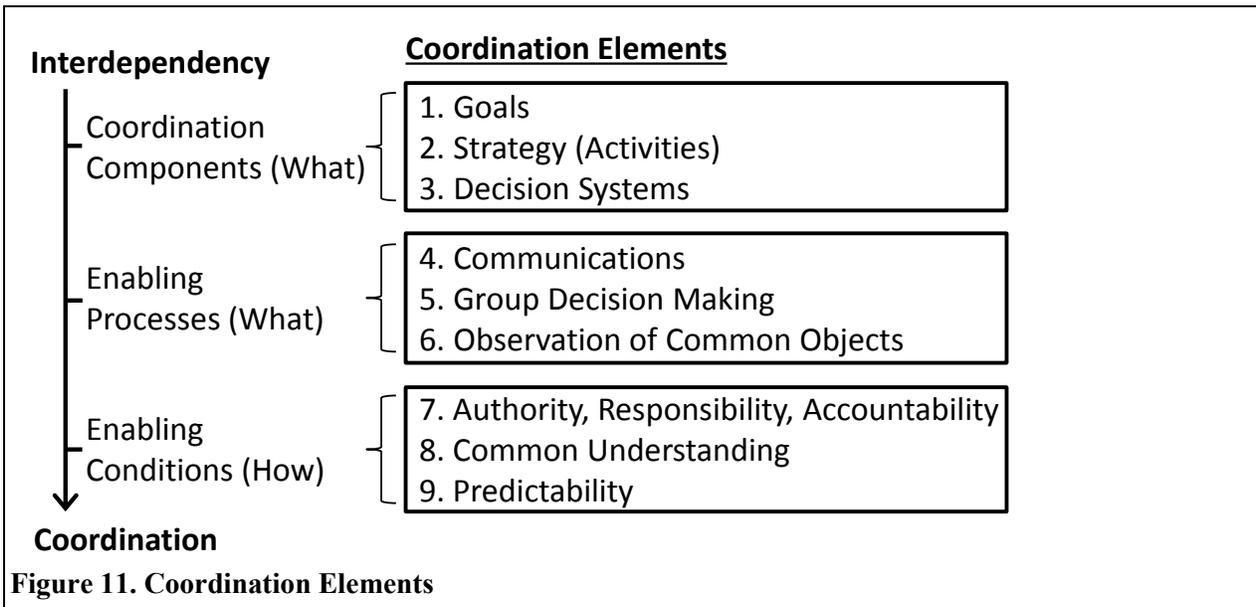
Predictability is concerned with future behavior and is applicable to coordination, decisions, and action behaviors. Predictability is what enables organizations to be proactive (Fannin & Rodrigues 1986). Without predictability coordination efforts are forced to be reactive, which can lead to accidents in the worst-case scenarios where a reaction is not feasible.

Coordination needs predictability to anticipate decision system behaviors, and to anticipate local or system outcomes as needed. Predictability should be accurate. In humans, training can influence predictability. In automation, predictability is constrained by the algorithm. The automation algorithm is constrained by the designer’s local and holistic models and ability to implement them into the algorithms. The design of automation predictability may benefit from use of a systems theoretic approach discussed in this thesis and other such as “intent specifications” (Leveson 2000) to manage comprehension of local and holistic interactions that can quickly push human cognitive limits.

Predictability is an enabling condition for coordination in sociotechnical systems. Analysis should address what is needed and how to achieve predictability.

3.2.2 Partial Coordination

Coordination is decomposed into three categories and nine coordination elements, summarized in Figure 11. As shown, when an interdependent condition exists within or between decision systems (top left), coordination (bottom left) should address the needed components, processes, and enabling conditions.



The nine coordination elements provide a perspective that coordination lies on a spectrum. Anchored on one end of the coordination spectrum is none or missing coordination. Anchored on the desired end of the

spectrum is holistic coordination, where all necessary elements are present. Between the spectrum anchors, there is *partial* coordination, which is a primary emphasis for analysis of coordination. The coordination spectrum can be summarized as follows:

- None. The coordination elements that indicate coordination exists or is occurring are missing, in particular coordination goals, coordination strategy, and group decision-making.
- Partial coordination. One or more of the nine coordination elements is missing or inadequate.
- Holistic coordination. Coordination has the necessary elements of nine in this framework.

Analysis of coordination may benefit from methods that can characterize and address partial or inadequate coordination.

3.2.3 Coordination Decomposed Summary

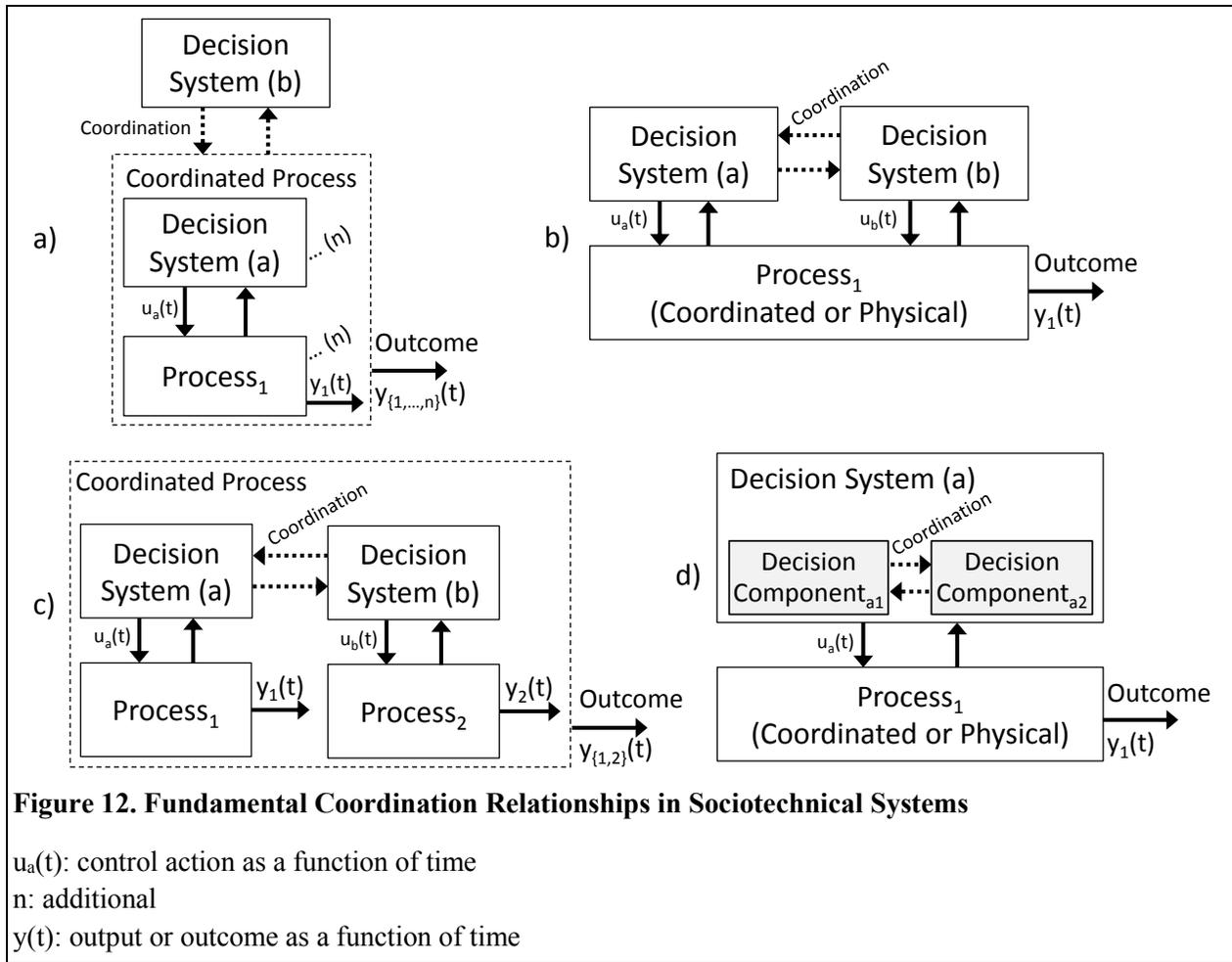
The thesis started with a definition of coordination: the management of and the processes needed to integrate interdependent entities. The nine coordination elements expand this definition. The “management of” refers to the following coordination elements (numbers for standardization): (1) coordination goals, (2) coordination strategy, (7) authority, responsibility, accountability, (8) common understanding, and (9) predictability. The “processes needed” refers to: (4) communications, (5) group decision-making and (6) observation of common objects. The (3) decision systems are the “interdependent entities” of interest. The nine coordination elements can be used to improve accident investigation and derive coordination-related safety design requirements that lead to safe outcomes.

3.3 Fundamental Coordination Relationships

This section derives a set of four *fundamental coordination relationships* in sociotechnical systems that provide descriptive power for analysis. By observation, there are three dimensions related to coordination interactions, including: 1) vertical or lateral coordination, 2) within or between decision system coordination and 3) coordination to control a single or multiple independent processes. The controlled process can be considered a coordinated process (i.e. other decision systems) or a physical process. Table 10 is a three-factor matrix that identifies four unique coordination relationships referenced to Figure 12. Figure 12 depicts the fundamental coordination relationships, labeled “coordination” (dotted arrows).

Table 10. Fundamental Coordination Relationship Matrix

	<i>Single Process</i>		<i>Multiple Independent Processes</i>	
	Between Decision Systems	Within Decision System	Between Decision Systems	Within Decision System
Vertical	Figure 12a	n/a	Figure 12a	n/a
Lateral	Figure 12b	Figure 12d	Figure 12c	n/a



3.3.1 Vertical Coordination, Between Decision Systems

Figure 12a represents vertical coordination between a decision system and a lower-level coordinated process. Vertical coordination is addressed by coordination by control methods. Mesarović et al. labeled this vertical interaction “conditioning” (Mesarović et al. 1970); that is, coordination by control is a way to condition a desired response from lower level decision units. Rules and regulations are typical method for coordination by control (Grote et al. 2009; Leplat 1998; Weichbrodt 2015). Real-time coordination by control methods are also common, such as with Air Traffic Control and aircraft.

Coordination by control methods restricts lower-level decision system degrees of freedom to achieve desired system outcomes. The restrictions on output behaviors can vary on a spectrum from low to high. Lower restrictions on degrees of freedom give more freedom of action for a coordinated process. Lower restrictions may be desired and even necessary to achieve successful outcomes when operating in uncertain internal or external conditions such as emergency management (Flach et al. 2013) and in military operations with the idea of communicating “commander’s intent” to subordinate commanders (Shattuck 2000). Lower restrictions may simply provide an acceptable envelope for system outcomes, leaving coordinated processes the freedom to determine actions to remain within the envelope.

On the other end of the spectrum, coordination by control may severely restrict degrees of freedom to achieve desired outcomes. In such cases, coordination by control methods may prescribe highly detailed actions for the coordinated process to perform to achieve desired results. An example is in commercial flight operations when aircrews operate under ATC coordination. Aircrews often have little freedom of action and depend upon ATC to coordinate the multiple aircraft under their control for collision avoidance and efficient movement. ATC coordination with aircrew is a vertical relationship similar to the control theory depiction of a controller and a physical process, which leads to Axiom [3.1].

[3.1] As coordination by control methods further restrict degrees of freedom on lower-level decision system actions, coordination strategy more resembles control actions on a physical process.

Unlike control of a physical process, however, lower level decision systems (e.g. aircrew) do not simply receive control action commands and execute without consideration. Aircrew ultimately make an individual decision to follow ATC coordination or not, which is conditioned largely by vertical coordination efforts with ATC.

3.3.2 Lateral Coordination, Between Decision Systems

Figure 12b and c represent lateral coordination relationships between decision systems. Lateral coordination is a fundamental interaction in sociotechnical systems. Lateral coordination seeks coordinated outcomes to achieve system goals while working within the given degrees of freedom.

Figure 12b shows lateral coordination where each decision system has direct channels to the process (physical or coordinated). A physical process coordination example is in aircraft control. Many cockpit configurations have direct flight control access for two flight crewmembers. A coordinated process example may be with parents and their interactions with a school system for concerns related to their children. Parents laterally coordinate and both have direct communication channels to the school. Lateral coordination directed towards a single process would benefit from a coordinated strategy that accounts for overlapping actions.

Figure 12c is lateral coordination between decision systems that each influence independent processes, coordinated and physical. An example of lateral coordination for independent physical processes includes multiple aircraft in operations where ATC does not provide separation services. Aircrew operating in uncontrolled airspaces and airfields use lateral coordination measures. An example of lateral coordination for independent coordinated processes is found in corporations. There may be a director of operations that manages operations and a director of human resources that manages recruitment and hiring. The company benefits from coordination of the two directors. The more holistic coordinated process outcomes benefit from lateral coordination of independent process outcomes.

3.3.3 Lateral Coordination, Within Decision Systems

Figure 12d represents within decision system coordination, which is a lateral coordination relationship. Lateral coordination among decision components is related to coordination of decisions and outputs of the decision system (e.g. control actions or coordination information). Human and automation decision

component examples exist in aviation. A remote pilot operator and a detect-and-avoid system coordinate decisions related to collision avoidance maneuvering. The Patriot missile system automation and human operators coordinate decisions for various phases of missile engagement.

Within decision system coordination of decisions benefits from information exchange related goals, strategy, and value functions. In cases where control action responsibility is mutable, lateral coordination benefits from information exchange assigning roles and responsibilities.

3.3.4 Fundamental Coordination Relationships Summary

The fundamental coordination relationships are basic conceptual building blocks of coordination in sociotechnical systems. As a basic building block, any given decision system may also be involved with one or more coordination relationships. For example, a supervisor or dedicated team lead may have vertical coordination responsibility (Figure 12a) and at the same time be part of a decision system that laterally coordinates for actions on the same physical process (Figure 12b).

There is potential for conflict, however, when coordinated processes are subject to highly limiting vertical coordination (Figure 12a) and mutual adjustment lateral coordination (Figure 12b or c) at the same time. A coordinated process may not be able to resolve simultaneous vertical and lateral coordination constraints. As an example, collision avoidance automation may suggest aircrew climb while air traffic control instructs aircrew to descend. The coordination strategies restrict degrees of freedom and are in conflict, which leads to axiom [3.2]:

[3.2] *When coordination methods are highly restrictive on decision system outputs, only one coordination strategy (vertical or horizontal) may be resolved at a time.*

The fundamental coordination relationships provide a common semantic and modeling framework for use in systems-theoretic analysis.

3.4 Perspectives on Coordination Related to System Outcomes

A descriptive and semantic coordination framework alone is of limited usefulness for engineering analysis. The coordination framework must be operationalized for analysis. This section describes in general terms *internal* and *external* perspectives that can be used to evaluate coordination against a defined set of acceptable outcomes. For safety and hazard analysis, acceptable outcomes are those free from accidents and the hazards that cause them.

In the following chapter, the internal and external coordination perspectives are operationalized for analysis with a new STPA extension.

3.4.1 Representing the Coordination Problem

Figure 13 represents a general coordination problem. There are two decision systems in coordination to influence an acceptable outcome with their coordinated output $y_{a,b}(t)$. The system outcome is the emergent result of the coordination interactions, the coordination output $y_{a,b}(t)$, and the coordination output interactions with the environment. The system outcome can be influenced by the coordination interactions between decision systems, which represent the internal perspective. The coordinated output with and without the environment represents the external perspective, which also influences the system outcome.

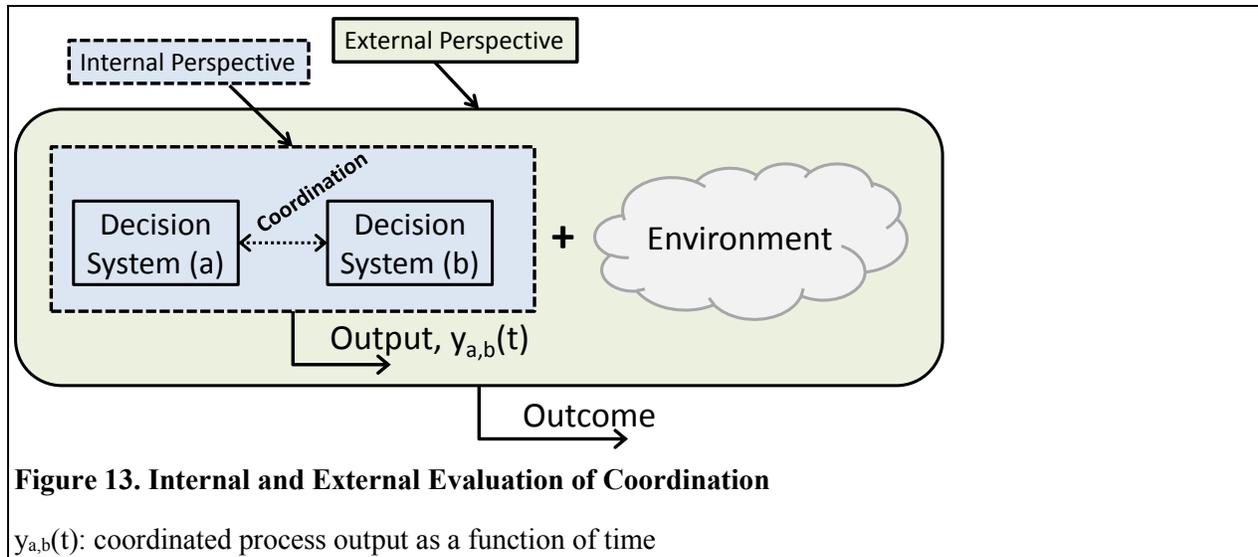


Figure 13. Internal and External Evaluation of Coordination

$y_{a,b}(t)$: coordinated process output as a function of time

3.4.2 Internal Perspective

The internal perspective is concerned with the coordination interaction itself, which is represented by the dashed (light blue) box surrounding Decision Systems (a) and (b) in Figure 13. The internal perspective asks if coordination has the necessary coordination elements to support a coordination strategy. If coordination is missing or there is partial coordination, the system outcome may be unacceptable given the worst-case context. For example, wartime communication channels used for aircraft coordination may be inadequate in contested airspace if there is communications jamming; in this scenario, one of the coordination elements (i.e. internal perspective) is inadequate for successful outcomes.

Having all coordination elements, however, does not indicate that the outcome will be acceptable. The coordinated strategy must still be evaluated, which is the external coordination perspective.

3.4.3 External Perspective, the Coordination Strategy

The external perspective is represented in Figure 13 by the solid (light green) box surrounding the decision systems in coordination and the environment. The solid box also represents the general system of interest. The external evaluation focuses on the coordination strategy element, and can lead to

unacceptable outcomes by: 1) the coordinated output $y_{a,b}(t)$ and 2) the coordinated output combined with environmental factors.

First, decision systems should develop a coordination strategy where the coordinated output $y_{a,b}(t)$ leads to acceptable outcomes (e.g. safe outcomes). For example, a coordinated process is engine start and launch procedures for the F-16 fighter aircraft. To safely launch the F-16, pilot(s) and ground crew must coordinate to accomplish a set of actions in sequence. Part of launching the aircraft includes an emergency power unit (EPU) check. The crew chief needs to communicate to the pilot when the EPU check is ready to be accomplished. If the crew chief has not finished necessary checks before the pilot begins the EPU check, the EPU check may lead to harming the crew chief under certain conditions.

Second, using the external perspective, one should evaluate the coordination strategy against the environment. For example, two pilots are flying independent F-16s on a collision course while accomplishing a flight test maneuver. The pilots develop a coordination strategy that aircraft (a) climbs and aircraft (b) descends to avoid a mid-air collision and continue the test point. This coordination strategy may be acceptable relative to the coordinated output $y_{a,b}(t)$ alone. However, aircraft (b) descends when already near terrain and is subsequently placed into a hazardous scenario that may lead to an unacceptable outcome—controlled flight into terrain.

For safety, the coordination strategy should not lead to hazardous scenarios. Hazardous scenarios can result from the coordinated output $y_{a,b}(t)$ or the coordinated output relative to the environment, which represent the external coordination perspective. Further, an external evaluation of coordination in dynamic systems must account for time.

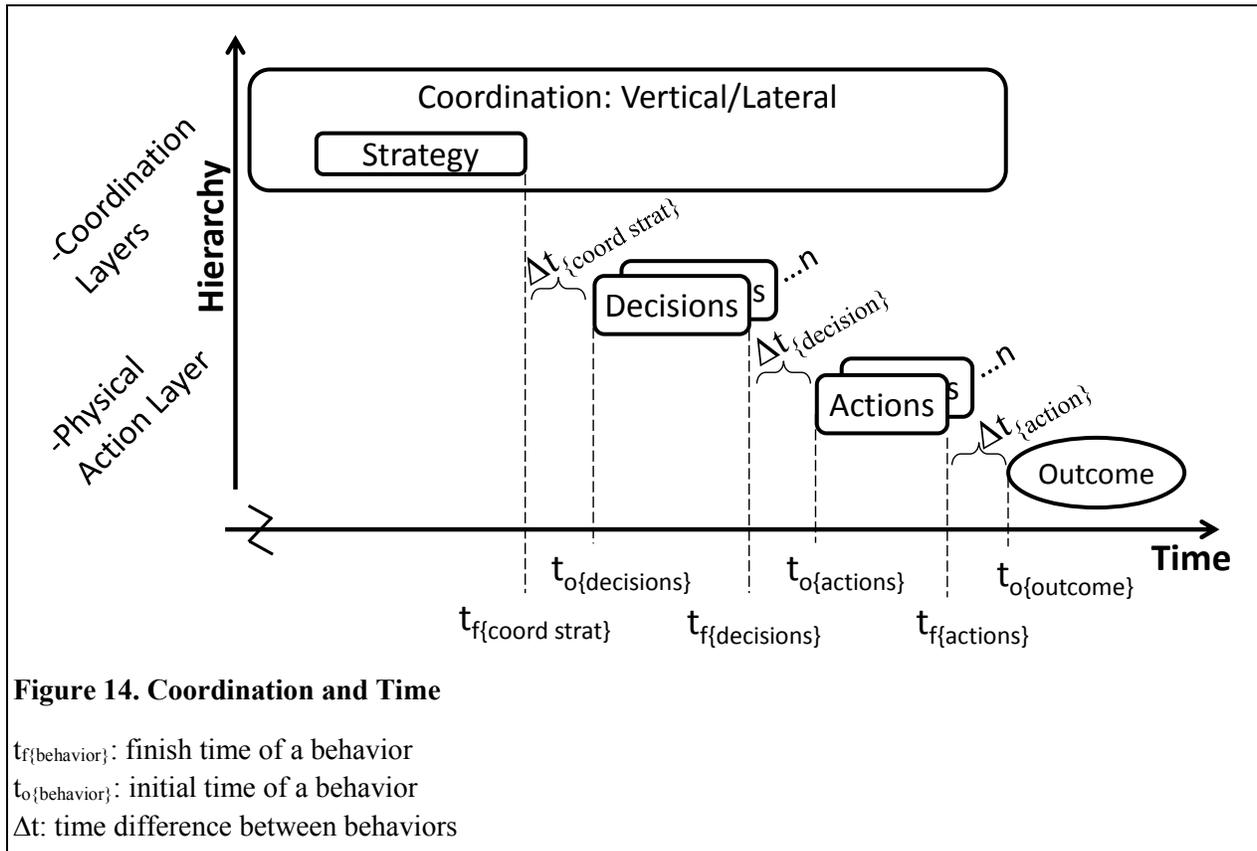
3.4.4 External Perspective, Temporal Constraints

Coordination takes place in dynamic systems that are temporally constrained; time is a necessary external perspective for the evaluation of coordination. In particular, the coordination strategy should be established before individual decision systems need them to avoid hazardous (or potentially hazardous) scenarios when under interdependent conditions. The coordination strategy can be established too late to influence an outcome; evaluation of coordination should investigate why a strategy was established late.

Figure 14 represents a temporal perspective for coordination in a dynamic sociotechnical system with time represented on the horizontal axis. The vertical axis represents a sociotechnical system hierarchy, with the decision-making hierarchy “coordination layers” and individual decision and action behaviors in the “physical action layer” at the hierarchy bottom. Coordination is an ongoing behavior with coordination elements such as observation, accountability, and common understanding ensuring the strategy is implemented as intended and that the strategy remains relevant through time. The ongoing concept is represented in Figure 14 by coordination temporally spanning the physical action layer behaviors.

Coordination behavior along with individual decision and control actions integrate through time and space to influence system outcomes. However, to influence an outcome with coordination there is a progression to the group and individual decision system behaviors. In the nominal case, coordination establishes a strategy, labeled in the figure by time $t_{f\{\text{coord strat}\}}$. Then decision systems can use the coordination strategy to make individual decisions and take appropriate actions on their own processes. In

the nominal case, there is adequate time to develop a coordination strategy and perform individual behaviors to influence the outcome as indicated in Figure 14 by some time difference $\Delta t_{\{\text{behavior}\}}$.



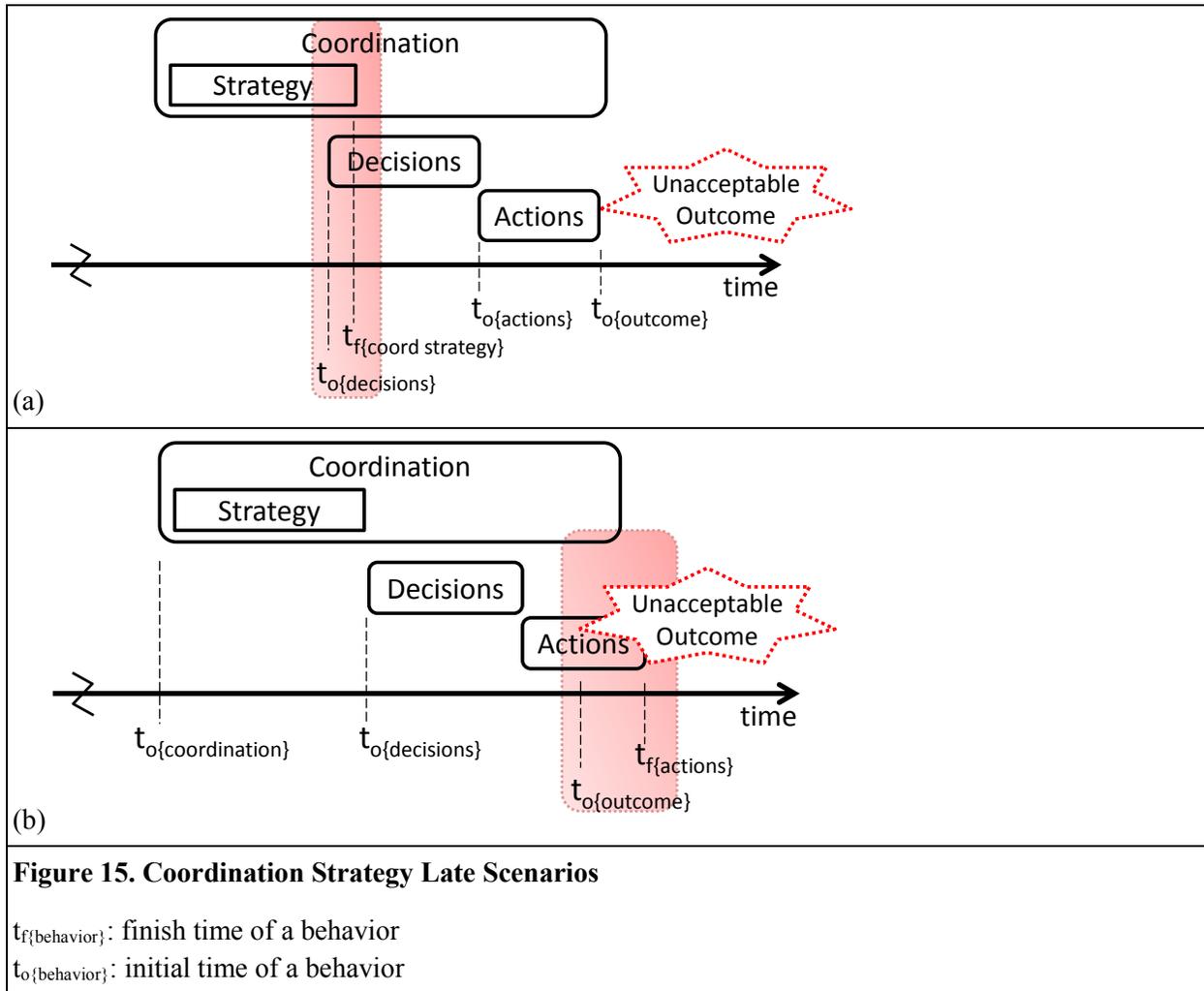
The concern from an external coordination perspective is when an unacceptable outcome is anticipated at $t_{o\{\text{outcome}\}}$, such as a hazardous outcome. The implication in evaluating coordination is that $t_{o\{\text{decisions}\}}$ may be a temporal constraint on when the coordination strategy must be established; otherwise, decision systems may be acting independently when under interdependent conditions. The temporal constraint leads to axiom [3.3].

[3.3] When required to influence an outcome by time $t_{o\{\text{outcome}\}}$, the coordination strategy established time $t_{f\{\text{coordination strategy}\}}$ shall be no later than the required individual decision time $t_{o\{\text{decision}\}}$.

Figure 15 depicts two scenarios related to a coordination strategy established too late to be an influence on unacceptable outcomes.

One coordination strategy late scenario occurs when the strategy is developed after when it is needed by individual decision systems to influence the outcome, shown in Figure 15(a). Decision systems in such scenarios act independently, which may lead to unacceptable outcomes. The other coordination strategy late scenario is when individual decision systems wait for the coordination strategy, as depicted in Figure 15(b), perhaps because decision systems are unaware of an impending unacceptable outcome. Waiting for

the coordination strategy can cause physical process actions to be too late to influence the unacceptable outcome.



While the coordination strategy can be developed too late to influence an outcome, there is competing concern with it being developed too early due to uncertainty in system dynamics and the environment as (Okhuysen & Bechky 2009) suggest: "...coordination is under persistent attack by the regular dynamics of organizations"(p. 494). As the time difference $\Delta t_{\{\text{coordination strategy}\}}$ grows larger, the coordination goals and strategy may be rendered obsolete by internal and external system changes. A coordination strategy may require updates to remain relevant.

Adequate time shall be allotted for coordination behavior to develop a coordination strategy before it is needed to avoid a hazardous scenario involving interdependent decision systems. Analysis of coordination should evaluate temporal constraints on development of a coordination strategy.

3.4.5 Coordination Perspectives for Analysis Summary

The evaluation of coordination can be framed using internal and external perspectives as described in this section. Coordination behavior should include the necessary coordination elements, have a strategy that leads to acceptable outcomes, and needs to develop a coordination strategy in time to avoid unacceptable outcomes. In the following chapters, the internal and external coordination evaluation perspectives are operationalized for use in hazard and accident analysis, extending STPA and CAST respectively.

3.5 Summary, a Coordination Framework

This chapter introduced a coordination framework to provide explanatory power for the observation and analysis of coordination behavior observed in sociotechnical systems. The coordination framework consists of four primary concepts.

First, a decision system was introduced as a basic unit of analysis to relate coordination behavior with decision and action behaviors observed in sociotechnical systems. The decision system functional model provides explanatory power for within and between decision system coordination, and vertical and lateral decision system coordination.

Second, coordination behavior was decomposed into elements as inspired by the reviewed organizational and coordination theory literature. Coordination behavior consists of three categories to include basic coordination components, coordination processes, and enabling conditions. The categories are further refined into nine coordination elements that expand the definition of coordination put forth in this thesis.

Third, a set of fundamental coordination relationships was derived. There are four fundamental coordination relationships when taking into account vertical or horizontal coordination, within and between decision system coordination, and coordination of a single process or multiple independent processes. These four coordination relationships can provide the conceptual representations for analysis of coordination in sociotechnical systems.

Last, internal and external perspectives on coordination behavior were introduced as a means to evaluate coordination against acceptable outcomes. For the goal of system safety, acceptable outcomes are those that do not lead to hazardous conditions. The internal perspective provides a means to evaluate whether coordination has the necessary components, processes and enabling conditions to achieve the system goals (requirements). The external perspective provides a means to evaluate the coordination strategy output relative to the outcome. Evaluation using the external perspective addresses the coordination output with and without the environment, and also potential temporal constraints on the coordination strategy.

The coordination framework is operationalized for analysis of coordination for safety in the following chapters, extending STPA and CAST.

4 EXTENDING STPA for COORDINATION

This chapter introduces STPA-Coordination, an STPA extension with additional steps to address coordination behavior within and between decision systems. STPA-Coordination uses flawed coordination guidance described in the chapter to identify coordination scenarios that may lead to unsafe control actions (i.e. hazards). After introducing STPA-Coordination and flawed coordination guidance, STPA-Coordination is applied to the set of fundamental coordination relationships derived in the coordination framework to demonstrate how to use the flawed coordination guidance in a theoretical sense; Chapter 5 applies STPA-Coordination to a real-world problem.

4.1 STPA-Coordination

STPA is a systems-theoretic hazard analysis technique. To simplify the description of the process used, it can be broken into two steps although that is not required. The two steps are shown in the first column Table 11, labeled Current STPA. The first step identifies control actions that can lead to hazards, or unsafe control actions. The second step identifies scenarios that can lead to the unsafe control actions and uses the control theoretic feedback model to guide causal analysis of the relationship between controllers and controlled processes.

While, theoretically, STPA identifies coordination and temporal degradation of controls as potential area for causal analysis, there is no guidance for how to identify coordination problems leading to unsafe control. Extended STPA is shown in the right column of Table 11, with STPA-Coordination in bold (right column, under STPA Step 2).

Table 11. Extended STPA

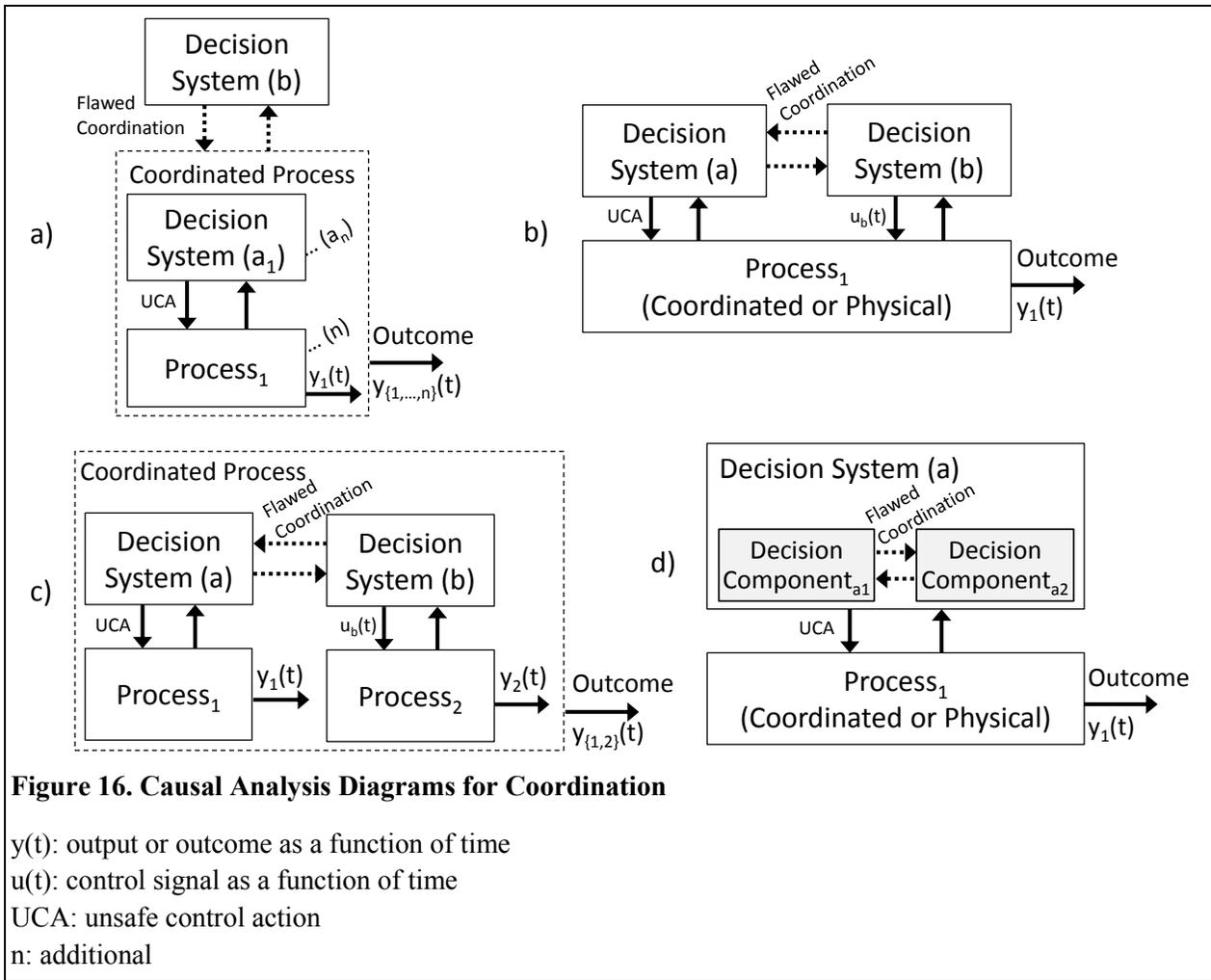
Current STPA (Leveson 2012)	Extended STPA
STPA Step 1. Identify unsafe control actions related to a single controller.	<ul style="list-style-type: none"> • Identify unsafe control actions related to a single decision system. • Identify additional unsafe control actions when there are multiple decision systems controlling the same process.
STPA Step 2. Identify hazardous scenarios that can lead to unsafe control actions: <ol style="list-style-type: none"> a) Examine the control loop. b) For multiple controllers of the same process, identify conflicts and potential coordination problems. c) Consider control degradation over time. 	STPA Step 2. Identify hazardous scenarios that can lead to unsafe control actions: <ol style="list-style-type: none"> a) Examine the control loop. b) STPA-Coordination. For processes with multiple controllers or coordinated decision making: <ol style="list-style-type: none"> i) Identify the interdependency. ii) Identify the fundamental coordination relationship. iii) Examine the four flawed coordination cases. c) Consider control degradation over time.

STPA-Coordination extends STPA with three additional steps to handle within and between decision system coordination in identifying scenarios that can lead to UCAs. The additional steps are described in Table 12.

Table 12. STPA-Coordination

STPA-Coordination	Description
i. Identify the interdependency	This step identifies a property necessary for coordination. In other words, there must be interdependency within or between decision systems for STPA-Coordination to be applicable. Identifying the interdependency may assist understanding of where and when coordination should exist.
ii. Identify the fundamental coordination relationship	Identify the fundamental coordination relationship to be analyzed. Depending on when in a system lifecycle STPA-Coordination is conducted, this step identifies the relationships that do or should exist to address the interdependency identified in the previous step. Identification of the relationship provides context for analysis. Analysis guidance related to the fundamental coordination relationships is described in section 4.4 below.
iii. Examine the four flawed coordination cases	Identify coordination scenarios that can lead to unsafe control using flawed coordination guidance. Flawed coordination guidance consists of four flawed coordination cases, each case refined by the applicable coordination elements. Flawed coordination guidance is described in sections 4.2 (flawed coordination cases) and 4.3 below (cases refined by coordination elements).

Figure 16 shows the fundamental coordination relationships labeled for STPA hazard analysis. The unsafe control action “UCA” originates from Decision System (a). The “flawed coordination” label identifies the interaction where STPA-Coordination applies.



The following sections introduce analysis guidance for use in identifying flawed coordination scenarios that can lead to UCAs.

4.2 Identifying UCAs from Flawed Coordination Cases

The question for STPA-Coordination to address is how can coordination lead to unsafe control actions (i.e. hazards)? The coordination framework is operationalized for STPA-Coordination with a set of four unique **flawed coordination cases** to guide unsafe control action causal analysis. The flawed coordination cases are unique based on two factors: 1) whether a coordination strategy exists or not, and 2) the internal or external perspective on coordination problem as defined in the coordination framework. The factors addressed by the flawed coordination cases are shown in the following 2 x 2 matrix, Table 13.

Table 13. Unique Flawed Coordination Cases

	Coordination Perspective: Internal	Coordination Perspective: External
Coordination Strategy: None	Case 1	Case 4
Coordination Strategy: Exists	Case 2	Case 3

The flawed coordination cases are identified in Figure 17, which represents the coordination problem introduced in the coordination framework.

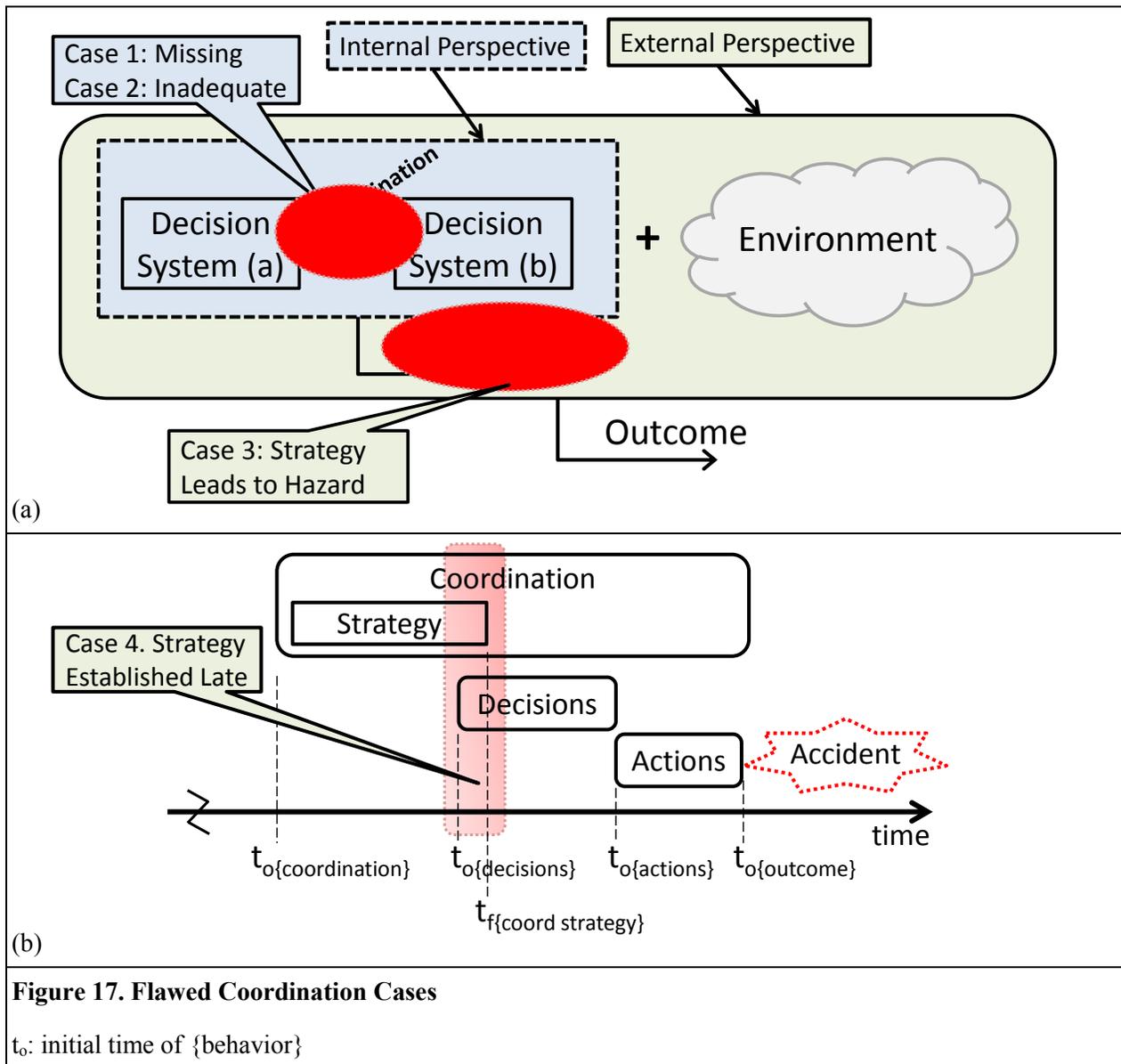


Table 14 describes each flawed coordination case, which STPA-Coordination uses to identify hazardous coordination scenarios that can lead to UCAs.

Table 14. Flawed Coordination Cases

	Flawed Coord Cases	Flawed Coordination Cases Description
Internal Coordination Perspective	1. Coordination Missing Leads to UCAs	<p>Flawed coordination cases #1-2 describe the coordination interaction itself within or between decision systems, shown in Figure 17(a). The cases are derived from the internal evaluation perspective in the coordination framework.</p> <p>Case 1 occurs when there is no coordination to address interdependent conditions and there should be. In particular, there is not a coordination strategy or group DM efforts to establish a coordination strategy. Causal analysis using case 1 identifies where coordination is missing and how this may lead to unsafe control actions.</p>
	2. Coordination Inadequate Leads to UCAs	<p>Case 2 occurs when there is at minimum a coordination strategy, but one or more of the coordination elements are missing or inadequate. Causal analysis using case 2 identifies how missing or inadequate coordination elements may lead to unsafe control actions.</p>
External Coordination Perspective	3. Coordination Strategy Leads to UCAs	<p>Flawed coordination cases #3-4 are represented in Figure 17(a) and (b). The cases address the coordination strategy and are derived from the external evaluation perspective in the coordination framework.</p> <p>Case 3 occurs when the coordination strategy includes actions that directly lead to unsafe control actions. There are at least two scenarios where the coordination strategy can lead to hazards. First, the coordination strategy dictates decision system actions that lead to hazardous outcomes. For example, a coordination strategy may put two physical processes (e.g. aircraft) in the same space at the same time to cause a collision. A coordination strategy may also put a physical process into a hazardous state relative to the environment, such as having aircraft maneuver towards the ground. Second, the coordination strategy may be infeasible and lead to hazards. Causal analysis using case 3 identifies how the coordination strategy may directly lead to unsafe control actions.</p>
	4. Coordination Strategy Established Late Leads to UCAs	<p>Case 4 occurs when a coordination strategy is developed too late to influence an unsafe outcome. The decision-making hierarchy must establish a coordination strategy in time for the physical layer decision systems to make appropriate decisions and take the proper actions in accordance with a coordination strategy. The temporal constraints on an unsafe scenario should be known, including constraints from the environment, controlled processes, and decision systems. Causal analysis using case 4 identifies how a coordination strategy is developed too late, which may lead to unsafe control actions.</p>

STPA causal analysis now has four flawed coordination cases that can guide identification of coordination scenarios that may lead to unsafe control actions (i.e. hazards). For example, how does inadequate coordination (flawed coordination case 2) lead to a control action not provided? Additional guidance is possible using the coordination elements derived in the coordination framework.

4.3 Flawed Coordination Guidance Using Coordination Elements

STPA step 2 causal analysis guidance using the four flawed coordination cases can be further refined using the nine coordination elements introduced in the coordination framework, which provides additional insights into identifying hazardous coordination scenarios that can lead to UCAs. Table 15 is the flawed coordination causal analysis matrix identifying (by dots) the case and element combinations to be assessed for leading to unsafe control actions; not all elements apply to each flawed coordination case as shown. What makes a coordination element inadequate is different based on the flawed coordination case perspective being analyzed.

Table 15. Flawed Coordination Causal Analysis Matrix

		Flawed Coordination Cases Lead to UCAs			
		1	2	3	4
Coordination Elements: Missing or Inadequate	1. Coordination Goals	•	•		•
	2. Coordination Strategy	•	•	•	•
	3. Decision Systems		•		•
	4. Communications		•		•
	5. Group Decision-Making	•	•		•
	6. Observation of Common Objects		•		•
	7. Authority, Responsibility, Accountability		•		•
	8. Common Understanding		•		•
	9. Predictability		•		•

Flawed coordination case 1 is coordination is missing. The coordination elements that apply to this case are: (1) coordination goals, (2) the coordination strategy, and (5) group decision-making. There is neither a coordination strategy nor efforts (group decision-making) to establish a strategy; that is, there is no intent to coordinate. In this case, missing coordination efforts can lead to unsafe control actions identified in STPA step one.

Flawed coordination case 2 is inadequate coordination when there is a coordination strategy. All the coordination elements apply to this case, which may be missing or inadequate, and should be evaluated.

Hazard analysis should identify scenarios where coordination elements are missing or inadequate, which can lead to unsafe control actions.

Flawed coordination case 3 is the coordination strategy leads to unsafe control actions. The coordination strategy (element 2) applies to this case in identifying when the strategy directly leads to unsafe control. The strategy can dictate unsafe control actions relative to other decisions systems and the environment. The strategy can also dictate infeasible actions for one or more decision systems that lead to hazardous control.

Flawed coordination case 4 is when the coordination strategy is established too late to influence an outcome. All coordination elements apply to this case as well. The focus is to identify scenarios involving the coordination elements where the coordination strategy may be established late, which leads to UCAs.

Table 16 provides detailed **flawed coordination guidance** for each flawed coordination case and applicable coordination element combination identified in Table 15; guidewords and guide phrases are used. For example, observation update rates on each decision system (coordination element 7, authority, responsibility, accountability) are inadequate (i.e. flawed coordination case 2), which can lead to a decision system not providing a control action when required for safety. The coordination element numbers reflect the numbers established in the coordination framework.

See APPENDIX A. Flawed Coordination Guidance and Examples for further discussion corresponding to Table 16 guidewords and phrases.

Table 16. Flawed Coordination Guidance for Unsafe Control Action Causal Analysis

<p>Flawed Coordination Case 1. Coordination Missing (coordination strategy missing)</p> <ul style="list-style-type: none"> • Coordination Basic Components <ol style="list-style-type: none"> 1. Coordination Goals: Missing 2. Coordination Strategy: Missing • Coordination Enabling Processes <ol style="list-style-type: none"> 5. Group Decision-Making: Missing
<p>Flawed Coordination Case 2. Coordination Inadequate (coordination strategy exists)</p> <ul style="list-style-type: none"> • Coordination Basic Components <ol style="list-style-type: none"> 1. Coordination Goals: Inadequate <ul style="list-style-type: none"> ○ Do not prioritize safety ○ Inconsistent: aware (internal motivations or external incentives) or unaware ○ Divergent from safety goals 2. Coordination Strategy: Inadequate <ul style="list-style-type: none"> ○ Ambiguous or missing: <ul style="list-style-type: none"> • Bounds of acceptable or desired actions (i.e. safe envelope) • Actions • Temporal constraints: begin/end times, duration, sequence, simultaneity ○ Flexibility vs standardization: inadequate for dynamic system or environment ○ Alternative coordination strategies:

Table 16. Flawed Coordination Guidance for Unsafe Control Action Causal Analysis

<ul style="list-style-type: none"> <ul style="list-style-type: none"> • Exist but unknown • Known but incompatible 3. Decision Systems: Missing or inadequate <ul style="list-style-type: none"> ○ Required experts ○ Human abilities and automation specifications ○ Human training • Coordination Enabling Processes <ul style="list-style-type: none"> 4. Communications: Missing or inadequate <ul style="list-style-type: none"> ○ Communication channels (channel capacity, bandwidth, noise, etc.) ○ Communication language and send/receive protocols (incompatible) 5. Group Decision-Making: Inadequate <ul style="list-style-type: none"> ○ Physical or virtual environments ○ Protocols ○ Value functions ○ Problem solving framework 6. Observation of Common Objects: Missing or inadequate <ul style="list-style-type: none"> ○ Observing different objects (asynchronous observations, different sensors) ○ Inadequate: resolution, delays, update rates, etc. • Coordination Enabling Conditions <ul style="list-style-type: none"> 7. Authority, Responsibility, Accountability (ARA): Missing or inadequate <ul style="list-style-type: none"> ○ Authority and Responsibility: not assigned, ambiguous ○ Accountability: <ul style="list-style-type: none"> • Confirmation of receipt, agreement, compliance, and completion of coordination strategy • Observation of decision systems • Observation rates • Confidence in other decision systems • Time constraints not established or monitored • Decision systems/components not coordinable by design or by organizational structure 8. Common Understanding: Missing or inadequate <ul style="list-style-type: none"> ○ Local and system states (absolute and relative), including decision systems ○ Models (local, holistic) ○ Process modes ○ Reference frames (e.g. geo-physical and time reference frames) ○ Coordination strategy 9. Predictability: Missing or inadequate <ul style="list-style-type: none"> ○ Models ○ Task familiarity ○ Time constraints
Flawed Coordination Case 3. Coordination Strategy Leads to Unsafe Control Actions

Table 16. Flawed Coordination Guidance for Unsafe Control Action Causal Analysis

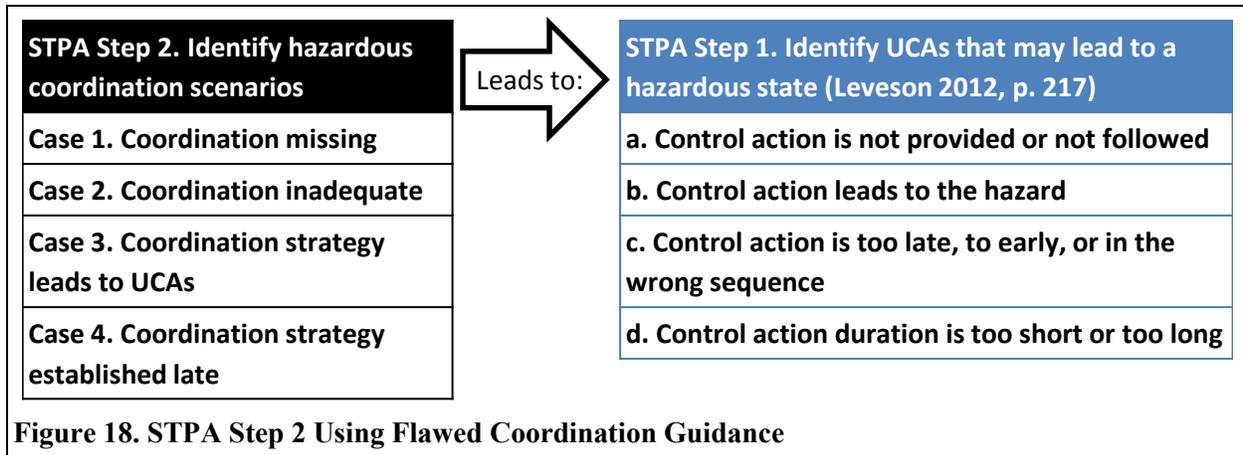
<ul style="list-style-type: none"> • Coordination Basic Components <ul style="list-style-type: none"> 2. Coordination Strategy: Infeasible or unacceptable <ul style="list-style-type: none"> ○ Development of strategy: Missing or inadequate <ul style="list-style-type: none"> • Inputs: process, environment, decision systems • Temporal constraints: timing duration, sequence, simultaneity • System/process models • Strategy evaluation methods ○ Maintenance of strategy: Missing or inadequate strategy update rates
<p>Flawed Coordination Case 4. Coordination Strategy Established Late</p> <ul style="list-style-type: none"> • Coordination Basic Components <ul style="list-style-type: none"> 1. Coordination Goals: established late 2. Coordination Strategy: established late 3. Decision Systems: missing, inadequate, established late • Coordination Enabling Processes <ul style="list-style-type: none"> 4. Communications: Delayed or take too much time <ul style="list-style-type: none"> ▪ Data transfer rates ▪ Protocols 5. Group Decision-Making: <ul style="list-style-type: none"> ▪ Protocols: take too much time ▪ Time constraints: unknown, incorrect 6. Observation of Common Objects: Missing or inadequate lead to strategy established late <ul style="list-style-type: none"> ▪ Asynchronous observations ▪ Observation update frequency too low ▪ Observation duration takes too much time • Coordination Enabling Conditions <ul style="list-style-type: none"> 7. Authority, Responsibility, Accountability: established late <ul style="list-style-type: none"> ▪ Authority and Responsibility: not assigned, ambiguous ▪ Accountability: time constraints missing, not monitored 8. Common Understanding: established late 9. Predictability: Missing or inadequate <ul style="list-style-type: none"> ▪ Dynamic models ▪ Time constraints

Table 16 flawed coordination guidance is recommended for identifying unsafe control action causation due to coordination within and between decision systems. However, the flawed coordination guidance is not prescriptive. The guidance is but one way to approach the coordination problem for hazard analysis, which was derived from the coordination framework and through case study research (Chapters 5 and 6). Additional details beyond the flawed coordination guidance may be required for hazard analysis of a particular system.

4.4 Theoretical Application: Causal Analysis Using Flawed Coordination Guidance

This section applies the flawed coordination guidance to the set of fundamental coordination relationships. The application is an initial assessment of the utility in using the introduced coordination framework and flawed coordination guidance. The application also assists in understanding the coordination problems and the coordination context for each relationship that may lead to UCAs, but from a more theoretical perspective. Using flawed coordination guidance in practical applications is given in Chapter 5 with a hazard analysis case study and in Chapter 6 with an accident investigation case study.

4.4.1 Flawed Coordination Guidance Setup



STPA step one assesses four unsafe control action categories based on STAMP, which are listed in Figure 18. Flawed coordination guidance is then used to identify hazardous coordination scenarios that can lead to the UCAs (STPA step 2). The analysis relationship is shown in Figure 18 by the “leads to” arrow from step 2 to step 1. For example, flawed coordination guidance can identify how coordination missing (case 1) leads to control actions not provided (a) or control actions provided that lead to hazards (b).

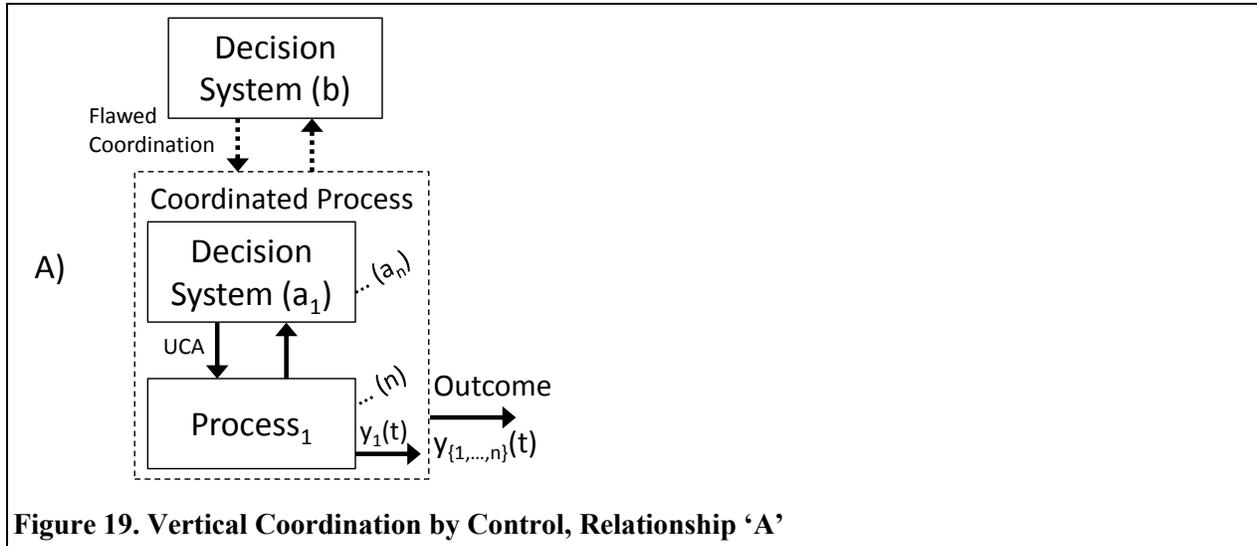
The rest of section 4.4 describes the application of flawed coordination cases to the four fundamental coordination relationships to identify unsafe controls. The discussion is a refinement of causal analysis guidance provided by Table 16 where it was considered unique; thus, not every case and element combination is discussed. The analysis symbols and nomenclature is provided in Table 17.

Table 17. Analysis Symbols and Nomenclature

η = set of acceptable outcomes, non-hazard state	\rightarrow = leads to
$y(t)$ = the output or outcome as a function of time	$\&$ = and
$u(t)$ = the control action as function of time	\sim = not

4.4.2 Causal Analysis Guidance for Vertical Coordination, Relationship ‘A’

Coordination relationship ‘A’ depicts a vertical interaction (or coordination by control) from Decision System (b) to one or more lower level Decision Systems (a_1, \dots, a_n) as shown in Figure 19. In Theory of Hierarchical, Multilevel Systems, (Mesarović et al. 1970) label vertical interactions as “conditioning” interactions and ask if there is “coordinability” between decision systems, which is the ability to influence lower level decision problems. An example of fundamental coordination relationship ‘A’ is air traffic control and aircrew subject to their control.



The flawed coordination causal analysis identifies how the vertical coordination with Decision System (b) may lead to Decision System (a) unsafe control actions. It is noted that the interaction between Decision System (a) and Process (1) may also be vertical coordination when Process (1) is a decision system. In such scenarios, use of flawed coordination guidance may be applied in addition to the control loop causal analysis guidance typical of STPA step two.

Flawed Coordination Case 1. Coordination Missing

In this case, the basis for vertical coordination is missing, notably the coordination goal and strategy elements with no other group decision-making efforts present. Decision System (a_1) UCAs can result when vertical coordination is missing.

Vertical coordination may be missing in novel and developing systems, such as emergency response systems and multi-national military campaigns. The presence of hierarchy also does not mean coordination exists. Hierarchical decision system (b) may not provide a coordination strategy for decision systems (a_1) through (a_n) to follow. An example could be when ATC does not provide a collision avoidance strategy for aircrew to follow because their radar system went down, which leads to aircrew not maneuvering to avoid collisions. Another example is if the standards for a new environment are not yet established, such as rules of engagement for wartime operations. Missile defense Army systems may

not have rules of engagement standards (i.e. a coordination strategy) with friendly aircraft, which could lead to missile system operators shooting down a friendly aircraft.

Flawed Coordination Case 2. Coordination Inadequate (coordination strategy established)

When Decision System (a) depends on higher-level coordination for guidance, inadequate coordination may lead to UCAs. Case 2 implies a vertical coordination strategy exists and one or more coordination elements are missing or inadequate. Table 18 describes select scenarios for flawed case 2 vertical coordination that can lead to UCAs.

Table 18. Causal Analysis Guidance, Fundamental Coordination Relationship A, Case 2

Coordination Elements	Causal Analysis Scenarios and Discussion
6. Observation of Common Object	<ul style="list-style-type: none"> • A lower level decision system may not follow a higher-level coordination strategy because they are not observing common objects. • Observation of common objects may not be possible in the vertical coordination sense, nor may it be desired in some scenarios. ATC for example may observe additional objects with radar than observed by aircrew. If inadequate observation is known and accepted, additional information and communication may be required to ensure common understanding between hierarchical decision systems.
7. Authority, Responsibility, Accountability	<ul style="list-style-type: none"> • Roles and responsibilities in the vertical sense should be established by the hierarchical structure. Analysis should seek scenarios where vertical coordination responsibility may be ambiguous. • Accountability is a two-way interaction, not simply a feedback control loop where the lower level decision system executes without consideration. Any hierarchical level n+1 should have confirmation that coordination goals, strategy, and needed coordination information were received by level n. Inadequate accountability may decrease confidence to the vertical coordination interaction for both decision system levels and lead to UCAs. • Coordinability in the vertical dimension is important. For humans, coordinability is the ability to influence through incentives, whether positive or negative, and from individual motivations. For decision automation, one is concerned if the decision-making hierarchy can influence its decisions. Inadequate coordinability can lead to UCAs

Flawed Coordination Case 3. Coordination Strategy Leads to Hazard

In flawed coordination case 3, Decision System (b) derives a strategy that leads to a hazard, which is similar to STPA step 1 unsafe control actions. The coordination strategy must be safe for Decision System (a₁) through (a_n) relative to themselves, such as aircraft cannot collide into each other. The strategy must also ensure that it does not violate environmental constraints, such as ATC directing aircraft into the ground.

The existence of alternative coordination strategies may cause hazardous scenarios when Decision Systems (a₁) through (a_n) are not following Decision System (b) or when the vertical coordination strategy is incompatible with the alternative. An example is ATC may be unaware that one or more of the aircrew are following TCAS suggested maneuvers and issue instructions that conflict with TCAS.

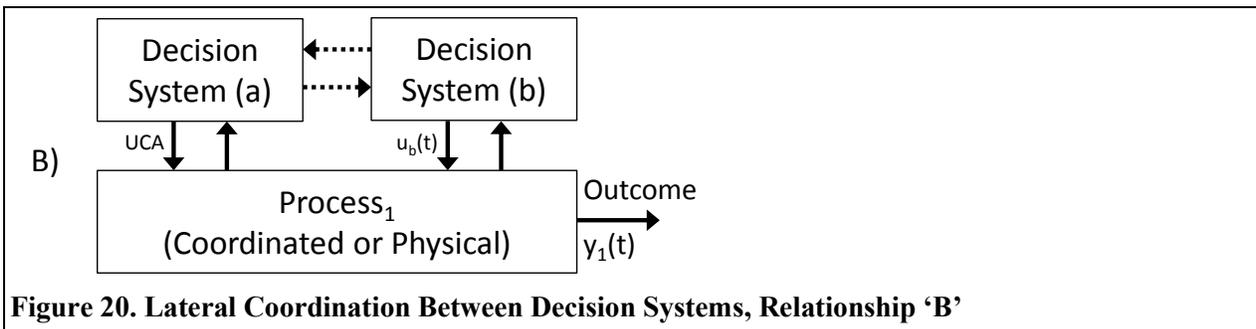
Decision System (b) strategy may not be feasible for those involved in its coordination strategy. For example, ATC may ask a UAS to maneuver within certain constraints, but the UAS does not have the performance to do so.

Flawed Coordination Case 4. Coordination Strategy Established Late

The guidance for this case is similar to flawed coordination guidance in Table 16.

4.4.3 Causal Analysis Guidance for Lateral Coordination, Relationship ‘B’

Relationship ‘B’ represents coordination of control actions on a single process, shown in Figure 20. An unsafe control action may occur when the control actions on Process₁ are not in coordination. Two aircrew with independent flight controls to the same aircraft is an example of fundamental coordination relationship ‘B’. The hazardous scenarios discussion for relationship ‘B’ focuses on 1) the transfer of process control and 2) parallel control actions on the process.



Decision systems should coordinate their control actions in Relationship ‘B’. The coordination action strategy and coordination elements related to enabling conditions are unique coordination challenges in Relationship B. Depending on context the control signal can be classified as a discrete or continuous signal in the metaphorical or engineering sense. For example, a discrete signal could be a mode change on automation or button press to release a missile, and a continuous signal can apply to flying an aircraft or driving a car. An overview of control signals is given in Table 19 to clarify concepts discussed in this section.

Table 19. Discrete vs. Continuous Control Action Descriptions

	Discrete Signal	Continuous Signal
Visualization		
Begin Time	n	t_0
Rise/Decay Rate	--	t_0 to t_1 ; t_2 to t_f
Amplitude	$x[n]$	$x(t)$
Duration of Signal	--	t_1 to t_2
End Time	--	t_f

Flawed Coordination Case 1. Coordination Missing

The guidance for this case is similar to flawed coordination guidance in Table 16.

Flawed Coordination Case 2. Coordination Inadequate (coordination strategy established)

Table 20 refines the inadequate coordination causal analysis guidance for fundamental coordination relationship ‘B’. The identified scenarios can lead to unsafe control actions.

Table 20. Causal Analysis Guidance, Fundamental Coordination Relationship ‘B’, Case 2

Coordination Elements	Discrete Signal, Causal Analysis	Continuous Signal, Causal Analysis
2. Coordination Strategy	Inadequate when it does not address the coordination problem of shared control actions on the same process.	
7. Authority, Responsibility, Accountability	<ul style="list-style-type: none"> Inadequate transfer of action responsibility, such as not assigned or ambiguous. An example is two people believe the other is responsible for a safety critical task such as removing a safety pin. However, nobody removes the safety pin and it leads to a hazardous scenario. Inadequate allocation of responsibility: Given set of needed control actions $\{u_1$ 	<ul style="list-style-type: none"> Inadequate transfer in neutral state: responsibility not assigned or ambiguous. An example neutral state is the F-16 Viper is trimmed by default to 1-g flight. In the neutral state, transfer of aircraft control may not be known since the aircraft is not reacting to an active control signal. Inadequate transfer in active state: observation of other decision system,

	<p>... u_n}, the summation of Decision System (a) and (b) control actions $u_a + u_b \neq \{u_1 \dots u_n\}$. An example is when launching an F-16 fighter aircraft, the pilot and crew chief are responsible for certain actions on the F-16 needed for safety of flight. If the actions are not all accomplished, hazardous outcomes may result.</p>	<p>update rates, confidence in other decision system information may lead to hazardous scenarios. As an example, when flying an F-16 two-seat model during a test maneuver or critical flight phase a transfer of aircraft control may lead to UCAs when inadequate. Control signal step functions and control signal coupling should be analyzed.</p>
8. Common Understanding	<p>The status of control actions are not given or not understood. In such scenarios, decision systems may not know when to interact with the process.</p>	
9. Predictability	<p>Inadequate model of $u_a(t) \& u_b(t) \rightarrow y_1(t) \rightarrow \eta$</p>	
	<p>Time constraints unknown leading to discrete signal too early/too late by one of the decision systems. A hypothetical example is a plant operator must wait 30 minutes after maintenance actions to start a process. However, the plant operator is either unaware of the time constraint or unaware of the elapsed time elapsed and begins the process, which may lead to a hazardous scenario.</p>	<p>Time constraints may not be known for continuous signal, leading to a signal being too long/too short or too early/too late. A hypothetical example could be autonomous cars need to transfer control to exit a freeway. However, the driver is not aware of the transition (i.e. too late) or the automation does not disengage control (too long) causing an interaction concern.</p>

Flawed Coordination Case 3. Coordination Strategy Leads to Hazard

A coordination strategy between Decision Systems (a) and (b) may directly lead to UCAs. Flawed coordination case 3 for relationship ‘B’ is similar to STPA step 1 analysis. Table 21 summarizes how a coordination strategy may lead to UCAs in the context of lateral coordination for the same process.

Table 21. Causal Analysis Guidance, Fundamental Coordination Relationship ‘B’, Case 3

Coordination Elements	Discrete Signal	Continuous Signal
2. Strategy	<p>Inadequate transfer of control or parallel signals: $u_a(t) \& u_b(t) \rightarrow y_1(t) \rightarrow \sim\eta$.</p> <ul style="list-style-type: none"> • Amplitude too high or too low. • Too early, too late, or in wrong sequence. 	<p>Inadequate transfer of control or parallel signals: $u_a(t) \& u_b(t) \rightarrow y_1(t) \rightarrow \sim\eta$.</p> <ul style="list-style-type: none"> • Amplitude too high or too low. • Onset or decay rate is too quick or too slow. • Too early or too late. • Too long or too short.

Flawed Coordination Case 4. Coordination Strategy Established Late

The guidance for this case is similar to flawed coordination guidance in Table 16.

4.4.4 Causal Analysis Guidance for Lateral Coordination, Relationship ‘C’

Relationship ‘C’ is coordination to achieve a safe coordinated outcome $y_{\{1,2\}}(t)$ from independent process outputs $y_1(t)$ and $y_2(t)$, shown in Figure 21. An unsafe control action of Decision System (a) may occur when lateral coordination between Decision System (b) is flawed. An example of relationship ‘C’ is a Patriot missile system and friendly aircraft each controlled by humans, where the safe outcome is no launched missiles on friendly aircraft.

It is necessary to address the coordination of the independent process outputs $y_1(t)$ and $y_2(t)$ in coordination causal analysis.

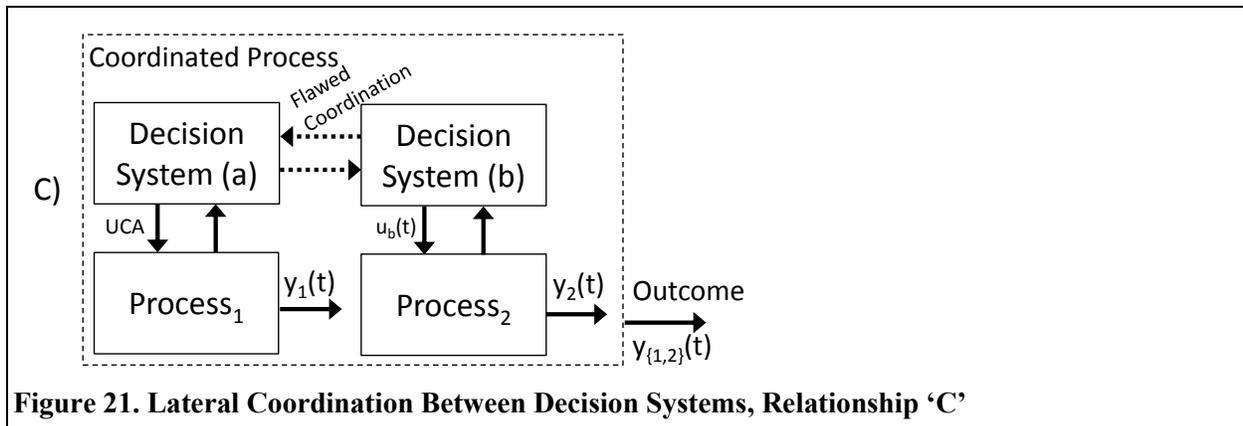


Figure 21. Lateral Coordination Between Decision Systems, Relationship ‘C’

Flawed Coordination Case 1. Coordination Missing

The guidance for this case is similar to flawed coordination guidance in Table 16.

Flawed Coordination Case 2. Coordination Inadequate (coordination strategy established)

Table 22 refines the inadequate coordination causal analysis guidance for relationship ‘C’.

Table 22. Causal Analysis Guidance, Fundamental Coordination Relationship C, Case 2

Coordination Elements	Causal Analysis Scenarios and Discussion
2. Coordination Strategy	Inadequate when the coordination strategy does not address process output interdependency.
7. Authority, Responsibility, Accountability	Accountability may be inadequate in the observation of and confidence in other decision systems to achieve expected process outputs. For example, there may be inadequate observation of a flight of F-16s to accomplish a

	coordinated task of neutralizing enemy ground fire to allow ground troops to continue an operation. The F-16s may have effectively neutralized the enemy fire, but inadequate accountability leads the ground troops to not continue operations, which may lead to unsafe control actions.
8. Common Understanding	Decision systems: unknown interdependency. An example is when aircraft unexpectedly enter protected airspace (e.g. military restricted areas) when military flights are ongoing. There is now interdependency that one or both aircraft are unaware, which can lead to hazardous actions.
9. Predictability	Inadequate model of $y_1(t) \& y_2(t) \rightarrow y_{\{1,2\}}(t) \rightarrow \eta$.

Flawed Coordination Case 3. Coordination Strategy Leads to Hazard

The problem formulation for relationship ‘C’ is $y_1(t) \& y_2(t) \rightarrow y_{\{1,2\}}(t) \rightarrow \sim\eta$.

Flawed Coordination Case 4. Coordination Strategy Established Late

The guidance for this case is similar to flawed coordination guidance in Table 16.

4.4.5 Causal Analysis Guidance for Within Decision System Coordination, Relationship ‘D’

Relationship ‘D’ is within decision system coordination, shown in Figure 22.

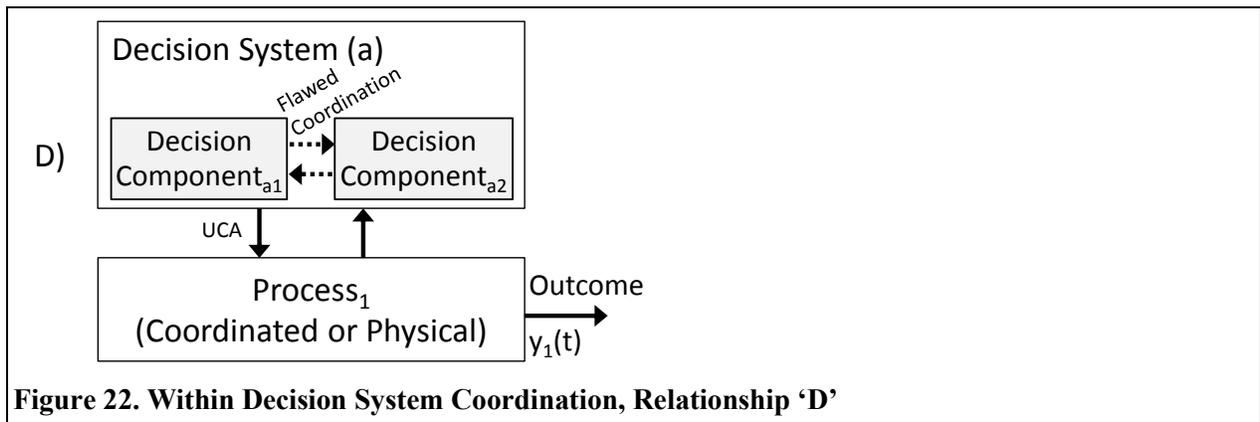


Figure 22. Within Decision System Coordination, Relationship ‘D’

In this abstraction, decision component coordination is concerned with Decision System (a)’s control action and Process₁ outcome. The conception is similar to the “controller” and feedback control loop model except that it is a functional representation for a common output. An example of within decision system coordination is unmanned aircraft and collision avoidance automation—known as the detect-and-avoid (DAA) system—that coordinate to produce a common signal output to a remote aircraft, such as a collision avoidance maneuver.

Flawed Coordination Case 1. Coordination Missing

The guidance for this case is similar to flawed coordination guidance in Table 16.

Flawed Coordination Case 2. Coordination Inadequate (coordination strategy established)

Table 23 refines the inadequate coordination causal analysis guidance for relationship ‘D’.

Table 23. Causal Analysis Guidance, Fundamental Coordination Relationship ‘D’, Case 2

Coordination Elements	Causal Analysis Scenarios and Discussion
7. Authority, Responsibility, Accountability	<ul style="list-style-type: none"> • Each component makes decisions. However, the decision authority and control actions responsibility may be inadequate, such as not assigned or ambiguous. For example, future concepts have the DAA maneuvering the UAS when needed which is relationship B where both have access to controls. There may be confusion when flying different UAS on whether the current DAA-equipped UAS will maneuver or not. • Confidence in component decisions may be inadequate. For example, decision automation that does not integrate first order information or that suggests actions that appear unsafe may be ignored. • Accountability may be inadequate when components are not coordinable. For example, the DAA may not be coordinable by the UAS pilot or other aircraft, which can lead to decisions that conflict with developing a coordination strategy. The UAS pilot may want to climb for collision avoidance but does not have a way to influence the DAA to check if a climb is an acceptable coordination strategy.
8. Common Understanding	<ul style="list-style-type: none"> • Common understanding may be inadequate when one or more components is unaware of an interdependency exists, especially if the component has final decision or control action responsibility. For example, the DAA may know of a potential collision but the UAS pilot does not. • Decision automation interactions with humans are a concern for Relationship ‘D’.
9. Predictability	Inadequate model of $u_a(t) \rightarrow y_1(t) \rightarrow \eta$

Flawed Coordination Case 3. Coordination Strategy Leads to Hazard

When an individual decision component makes unsafe decisions in relationship ‘D’, this may directly lead to unsafe control actions.

Flawed Coordination Case 4. Coordination Strategy Established Late

The guidance for this case is similar to flawed coordination guidance in Table 16.

4.5 Summary, Extending STPA for Coordination

STPA has limited guidance for multiple controller coordination interactions that can lead to unsafe control actions, until now. This chapter introduced STPA-Coordination, which extends STPA unsafe control action causal analysis guidance (step 2) to address flawed coordination. STPA-Coordination uses flawed coordination guidance derived from the coordination framework to identify coordination scenarios that can lead to unsafe control actions.

Flawed coordination guidance includes the use of four flawed coordination cases and set of nine coordination elements. Causal analysis using flawed coordination case 1 analyzes how missing coordination can lead to UCAs. Flawed coordination case 2 analyzes how inadequate coordination can lead to UCAs. Flawed coordination case 3 causal analysis identifies how the coordination strategy can directly lead to UCAs. Last, flawed coordination case 4 is used to identify how a coordination strategy can be established late, which may lead to UCAs. Table 16 provides guidewords and phrases for flawed coordination guidance.

STPA-Coordination enables causal analysis of within and between decision system coordination, and vertical and lateral coordination. As part of STPA, STPA-Coordination can be considered efficient because only hazardous coordination scenarios are identified. Extended STPA provides causal analysis guidance for an expanded set of sociotechnical system relationships using the flawed coordination analysis guidance in addition to the feedback control model guidance.

The chapter also provided an initial assessment of the coordination framework and STPA-Coordination in its theoretical application to the set of fundamental coordination relationships. To further assess validity of the coordination framework and analysis extensions, STPA-Coordination applied to a real-world case study is next.

[Page intentionally left blank]

5 STPA-COORDINATION CASE STUDY: UAS COLLISION AVOIDANCE

A significant safety challenge in aviation today is the integration of unmanned aircraft systems (UAS) into military and civilian flight operations. How can UAS maintain self-separation and avoid collisions with other aircraft? This safety concern is largely a coordination concern where UAS and other aircraft are interdependent on the shared airspace.

This Chapter presents a case study applying STPA-Coordination to analyze UAS integration and the collision avoidance safety problem. STPA-Coordination results and comparisons to a Functional Hazard Analysis (FHA), a requirements analysis, and to FAA-established

Safety Risk Management processes (Federal Aviation Administration 2014c) are included in the case study. The purpose of the case study is to demonstrate the utility of STPA-Coordination, and by association the coordination framework, to analyze and derive coordination related safety requirements for system design.

The case study was chosen for several reasons. First, UAS integration is a current significant challenge for involved stakeholders and the results may be useful for this problem. Second, UAS collision avoidance is largely a coordination problem of interdependent aircraft that share the same airspace. Last, there are published documents by RTCA Special Committee (SC) 203—a professional aviation standards-making US organization—containing official safety analysis and requirements results for comparison to STPA-Coordination (RTCA SC-203 2013a; RTCA SC-203 2013b).

5.1 Case Study Background

UAS are being integrated into military and civilian flight operations around the world. The FAA envisions “safe and seamless” integration of UAS in the NAS (National Airspace System) where flight operations co-exist with today’s manned aircraft without the need for accommodation (Federal Aviation Administration 2013a). Military UAS operations concepts include autonomous swarm UAS tactics and loyal wingman concepts where manned and unmanned aircraft coordinate to accomplish missions.

One of the key technology enablers for integration is the Detect-and-Avoid (DAA) system, or more generally a collision avoidance system (CAS). Efforts to integrate UAS into the NAS and efforts to develop DAA technology are in design phases. While the DAA system’s technical functions—detect, track, evaluate, prioritize, declare, determine action, command, execute (Federal Aviation Administration 2013b)—have been stable for some time, efforts to establish an accepted safety analysis on UAS and the DAA have been ongoing for over a decade through the sunset RTCA SC-203 and current SC-228. In



Figure 23. Unmanned Aircraft Systems Concept
Adapted from (DARPA 2016). Reprinted with permission.

addition, the initial SC-228 safety working group was disbanded in late 2015, with a new safety effort in infancy again.²

The events just discussed are not intended to marginalize the RTCA safety efforts, but to highlight the immense challenges in characterizing the safety of this sociotechnical system, which are using traditional safety analysis methods. Perhaps an alternative approach is needed; this case study demonstrates the use of one such alternative with extended STPA.

5.2 Systems Engineering Baseline

The safety engineering process is embedded within system engineering. Initial steps involve scoping and defining the system with objectives. For safety, these objectives are the system safety constraints derived from system accidents and hazards. Following is the system engineering baseline for analysis of UAS collision avoidance, with traceability of the system safety constraints back to the accident.

- Sociotechnical System: National Airspace System (NAS), enabling safe and efficient flight operations for airborne stakeholders.
- Goal of interest: Safe flight operations, freedom from accidents.
- Accidents (A) of interest:
 - A1. Mid-air collisions.
 - A2. Collisions with terrain and ground obstacles.
- System Hazards (H):
 - H1. Violation of aircraft minimum separation. (←A1)
 - H2. Controlled flight into terrain. (←A2)
 - H3. Lack of aircraft controlled flight. (←A1, A2)
- System Safety Constraints (SC): The SCs are derived from the hazards and represent high-level constraints on system operations. Further refinements may occur as the analysis proceeds top-down to the physical processes.
 - SC1. Flight operations shall not lead to loss of minimum separation requirements. (←H1)
 - SC2. Flight operations shall not induce or contribute to a controlled flight into terrain. (←H2)

² Author was involved in the Safety Working Group for RTCA SC-228 until it was disbanded late 2015.

- SC3. Flight operations shall not induce or contribute to lack of aircraft controlled flight. (←H3)

5.3 Safety Control Structure

The safety control structure represents the control and coordination relationships needed for safe system outcomes. For airspace safety and UAS collision avoidance, the safety control structure is shown in Figure 24. Only the control loops up to air traffic management are shown, including ATC, aircraft decision systems, and the aircraft physical process. The air traffic management decision system in the US is the Federal Aviation Administration, with Air Traffic Organization and Aviation Safety offices primarily responsible for developing rules and regulations related to flight and collision avoidance. The aircraft decision system of interest controls the UAS and is comprised of UAS pilots and the collision avoidance decision automation called the detect-and-avoid (DAA) system.

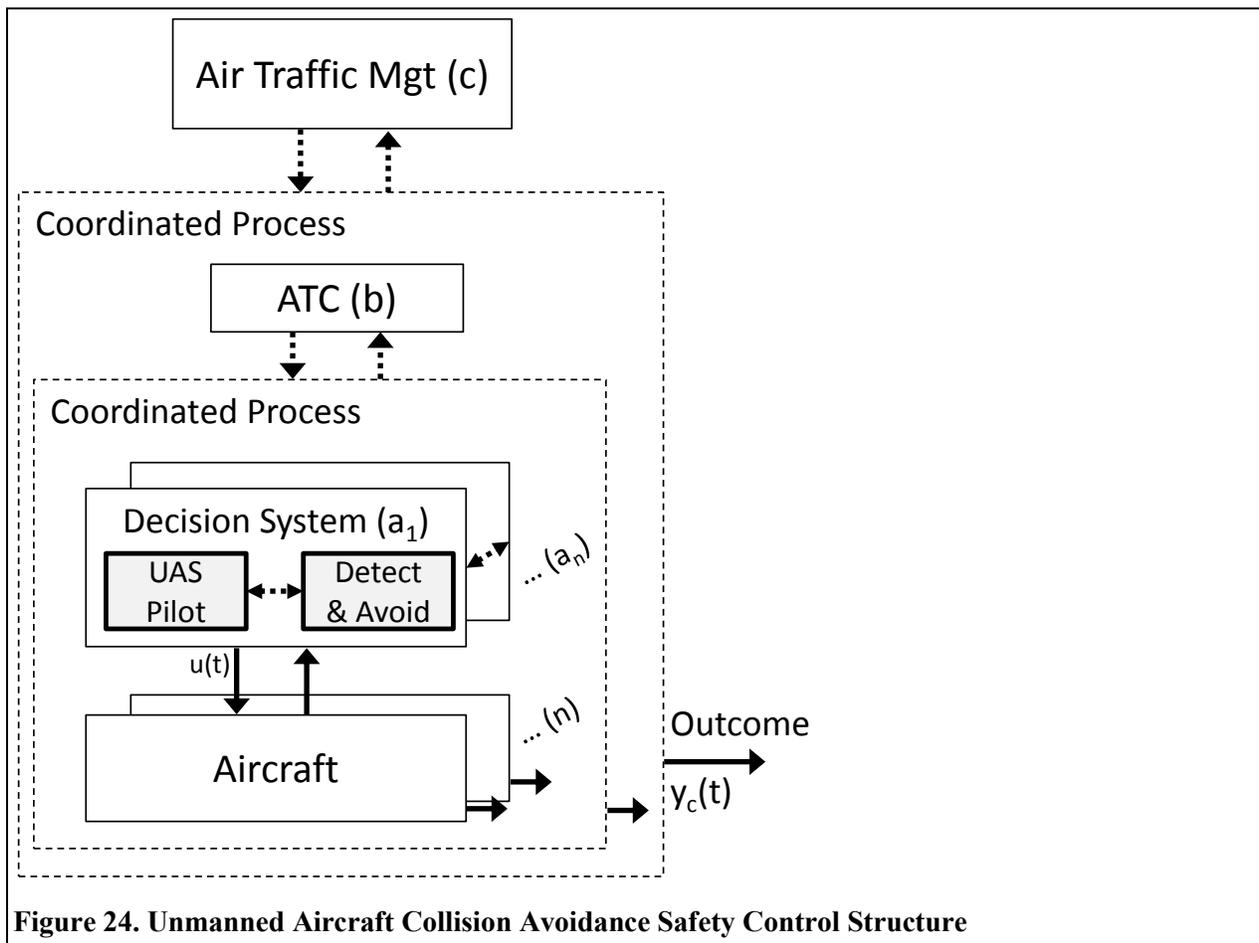


Figure 24. Unmanned Aircraft Collision Avoidance Safety Control Structure

Table 24 describes the roles and responsibilities of decision systems and associated decision components to be analyzed with STPA-Coordination.

Table 24. Decision System Roles and Responsibilities

Decision System	Role and Responsibility Related to Collision Avoidance
Air Traffic Control Decision System	The role of ATC is to implement airspace rules and regulations as a coordination authority over individual aircraft. ATC is responsible for the safe separation and efficiency of aircraft ground and flight operations under their control.
Unmanned Aircraft Decision System	The role of UAS decision system is to safely, comprehensively, and efficiently manage and fly the UAS in all ground and flight phases. The UAS decision system is responsible for avoiding ground and airborne obstacles, operating the UAS within higher-level safety constraints, and maneuvering the aircraft within safe and feasible limits.
	<i>Decision System Component: UAS Operator.</i>
	The role of UAS operators is to make decisions and control the aircraft. The UAS operator interacts with the DAA for collision avoidance and is responsible for selecting the DAA operating mode.
	<i>Decision System Component: Detect-and-Avoid (DAA) collision avoidance system.</i> The role of DAA is to determine when collision avoidance is a concern and provide maneuver guidance for the UAS operator. Its future authority and responsibility may enable automatic collision avoidance maneuvers when self-determined to be necessary (RTCA SC-228 2014). The DAA functional responsibilities include: detect, track, evaluate, prioritize, declare threat, determine action, command and execute maneuvers (Federal Aviation Administration 2013b).

5.4 STPA-Coordination for UAS Collision Avoidance

UAS are interdependent with ATC and other aircraft decision systems to ensure the shared airspace is collision free. With this interdependency is the need for coordination and the use of STPA-Coordination may benefit identification of hazardous scenarios. Further, STPA-Coordination recommendations address the coordination elements for each flawed coordination case, which if implemented may lead to safe coordination.

The case study uses the following assumptions for UAS flight operations in the NAS, which scope the STPA-Coordination analysis:

- UAS operations will be seamless, without special accommodations observed today with use of Certificates of Authorization and special airworthiness certificates.
- Current airspace designations (e.g. Classes A, B, C, etc.) and ATC separation services are used for integrated UAS flight operations.

- Part 91 Code of Federal Regulations §91.113 and 115 right-of-way and §91.181 course to be flown regulations are used for integrated UAS flight operations. The right-of-way rules give standardization for collision scenario maneuvers and the course to be flown rule allows UAS to maneuver for perceived “well clear” violations.
- The pilot has final maneuver decision responsibility being able to follow, reject, or modify the DAA maneuver guidance.
- There will be future capability for automatic collision avoidance maneuvers by DAA (RTCA SC-228 2014).
- The DAA provides suggestive horizontal and vertical maneuver bands to resolve DAA alerts (RTCA SC-228 n.d.).
- UAS can be “loyal wingman,” which is a future concept of UAS interacting with manned aircraft for coordinated flight operations (US Department of Defense 2013).

5.4.1 STPA Step 1, Unsafe Control Actions

Unsafe control actions were derived from the perspective of the UAS decision system with the goal of collision avoidance. One way to keep the analysis tractable was to treat the control action as a generic separation maneuver without further refinement into vertical, lateral, and energy changes, which are descriptors that can have nearly unlimited combinations. The separation maneuver implies any combination of geometry and timing options. The unsafe control actions are given in Table 25.

Table 25. Unsafe Control Actions, UAS Decision System

Unsafe Control Actions (UCA)	Unsafe Control Action Descriptions—UAS Decision System
UCA.1 Control required for safety is not provided	UCA1 UAS decision system fails to command separation maneuver when safe separation violation imminent. (←H1)
UCA.2 Providing control action causes hazard	UCA2.1 UAS decision system commands separation maneuver into the intruder aircraft when separation violation (believed) imminent. (←H1)
	UCA2.2 UAS decision system commands separation maneuver into additional aircraft when separation violation (believed) imminent. (←H1)
	UCA2.3 UAS decision system commands separation maneuver into terrain when separation violation (believed) imminent. (←H2)
	UCA2.4 UAS decision system commands separation maneuver that is in conflict with established controls, when separation violation (believed) imminent. (←H1)
	UCA2.5 UAS decision system commands separation maneuver beyond aircraft capability when separation violation (believed) imminent. (←H3)

Unsafe Control Actions (UCA)	Unsafe Control Action Descriptions—UAS Decision System
	UCA2.6 UAS decision system commands separation maneuver during critical flight phases (e.g. high workload, low safety margins, near terrain), when separation violation (believed) imminent. (←H2, H3)
	UCA2.7 UAS decision system commands separation maneuver that disrupts continuous control of remote aircraft, when separation violation (believed) imminent (←H1, H2, H3)
UCA.3 Provided at incorrect time (too early/late) or in wrong sequence	UCA3 UAS decision system commands separation maneuver too late for system response capabilities when separation violation imminent.
UCA.4 Provided for incorrect duration (too soon/long)	UCA4.1 UAS decision system stops maneuver too soon when required for safe separation. (←H1)
	UCA4.2 UAS decision system holds maneuver too long when required for safe separation, maneuvering into another aircraft’s safe separation zone or terrain obstacle. (←H1, H2)

5.4.2 STPA-Coordination for UCA Causal Analysis (Step 2)

STPA-Coordination is used for coordination-related causal analysis of UAS decision system unsafe control actions. The results of STPA control loop causal analysis are provided in APPENDIX B. RTCA SC-228 Draft STPA on UAS Integration Report, which was accomplished during 2014-2015 to support RTCA SC-228 Safety Working Group safety analysis efforts. STPA-Coordination steps consist of:

1. Identify the interdependency:
 - Shared goals. Accident free operations, collision avoidance.
 - Shared resources. Airspace for aircraft navigation.
2. Identify the coordination relationship:
 - Fundamental Coordination Relationships are shown in Figure 25.
3. Examine the flawed coordination cases to identify coordination scenarios that can lead to unsafe control actions.

The focus for STPA-Coordination in this case study is the UAS aircrew and the DAA collision avoidance system. Any aircrew and any aircraft, however, may be applicable to the analysis and recommendations. The baseline perspective used for STPA-Coordination was the current US NAS rules and regulations and the currently used TCAS functionality, and UAS integration ConOps. However, STPA-Coordination of UAS and the DAA is not limited to status quo constraints in the analysis and design recommendations. In many cases, the recommendations are in stark contrast to the status quo.

It important to note that the safety design paradigm in current NAS operations is largely conceived as a chain-of-failure events or what the FAA labels “defense in depth” (Federal Aviation Administration 2014c). In the NAS, collision avoidance defense layers include procedures, ATC, TCAS, and the (remote) pilot. The defense layers are conceptually seen as independent events that temporally occur in the order just written. However, the defense layers are not independent events that occur in a linear order, with one failing and another taking over. Rather, the defense layers are all inexorably integrated and occurring in parallel. This is where extended STPA for safety analysis contributes.

5.4.2.1 Fundamental Coordination Relationships

The STPA-Coordination case study considers the coordination portions of the safety control structure decomposed into the fundamental coordination relationships as shown in Figure 25.

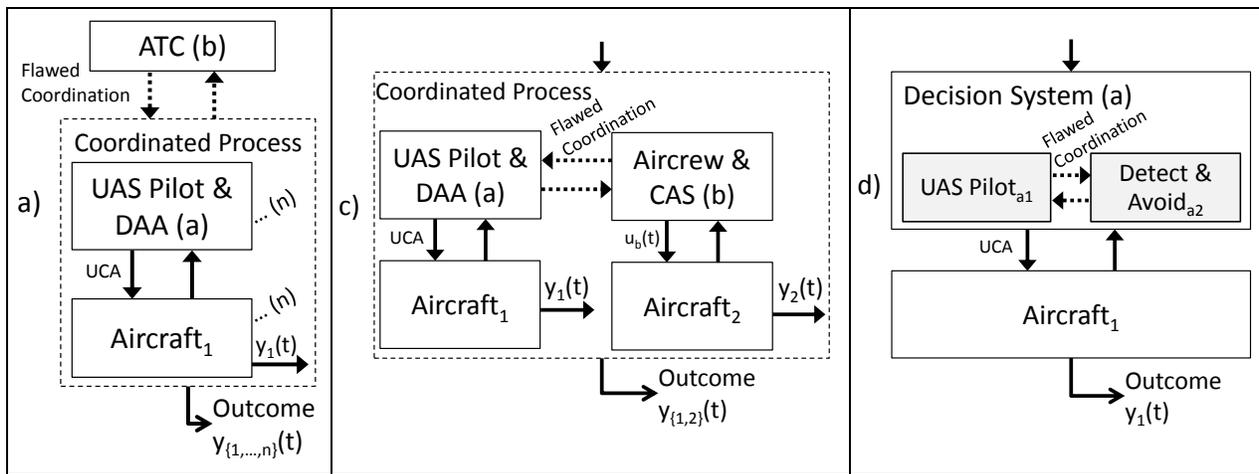


Figure 25. Coordination Relationships for Collision Avoidance

5.4.2.2 Lateral Coordination Causal Analysis

STPA-Coordination was used to analyze within and between decision system lateral coordination. The lateral coordination relationship of interest is represented in Figure 25(b) and (d), which shows the UAS and aircraft decision systems that interact directly with and control the UAS. While the case study focus is on the UAS decision system, its lateral interactions can be with any aircraft decision system such as: remote aircraft or not, and aircraft equipped with a collision avoidance system (CAS) or not.

STPA-Coordination results are presented in tabular format with the following column descriptions:

Hazardous Coordination Scenarios.	The UCA.	Requirements and recommendations.
<ul style="list-style-type: none"> Scenarios categorized by flawed coordination case and coordination element. “Note” provides additional narrative on the scenario. “within DS” identifies within decision system scenarios, UAS aircrew coordination with the DAA. 	Identifying the UCAs that can result from each coordination scenario.	Requirements and recommendations to address the hazardous scenario.

STPA-Coordination hazardous scenarios are traceable to the accident, with traceability provided in the “UCA” column. The hazardous coordination scenarios lead to one or more identified unsafe control actions, which is traceable to the accidents of interest. The results of STPA-Coordination for UAS decision system lateral coordination are presented in Table 26.

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<p>Flawed Case 1. Coordination Missing. Coordination missing between UAS decision system (a) and other aircrew (b), which may lead to UCAs.</p>		
1. Coordination Goals. n/a	n/a	n/a
<p>2. Coordination Strategy. n/a</p> <p>Note. Some form of lateral coordination exists in flight operations at all times in the US NAS. Higher-level rules and regulations (i.e. standardization) address maneuvers and navigation for collision avoidance. Applicable regulations include (Federal Aviation Administration 2014d):</p> <ul style="list-style-type: none"> • CFR §91.113 and §91.115 “Right-of-way rules.” These rules provide coordination strategy for aircraft in distress, converging, approaching head-on, overtaking, and in landing scenarios. • CFR §91.159 “VFR cruising altitude or flight level.” This rule provides coordination strategy for altitude deconfliction for aircraft above 3,000 feet AGL (above ground level) and below 18,000 feet MSL (mean sea level). VFR cruising altitudes are odd thousand +500 feet when navigating east (0-179 degrees) and even thousand +500 feet navigating west (180-359 degrees). This rule separates VFR traffic by 1000 feet and separates VFR-IFR traffic by 500 feet. 	n/a	n/a
<p>5. Group Decision-Making. n/a</p> <p>Note. UAS and aircraft decision systems can engage in pre-planned or real-time group DM.</p>	n/a	n/a
<p>Flawed Coordination Case 2. Coordination Inadequate. Coordination is inadequate between UAS decision system (a) and other decision systems (b), which may lead to UCAs.</p>		
1. Coordination Goals. n/a	n/a	n/a

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<p>2. Coordination Strategy. Lateral coordination between decision systems is inadequate when needed for self-separation or collision avoidance.</p> <ul style="list-style-type: none"> • Decision systems have alternative lateral maneuver strategies for collision avoidance while operating in shared airspace. One strategy is to follow CFR §91.113 and §91.115 Right of way rules. Another strategy is for UAS aircrew to follow DAA alerts and maneuver guidance. The alternative coordination strategies may be incompatible. • (within DS) The DAA may provide guidance that is not compatible with an emergency scenario. Aircraft in an emergency should have priority, which is the current regulation. One can think of this as having priority to descend and use the shortest means (i.e. a straight line) to the nearest airport. The DAA may even be in cooperation with another collision avoidance system in this case. If the DAA is lower in altitude, it may recommend a descent, which is in the same sense that the emergency aircraft is going. • (Within DS) The DAA provides a maneuver envelope to aircrew. A right-of-way rule for a head-on collision potential scenario is aircraft pass to the right. The DAA may not account for the standard and provides a maneuver envelope that is incompatible with coordination standards. <ul style="list-style-type: none"> ○ In a cooperative scenario, the DAA may suggest to (a) a right or left horizontal maneuver and (b) is to remain on current trajectory. Let us say (a) chooses to maneuver left. For decision system (b) to remain on current trajectory in hopes that the (a) will move and solve the problem may be unreasonable; (b) may alter course to the right following accepted standards. ○ A similar scenario could happen in a non-cooperative scenario. 	<p>1, 2.1, 2.4, 3</p>	<ul style="list-style-type: none"> • Comprehensive lateral coordination shall be established between UAS and aircraft decision systems as determined by STPA-Coordination, which includes establishing enabling conditions (elements #7-9). • Vertical ATC coordination shall be established as determined by STPA-Coordination analysis, presented next in Table 27 • UAS decision systems shall provide emergency status to others for integration into coordination maneuvers. <ul style="list-style-type: none"> ○ Consider. The DAA shall have a simple means to relay emergency status and intentions to ATC and other aircraft decision systems. • Consider. Aircraft decision systems involved in a collision scenario shall make positive corrections to mitigate collision potential. At least two beneficial side effects include: 1) give confirmation that guidance was received and 2) provide confidence that a collision will be avoided. Without movement from one or more of the aircraft, doubts may occur. <ul style="list-style-type: none"> ○ The DAA/CAS cooperative maneuvers shall ensure positive corrections ○ If no change maneuvers are deemed acceptable, accountability in coordination strategy is needed to increase confidence. • Standardization and the DAA <ul style="list-style-type: none"> ○ DAA shall follow coordination by standardization protocols.

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<ul style="list-style-type: none"> ○ Note. TCAS provides a vertical climb rate band highlighted green as an example of a safe envelope. ● Use of lateral coordination strategy for collision avoidance can be ambiguous. Aircraft decision systems do not know which coordination strategy to follow for collision avoidance—lateral or vertical coordination strategies. <ul style="list-style-type: none"> ○ Note. When using TCAS, FAA guidance is to follow an RA “...unless doing so would jeopardize the safe operation of the flight, or unless the flight crew can assure separation with the help of definitive visual acquisition of the aircraft causing the RA” (Federal Aviation Administration 2011) p. 38. ○ Let us assume UAS aircrew are trained to interact with the DAA in a similar interaction just discussed with TCAS operations—follow the DAA guidance unless safety is concerned. With this guidance, <i>every</i> collision avoidance encounter involving the DAA is an <i>individual</i> decision to follow maneuver guidance or not. ○ (within DS) The DAA does not provide cooperation information to aircrew. The aircrew cannot determine if the maneuver guidance is in cooperation with other decision systems or not. DAA cooperation is ambiguous. The UAS aircrew may end up making independent decisions in an interdependent scenario where coordination is needed; this limits the benefits of having DAA cooperation in the first place. <ul style="list-style-type: none"> ▪ Note. A comparable scenario may occur when using TCAS, which does not provide pilots information on whether an RA maneuver is in cooperation with 		<ul style="list-style-type: none"> ○ If able to follow procedural standards, predictability, common understanding, and the outcomes may benefit. ○ The DAA shall inform other collision avoidance systems of UAS emergency status to account potential descent and non-maneuvering intentions in a collision scenario. ○ The DAA shall receive emergency status information from others. ○ If the DAA cannot follow coordination standards, the maneuver strategy shall be compatible with standardization. ○ If the DAA cannot follow coordination standardization, the maneuver strategy shall cooperate with other decision systems. ○ The DAA shall have flexible maneuver strategy to handle scenarios not addressed by coordination standards. For example, lateral maneuvers may not work with aircraft on parallel approaches. ● To reduce ambiguity, UAS decision systems shall follow one coordination strategy at a time (assuming comprehensive coordination exists). <ul style="list-style-type: none"> ○ Note. Referencing the coordination framework Axiom [3.2] above, decision systems should follow one coordination strategy at a time when the strategy dictates control actions, which is the

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<p>another TCAS.</p> <ul style="list-style-type: none"> ○ Ambiguity can occur when ATC provides separation instruction for collision avoidance at the same time or during a DAA alert with guidance. It is reasonable for aircrew to debate which guidance to follow as ATC may have the preferred solution. • (within DS) The DAA does not calculate and integrate into coordination maneuver strategy the time when maneuvers can no longer influence an NMAC (near mid-air collision)—a no-influence threshold. <ul style="list-style-type: none"> ○ Note. A comparable scenario may occur when using TCAS. “TCAS calculates a time to reach the CPA (Closest Point of Approach) with the intruder, by dividing the range by the closure rate. This time value is the main parameter for issuing alerts” (Federal Aviation Administration 2011) p. 6. The safety concern with using time to CPA is that the capability to avoid an NMAC may occur at some point prior to CPA. Even if time to CPA was displayed this can be misleading. ○ The no-influence threshold time is dynamic. The dynamic threshold in part depends on individual aircraft energy, energy change potential, and configuration. The DAA maneuver strategy may use a generic aircraft performance model instead of capturing the wide range of UAS aircraft performance between small and medium UAS, and commercial aircraft for examples. • (within DS) Strategy is safe, but UAS aircrew do not follow them due to ambiguity with DAA displays and information. Hazardous coordination scenario refinements relating to human factors and displays in not the focus of this case study, 		<p>case.</p> <ul style="list-style-type: none"> • Assuming comprehensive coordination, strategy shall use a layered approach to collision avoidance. <ul style="list-style-type: none"> ○ First layer with longer time constants may use ATC or procedural control (i.e. coordination by control methods). ○ Second layer for collision scenarios closer in time and higher in probability use comprehensive lateral coordination aided by DAA or other collision avoidance automation. • The DAA shall provide cooperation status with other aircraft decision systems to the UAS aircrew. The DAA and other collision avoidance systems are not the decision makers and their cooperation must be known beyond their automation. • Consider. All aircraft in shared airspace should have compatible collision avoidance equipment. • Consider. All flight operations in shared airspace shall use a single frequency, verbal and digital. • The DAA/CAS shall account for time when maneuvers can no longer influence an unsafe outcome (i.e. NMAC), which is not CPA as used in TCAS. • The DAA shall account for individual UAS performance and energy characteristics for calculating the dynamic no-influence threshold. • The DAA shall unambiguously display

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<p>but is potential future work.</p> <ul style="list-style-type: none"> In addition, aircraft decision system lateral coordination strategy has inadequate enabling conditions. (see coordination elements #7-9) 		<p>maneuver guidance, following human factors principles and results of display studies so that UAS aircrew are given the best opportunity to implement a cooperative maneuver strategy.</p>
<p>3. Decision Systems. n/a</p>	<p>n/a</p>	<p>n/a</p>
<p>4. Communications.</p> <ul style="list-style-type: none"> The bandwidth required for lateral coordination is inadequate. For UAS and DAA operations, the bandwidth needs to be available for (near) real-time coordination when collision scenario develops. (within DS) The DAA send/receive protocols and language may not be compatible with other collision avoidance or electronic identification systems. The channel capacity required for UAS and DAA lateral coordination efforts is inadequate. Communication transmissions occluded or degrade potentially due to: <ul style="list-style-type: none"> External signal jamming. Electromagnetic interference with onboard or external equipment. (within DS) The DAA electromagnetically interferes with communications. Communications equipment location. The aircraft maneuvers and its physical silhouette occlude communication signals. 	<p>1, 2.1, 2.6, 3, 4</p>	<ul style="list-style-type: none"> DAA communication shall be compatible with existing collision avoidance systems, or Collision avoidance systems shall be upgraded for compatibility. Communication bandwidth shall permit (near) real-time DAA coordination with other decision systems when needed for collision avoidance. Communication channel capacity shall meet (near) real-time information requirements needed for lateral coordination. The location of communications equipment shall not interfere with coordination-related communication transmissions. The placement of communications equipment shall not unduly limit UAS maneuvers (i.e. maneuver adequate for operations). The DAA shall be electromagnetically compatible with UAS onboard equipment, UAS external support equipment, and external NAS equipment. If maneuver limits are needed to prevent degraded or interrupted communications, the UAS decision system shall know limitations: <ul style="list-style-type: none"> The DAA shall integrate this information for maneuver

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
		<p>decisions.</p> <ul style="list-style-type: none"> ○ The UAS operator shall be trained of maneuver limitations. ○ The UAS operator shall be provided alerts approaching maneuver limitations. ○ Consider. UAS flight control filters on UAS operator maneuver inputs.
<p>5. Group Decision-Making. In the current NAS, should ATC “fail” to separate aircraft then collision avoidance is left to UAS and other aircraft. Group DM may be beneficial. Group DM for collision avoidance can use verbal or digital communication means. Inadequate group DM may lead to UCAs.</p> <ul style="list-style-type: none"> • Aircrew do not use available communication channels, verbal or digital, for group DM. They may not use communication channels: <ul style="list-style-type: none"> ○ Desire not to disrupt channels, especially during heavy traffic communications. ○ Protocols and training do not promote free form dialogue on ATC frequency that may be needed for collision avoidance maneuver group DM. • Aircrew do not observe the correct communication channels and cannot engage in group DM. • (within DS) The DAA may or may not be in cooperation with the other aircraft. When not in cooperation, aircrew are perhaps making independent decisions based on limited and non-coordinated DAA information and guidance. 	<p>1, 2.1, 2.4, 2.6, 4</p>	<ul style="list-style-type: none"> • Regulations shall establish group DM protocols. Some protocols for consideration include: <ul style="list-style-type: none"> ○ Group decision-making shall use the same frequency. ○ Other communications shall cease on frequency until collision avoided, or be sent by other means if available (e.g. digital or on simulcast frequency). ○ Group decision-making shall have means for digital language communication. ○ The DAA shall enable group DM for collision avoidance strategy selection. • The DAA shall inform aircrew if maneuver guidance is in cooperation with other aircraft.
<p>6. Observation of Common Objects. Decision systems in lateral coordination should observe common objects, including each other. This same concept is recursive for decision components within decision systems. The following are scenarios where observation of common objects is lacking, which may</p>	<p>1, 2.1, 2.2, 2.3, 2.4, 2.6, 4</p>	<ul style="list-style-type: none"> • Decision systems shall share observed information with each other. <ul style="list-style-type: none"> ○ The DAA shall send and receive observed information within and between decision systems.

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<p>lead to UCAs:</p> <ul style="list-style-type: none"> • One or more aircraft decision systems do not observe each other because of the following: <ul style="list-style-type: none"> ○ Subsystems to provide aircraft state information to decision systems are not available (inspired by RTCA SC-203 2013). ○ (within DS) DAA and displays are not compatible for sharing information. ○ (within DS) DAA observation subsystems and displays degrade or fail. ○ (within DS) Limitations with observation subsystems: <ul style="list-style-type: none"> ▪ In certain environmental conditions. For example, the DAA cannot observe through clouds, precipitation, haze, night, smoke, etc. ▪ Against airborne objects: size, shape, materials, etc. • Aircraft decision systems do not observe each other in shared airspace because they do not expect each other. For example, an aircraft may be in special use airspace (e.g. military operating areas, restricted airspace, etc.) and a UAS inadvertently enters the special use airspace. Either may not be aware of or discredit alerts because traffic is not as expected. • One or more aircraft decision systems do not observe the same surrounding aircraft (same reasons as for not observing each other). • Aircraft decision systems cannot resolve maneuver guidance that is deemed unsafe by one and not the other decision system. <ul style="list-style-type: none"> ○ One scenario is that a UAS decision system is told to climb, but cannot for other traffic. The other aircraft remains level or descends. The level aircraft is a clear problem, as is a descending aircraft that delays maneuver. 		<ul style="list-style-type: none"> • UAS decision systems shall have station keeping and navigational capability to avoid inadvertent entry or exit from special use airspace and becoming a collision potential with other aircraft. • UAS decision systems shall be alerted to special use airspace boundaries. • Consider. DAA shall have a mode that alerts when intruder is within a safety envelope regardless of perceived collision potential; this accounts for the unpredictable nature of special use airspace operations. For example, alert for aircraft within 3 nautical miles and 5000 feet when in <i>special use airspace</i> mode. • UAS decision systems shall fly in a manner that accounts for observation equipment limitations. For example, avoid clouds or ensure another means for observation such as flight under ATC if IMC flight is necessary. • Decision systems shall observe or otherwise have knowledge of terrain and ground obstacles. <ul style="list-style-type: none"> ○ The DAA shall observe terrain and ground obstacles by one or more of sensors or digital database. • The DAA shall have a means to check observation of common objects with other collision avoidance systems. <ul style="list-style-type: none"> ○ Consider. The DAA checks number count of airborne objects being considered with other system. ○ Consider. The DAA checks geo-time stamp of objects being considered with other

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<ul style="list-style-type: none"> ○ (within DS) The DAA may receive a cooperative maneuver vector from another collision avoidance system that is unsafe from what it observes. The DAA, however, cannot re-negotiate another maneuver set. For example, TCAS directs the DAA to climb, but a climb places the UAS into another aircraft that TCAS does not observe. The DAA may not have the ability to resolve this scenario and instead forced to resolve the follow-on scenario next. ● (within DS) The DAA does not observe the same objects as the aircrew and subsequently provides maneuver guidance that aircrew will not follow. Observation discrepancies may develop from: <ul style="list-style-type: none"> ○ Non-cooperating aircraft are not observed by the DAA. Aircraft may not have IFF (Identification, Friend or Foe), ADS-B (Automatic Dependent Surveillance-B), or have failures of other cooperative systems for example. ○ Airborne obstacles not observable by DAA self-observation technology such as radar, laser, electro-optics, or acoustics due to: <ul style="list-style-type: none"> ▪ Obstacle size, shape, materials. ▪ Technology limitations from environment: terrain, clouds, etc. ○ Terrain and other ground obstacles. ● (within DS) UAS aircrew observe different aircraft than the DAA. The DAA can display the aircraft symbol, but does not correlate the factor traffic to the electro-optics displays used by the aircrew for visual processing. In such scenarios, the aircrew may not follow DAA guidance if mistakenly believing they observe the factor traffic. 		<ul style="list-style-type: none"> ○ system. ○ The DAA shall alert when a discrepancy exists in observation of common objects. ● The DAA shall (re-) negotiate a compatible and safe maneuver set where UAS maneuvers are constrained by other ground or airborne objects. ● Consider. Design and regulation requirements to ensure electronic identification capability on aircraft and other airborne objects flying in the NAS. <ul style="list-style-type: none"> ○ Note. Current US NAS Class D, E, and G airspaces do not require aircraft to be equipped with transponders. Observation of common objects can be difficult in today’s NAS. ● Consider. The DAA shall have self-observation capability beyond sector coverage, such as forward hemisphere coverage. Full volume or spherical self-observation coverage would provide more information to the UAS decision system and reduce observation gaps between UAS aircrew and the DAA. Full volume coverage may be achieved by: <ul style="list-style-type: none"> ○ Static full volume coverage by one or more overlapping sensors. ○ Sensors that sweep and rotate dynamically. ● Visual correlation to factor traffic shall be used to assist UAS decision systems. Visual correlation may be achieved through:

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
		<ul style="list-style-type: none"> ○ Consider. DAA electro-optic sensors shall automatically or on demand slave to factor traffic to assist in visual acquisition. ○ Consider. DAA electro-optics displays shall digitally correlate traffic using synthetic highlights, such as a digital container around a designated collision threat.
<p>7. Authority, Responsibility, Accountability.</p> <p>Authority and Responsibility. n/a</p> <p>Note. Aircraft decision system authority and responsibility is adequate for this case study. The decision systems have the authority and responsibility to manage their aircraft in safe manner to avoid collisions. Coordination authority and responsibility, however, may be inadequate—see coordination late Case 4.</p> <p>Accountability. Accountability for lateral coordination is inadequate. For collision avoidance, accountability includes: 1) confirmation of maneuver strategy received, 2) acknowledge agreement or suggest alternative strategy, 3) update decision systems when complying with maneuver and 4) when maneuvers complete. The following scenarios have inadequate accountability that may lead to UCAs.</p> <ul style="list-style-type: none"> • Decision systems are not on same frequency and accountability does not exist. • Decision systems are on the same frequency, whether controlled or uncontrolled airspace. Decision systems may not acknowledge strategy or provide updates on the execution of the strategy for other decision systems. • (within DS) DAA provides maneuver guidance without other decision system cooperation. Lack of cooperation may occur from: 	<p>1, 2.1, 2.4, 2.6, 3, 4</p>	<ul style="list-style-type: none"> • Coordination strategy shall establish accountability or protocol to achieve accountability in conditions where real-time communication can exist. • Consider. Regulations should allow decision systems to achieve accountability on same frequency as ATC. • The DAA/CAS shall provide means to establish lateral coordination accountability. Accountability requirements at a minimum shall include: <ul style="list-style-type: none"> ○ UAS decision systems shall confirm receipt of DAA derived maneuver strategy. ○ UAS decision systems shall confirm agreement with maneuver strategy (if not, coordination element #4 group DM shall exist for negotiation). ○ When complying with the DAA derived maneuver, the DAA shall automatically send signal to other decision system, or ○ When complying with the coordination maneuver

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<ul style="list-style-type: none"> ○ Other aircraft not equipped with collision avoidance systems. ○ Other aircraft collision avoidance equipment failure. ○ Incompatibility with other collision avoidance systems. ● (within DS) The DAA does not have means to establish accountability for lateral coordination. Both decision systems have cooperating DAA/CAS and both provide compatible maneuver guidance, such as aircraft (a) climb and (b) descend. <i>Cooperation is not coordination</i>, however. Specifically, DAA cooperation with other collision avoidance systems is not lateral aircraft decision system coordination. Some DAA inadequate accountability scenarios include: <ul style="list-style-type: none"> ○ Decision systems do not confirm receipt of DAA/CAS cooperative maneuver strategy and they actually did not receive the maneuver guidance. ○ Decision systems do not acknowledge agreement with DAA/CAS maneuver guidance and one or more actually disagree with guidance. ○ Decision systems do not confirm compliance with the DAA/CAS maneuver guidance, and they did not comply. ○ Decision systems do not confirm collision avoidance maneuver completion. 		<p>strategy, the aircrew shall manually indicate maneuver execution with button press that translates into a DAA signal or through verbal updates as appropriate for the situation.</p> <ul style="list-style-type: none"> ○ UAS decision systems shall confirm maneuver completion through the DAA or verbally. ● ATC and aircrew shall be trained in collision avoidance accountability requirements.
<p>8. Common Understanding. Successful coordination needs common understanding among decision systems. Following are scenarios that can lead to inadequate common understanding and ultimately lead to UCAs.</p> <ul style="list-style-type: none"> ● There are alternative coordination strategies for collision avoidance and UAS decision systems are not aware of which strategy is being used. <ul style="list-style-type: none"> ○ Note. In the NAS status quo, aircraft decision systems do not know which coordination strategy is being used: either 	<p>1, 2, 3, 4</p>	<ul style="list-style-type: none"> ● With comprehensive coordination, regulations shall prescribe a layered set of coordination strategies to use in efforts to minimize alternative strategies for decision systems trying to avoid a collision. ● To assist UAS aircrew common understanding of factor airborne and ground obstacles and collision time constraints, the DAA displayed information:

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<p>following ATC, following TCAS, or no coordination at all.</p> <ul style="list-style-type: none"> • UAS decision systems may have different understanding or awareness of the severity of the separation violation scenario. With different perspectives on the risk, concerns other than collision may take over. Potential reasons for risk divergence include: <ul style="list-style-type: none"> ○ Decision system judgement of time remaining before a maneuver is needed. ○ Observation of an object believed to be the factor traffic, but in fact is the wrong object. This could occur from inadequate correlation between displays and the real-world. <ul style="list-style-type: none"> ▪ Judging distance from another airborne object can be difficult by visual means alone. Some factors include: <ul style="list-style-type: none"> • Environmental conditions such as sun angle, haze, precipitation, smoke, clouds, background terrain features, color, etc. • Object size and aspect angle. • Limited familiarity with judging distances. ▪ Judging bearing may be difficult due to lack of references and familiarity of task. ○ (within DS) DAA cautions and warnings may be disabled. ○ (within DS) DAA may have failed or is partially degraded. ○ (within DS) DAA may not have severity level distinctions designed into the automation. ○ (within DS) DAA may have different 		<ul style="list-style-type: none"> ○ Shall have current ownship state information. ○ Shall have relative state information to factor obstacle. ○ Shall have a time measure (recommend time to no escape). • Display of ownship state and relative state information to factor obstacles shall be unambiguous to UAS aircrew. • The DAA system shall have distinctive alert levels to signify severity. • Severity alerts shall be consistent across collision avoidance systems. <ul style="list-style-type: none"> ○ A high severity alert on decision system (a) should match a high severity alert on decision system (b). • Disabling DAA cautions and warnings shall be a deliberate action to avoid inadvertent disabling. • Cautions and warning shall be “on” as default. • The DAA system shall meet minimum uncertainty requirements for flight certification. • The DAA system shall meet minimum reliability requirements for flight certification. • Decision systems shall be alerted when state information may be missing, incorrect, or beyond acceptable uncertainty. <ul style="list-style-type: none"> ○ Consider. DAA/CAS cooperative maneuver guidance shall default to procedural guidance, such as altitude separation based on last known altitudes. ○ Consider. Regulation shall

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<p>severity distinctions compared to other collision avoidance systems. The DAA may alert for SST, but how does this correspond to decision system (b) alerts.</p> <ul style="list-style-type: none"> • Common understanding may be hindered by too much uncertainty in decision system states. Uncertainty may derive from: <ul style="list-style-type: none"> ○ Self-observation. ○ Electronic position identification. ○ Between decision system communications (e.g. communication delays, noise or jamming). • (within DS) DAA ownship state information or state information received from other aircraft decision systems may be missing or wrong due to: <ul style="list-style-type: none"> ○ Degradation of one or more systems providing state information, such as GPS, gyros, RALT (radar altimeter), etc. ○ Failure of one or more systems providing state information. • (within DS) DAA provides ambiguous information to UAS aircrew relating to ownship state or state relative to separation/collision potential. • (within DS) DAA maneuver guidance does not integrate the same information or constraints as other decision components (e.g. aircrew and collision avoidance systems). With different inputs, maneuvers may lead to UCAs. Examples of input differences that could influence common understanding include: <ul style="list-style-type: none"> ○ Information on ground data and obstacles. ○ Information on other airborne aircraft or obstacles. ○ Information related to aircraft physical characteristics, such as wingspan and length. ○ Information related to aircraft performance, aerodynamic, and structural characteristics. 		<p>direct verbal communications for collision avoidance lateral coordination when DAA/CAS degrade or fail.</p> <ul style="list-style-type: none"> • Decision systems shall integrate the same information for collision avoidance maneuver decisions, including: <ul style="list-style-type: none"> ○ Terrain and ground obstacle data. ○ Information on airborne objects. • Decision systems shall use the same or similar performance models for a given aircraft and configuration. • Consider. Aircraft decision systems shall use the same set of maneuver combinations to ensure common understanding and avoid potential conflict in maneuver suggestions. • The DAA/CAS shall communicate separation and collision avoidance maneuver limitations, such as TCAS not having horizontal maneuver guidance capability. • The DAA shall not be constrained in maneuver guidance by a limited maneuver set of other collision avoidance systems. For example, the DAA shall recommend a horizontal maneuver should it be most beneficial in a scenario with a TCAS-equipped aircraft that can only recommend vertical maneuvers. • Consider. The set of collision avoidance maneuvers to include vertical, horizontal and speed options for greater flexibility in response to environment and a wide range of aircraft performance.

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<ul style="list-style-type: none"> • (within DS) The performance models and assumption used to determine maneuvers may be different for each decision system, which may lead to UCAs. • (within DS) The set of possible maneuvers to solve a potential collision scenario is different for each decision component, which may lead to UCAs. The DAA may have both horizontal and vertical maneuver guidance, while TCAS/ACAS has vertical maneuvers only. The aircrew has an unlimited set of maneuvers for problem solving using a combination of horizontal, vertical, and speed. Example concerns include: <ul style="list-style-type: none"> ○ An outcome with greater safety margin may exist with control actions outside the set of those considered by the decision component. ○ Decision components may not be aware of control action limitations in recommended actions by other decision components. ○ Decision components may recommend or determine conflicting maneuvers, and the aircrew (or decision component with decision authority) must resolve the conflict. • (within DS) DAA and collision avoidance automation used by each aircrew may be in automation modes that are incompatible and provide different decision information to each aircrew. <ul style="list-style-type: none"> ○ A worst case example would be that the systems are not turned on. ○ Another example is one system in standby and not providing maneuver guidance. If the collision avoidance mode is not functioning, for any reason, UCAs may occur. • (within DS) The DAA provides unidirectional guidance (e.g. climb only, left turn only, etc.) 		<ul style="list-style-type: none"> • The DAA shall have a means to alert other decision system of incompatible or incorrect mode for cooperation, such as another TCAS or DAA in standby. • The DAA shall receive alerts from other collision avoidance systems if in standby or other incompatible mode for cooperation. • The DAA shall highlight (e.g. by display) airborne and ground obstacles that are accounted for in the maneuver guidance to help assist common understanding with the UAS aircrew. For example, if a maneuver envelope is not suggested due to an obstacle then highlight the obstacle as a secondary conflict. This provides a quick means for aircrew to assimilate information and assess the acceptability of the DAA solution. • The DAA shall give cooperation status when providing collision alerts and maneuver guidance so that aircrew can more adequately calibrate their trust. • Aircraft decision systems shall alert each other (and ATC) when aircraft is not fully controllable so coordination can account for inability to maneuver. • The DAA shall alert other DAA/CAS when the UAS is no longer controllable by aircrew, such as in lost link scenarios. • Consider, the DAA shall automatically cooperate and maneuver for collision avoidance should UAS aircrew flight controls fail or degrade. • Consider. The DAA alerting thresholds shall match other CAS thresholds for collision avoidance in efforts to

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<p>because of observed obstacles. However, the aircrew are not aware of the obstacle (display clutter options, just miss it, etc.). The UAS aircrew may desire to maneuver in the opposite sense, which may place the UAS in a more unsafe position. Examples of internal motivations that may cause hazards when common understanding is inadequate:</p> <ul style="list-style-type: none"> ○ Desire to maneuver IAW right-of-way rules. ○ Based on display observations, believe the DAA to be wrong. ○ Confidence in algorithm accuracy is low and believe own maneuver strategy is more safe. ○ Note. Other limited confidence examples may result from DAA suggestive maneuvers that go against accepted practice or are too dynamic (due to uncertainty for example), such as: <ul style="list-style-type: none"> ▪ Lateral maneuvers that place UAS heading further in front of collision traffic versus a maneuver to the aircraft tail. ▪ Lateral maneuvers that go against right-of-way rules. ▪ Lateral maneuvers near the unacceptable boundary region when the boundary is dynamic (e.g. if trying to minimize trajectory deviations). ● Verbal radio communications help aircrew build common understanding. Aircrew may be on different radio frequencies: <ul style="list-style-type: none"> ○ By policy design (e.g. it is allowed to have aircrew on different UHF/VHF frequencies with the same controller). ○ By memory lapse: <ul style="list-style-type: none"> ▪ Aircrew memory lapse at designated time or event to switch frequencies. 		<p>promote timely and beneficial maneuver strategy cooperation.</p>

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ▪ Aircrew memory lapse on controlling agency handoff frequency. <ul style="list-style-type: none"> ○ By slips during manual inputs of next radio frequency. • (within DS) The DAA knows if the alerts and maneuver guidance are in cooperation with other aircraft decision systems. However, the DAA does not inform UAS aircrew of the cooperation status. UAS aircrew may blindly follow DAA maneuver guidance when it was not in cooperation with any other decision system. • (within DS) The DAA believes it is in cooperation with another CAS. But the other aircraft is in fact not controllable due to some failure or degradation of systems related to flight control, including lost link. The DAA/CAS may decide to keep the UAS on current trajectory while the other non-controllable aircraft maneuvers away. • (within DS) The DAA has different alerting thresholds than other CAS for developing and providing collision avoidance maneuver guidance. In such cases one aircraft may be maneuvering before needed or while the other aircraft is developing a maneuver strategy. 		
<p>9. Predictability.</p> <p>Note. In UAS integration ConOps, there are two predicted risk thresholds for DAA caution and warning maneuver guidance as shown in Figure 26. The first and lower risk threshold is the SST (Self-Separation Threshold) boundary. The SST seeks to avoid the well clear violation (WCV), which is derived in part from 14 CFR §91.181 mandate to “pass well clear of other air traffic” (Federal Aviation Administration 2014d). The next and higher risk threshold is the CAT (Collision Avoidance Threshold) boundary. Maneuvering by the CAT seeks to avoid an NMAC.</p>	<p>1, 2.1, 2.2, 2.4, 2.5, 2.6, 2.7, 3, 4</p>	<ul style="list-style-type: none"> • Temporal constraints for maneuvering shall be known by decision systems. The most critical temporal constraints is the predicted time when maneuvering within feasibility constraints can no longer influence a safe outcome or avoid a collision (this is different than CPA used for TCAS). Some recommendations include one or a combination of the following: <ul style="list-style-type: none"> ○ Countdown timer in minutes/seconds to when a maneuver must be accomplished. ○ A color gradient from green,

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<div data-bbox="203 315 803 724" data-label="Diagram"> <p>The diagram illustrates four concentric, irregularly shaped regions representing separation boundaries around a central aircraft symbol (a red airplane). From the innermost to the outermost, the regions are: NMAC (orange, with a crosshair symbol), CAT (yellow), WCV (blue), and SST (green). Dashed lines indicate the boundaries between these regions. An arrow points from the central aircraft towards the SST region.</p> </div> <p data-bbox="194 730 779 840">Figure 26. UAS Separation Boundaries. Reprinted from (Federal Aviation Administration 2013b), p. 3-20. Figure in public domain.</p> <p data-bbox="186 892 730 955">The models used to predict maneuvers may be inadequate and lead to UCAs.</p> <ul data-bbox="186 966 812 1890" style="list-style-type: none"> • The decision systems may be missing temporal constraints to predict when maneuvers are required. <ul style="list-style-type: none"> ○ (within DS) The DAA does not display for UAS aircrew the time when maneuvers can no longer influence an NMAC. • The decision systems may have incorrect temporal models or not account for worst case environment impact on time (e.g. algorithms that use average or highest likelihood time). With inadequate temporal models, timing of maneuvers may lead to UCAs. • (within DS) Without accountability, DAA ability to predict is limited against an observed decision system maneuvering independently. Problems may arise when: <ul style="list-style-type: none"> ○ Decision system (b) may not be maneuvering per algorithm assumptions, such as in straight line and constant velocity flight. ○ Decision system (b) may not meet physical property assumptions, such as aircraft wingspan. 		<p data-bbox="1055 315 1412 535">yellow, to red. However, alone, this does not tell you how much time is left unless you see when the color changed which should not be relied upon.</p> <ul data-bbox="925 546 1437 1858" style="list-style-type: none"> ○ An analog scale that displays countdown by a dynamic ticker on a fixed scale, or a dynamic scale and fixed thresholds. • Consider use of worst-case temporal models. If other than worst-case models are used for collision avoidance, verify assumptions for scenarios dismissed and ensure aircrew aware of temporal model limitations. • Decision systems shall share maneuver intentions. • The DAA shall integrate accountability information (i.e. confirmation of maneuver strategy received and agreed) to maneuver guidance coordination, which may reduce unnecessary deviations. • Consider. When accountability is established between decision systems, the DAA should reduce maneuver guidance uncertainty to reflect improved predictability. This may reduce NAS disturbances, which is perhaps more beneficial in terminal area (i.e. dense) flight operations. • The DAA shall use performance models that account for various aircraft and configurations. Performance of commercial heavy aircraft is different than a typical small or medium weight UAS that will be encountered in future UAS integrated flight operations.

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<ul style="list-style-type: none"> ○ Decision system(b) may have energy beyond DAA algorithm assumptions, such as maneuvering against a fighter aircraft with relatively high energy. ● Predictability is inadequate when not sharing decision system maneuver intentions. If maneuver intentions are not shared, a maneuver bubble around each decision system is needed. The assumed bubble has at least two concerns: <ul style="list-style-type: none"> ○ Calculated maneuvers are more dramatic than necessary, if needed at all. In some cases, maneuvers in excess of what is needed may lead to UCAs. ○ Maneuvers are not enough if one of the decision systems will maneuver or has performance in excess of the assumed bubble. ● (within DS) The DAA may not update and improve maneuver guidance when accountability established between decision systems. Leaving larger safety margins in maneuver guidance may inadvertently lead to UCAs (←UCA.2*) ● (within DS) The performance models used for determining maneuvers are inadequate, which may be caused by: <ul style="list-style-type: none"> ○ Simplifying assumptions may inadequately characterize aircraft performance observed in integrated flight operations, including lower performance UASs, passenger airliners, and higher performance fighter aircraft. ○ Note. A comparable scenario may exist with TCAS in that it is “designed to work on typical passenger airliners” (Kochenderfer et al. 2008) p. 52. ○ Incorrect performance model, wrong aircraft or configuration was used to calculate maneuver. 		<ul style="list-style-type: none"> ● The DAA and CAS shall share aircraft type and configuration for use in coordination. An example type and configuration breakout could be a 3 x 3 matrix as follows: <ul style="list-style-type: none"> ○ Aircraft performance: high, medium, low. ○ Aircraft configuration. High drag, normal, low drag.
<p>Flawed Coordination Case 3. Coordination Strategy Leads to Hazard. UAS decision system coordination strategy directly leads to UCAs.</p>		

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
1. Coordination Goals. n/a	n/a	n/a
<p>2. Coordination Strategy.</p> <ul style="list-style-type: none"> • Not feasible. Coordination strategy inadequately accounts for aircraft constraints and limitations and the decision system exceeds them during separation and collision avoidance maneuvers. Example scenarios are concerned with the avoidance maneuver: onset rate, amplitude, and time at amplitude. <ul style="list-style-type: none"> ○ Maneuvers do not account for aerodynamic limitations and stall the aircraft. ○ Maneuvers do not account for performance limitations. An aircraft may not climb adequately near a performance altitude ceiling. ○ Maneuvers do not account for structure limitations and exceed speed or life load limitations that can degrade or fail the aircraft physical structure. • Not acceptable. <ul style="list-style-type: none"> ○ The coordination strategy does not provide a stop time or provides an inadequate stop time. See flawed case 2, predictability and common understanding for additional details. ○ (within DS) DAA and CAS recommend maneuvers that lead to UCAs. <ul style="list-style-type: none"> ▪ Coordinated maneuvers have aircraft cross flight paths (i.e. the maneuvers are into each other). <ul style="list-style-type: none"> • Note. Current TCAS logic recommends aircraft cross flight paths (i.e. the same altitude) given certain scenarios. Crossing flight paths in such close proximity may create a collision potential. 	1, 2, 3, 4	<ul style="list-style-type: none"> • Coordination strategy shall account for aerodynamic and performance limitations. • The DAA shall account for aircrew (human) performance limitations. • The coordination maneuver strategy shall include adequate start and stop times, which are explicit in maneuver guidance. <ul style="list-style-type: none"> ○ Implicit timing that relies on assumptions and training may be inadequate. • The coordination strategy shall not maneuver aircraft to cross altitudes, unless to do so would lead to a hazard such as damaging the aircraft. • Consider. If cross altitude maneuvers are deemed acceptable, a counter maneuver should be implemented that improves margins in case of errors in maneuver execution or calculations. For example, if aircraft in climb is deemed safe to continue climb through another aircraft’s level flight, have the level aircraft maneuver down and/or horizontally also. • The coordination strategy shall not maneuver aircraft into additional airborne obstacles that may lead to another mid-air collision. • The coordination strategy shall not maneuver aircraft towards terrain or other ground objects in a manner that may lead to a ground collision. Information to integrate include: <ul style="list-style-type: none"> ○ Terrain and ground object data. ○ Rate of descent. ○ Ability to change energy state.

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<ul style="list-style-type: none"> • Algorithms may assume velocity and accelerations, and only account for (near) real-time position information. • Algorithms may inadequately account for converging flight paths and heading crossing angle. ▪ Maneuver one or more of the aircraft into other airborne obstacles. In such cases, the coordination strategy could lead to other separation violations. <ul style="list-style-type: none"> • The algorithms may prioritize the closest threat only. • The algorithms may ignore other traffic all together. • The DAA/CAS with responsibility to develop the cooperative maneuver ignores the non-priority vicinity traffic. ▪ Maneuver one or more aircraft towards terrain or other ground obstacles. <ul style="list-style-type: none"> • The maneuver algorithms are not integrated with ground collision systems. • The maneuver algorithms do not input terrain data. • The maneuver algorithms have access to terrain data, but terrain data are missing or expired. • Algorithms do not 		<ul style="list-style-type: none"> ○ Dive angle. ○ Altitude threshold where ground collision cannot be avoided. • The DAA shall alert UAS aircrew when missing terrain data, corrupted, or expired terrain data. • The DAA shall account for follow on traffic post-maneuver. If traffic may be a factor within a pre-defined time threshold, an alternative coordination strategy should be selected.

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<p>account for geo-temporal constraints in descent maneuvers. For example, based on energy and aircraft maneuverability there is a point in space prior to impact, where ground impact cannot be stopped (inspired by (Gray III 2016)).</p>		
<p>Flawed Coordination Case 4. Coordination Strategy Established Late. Aircrew coordination strategy is established late, which may lead to UCAs.</p>		
1. Coordination Goals. n/a	n/a	n/a
<p>2. Coordination Strategy.</p> <ul style="list-style-type: none"> • The coordination strategy may not be established in time to influence (near) mid-air collision scenarios. • The coordination strategy does not provide a start time for maneuvers. • The coordination strategy start time is inadequate. 	1, 2.1, 2.4, 2.6, 3, 4.1	<ul style="list-style-type: none"> • The coordination elements shall integrate to establish an acceptable strategy within dynamic time constraints.
3. Decision Systems. n/a	n/a	n/a
<p>4. Communications.</p> <ul style="list-style-type: none"> • (within DS) The DAA does not account for communication delays in determining separation alerts and maneuver guidance. As the collision potential nears, accounting for communication delays on the order of seconds becomes more critical. 	1, 2.1, 2.4, 2.6, 3, 4.1	<ul style="list-style-type: none"> • The DAA shall have a means to measure communication delays between aircraft decision systems and ATC. • The DAA shall integrate communication delays into alerts and maneuver guidance.
<p>5. Group Decision-Making. Group DM processes may lead to UCAs.</p> <ul style="list-style-type: none"> • If group DM uses digital means, the process may take too long. For example, having to input text may not be quick enough for group DM in collision scenarios. • Group DM protocols do not track time constraints on the current separation or collision scenario. In 	1, 2.1, 2.4, 2.6, 3, 4.1	<ul style="list-style-type: none"> • If digital means are used to assist in group DM, the DAA shall have standard messages available for negotiation with other aircraft decision systems. An example text session may be: Decision system (a) “I climb, you descend” with a response from decision system (b) “copy, descending.”

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<p>such cases, decision systems may delay group DM to gather more information.</p> <ul style="list-style-type: none"> (within DS) The DAA maneuver guidance does not account for human performance limitations, such as the time needed to make decisions and take actions. Providing maneuver guidance without time to make decisions and take follow on actions could lead to UCAs. For example, pilots are expected to make takeoff abort decisions within several seconds and abort thresholds are computed off of this decision time assumption. 		<ul style="list-style-type: none"> Decision time constraints shall be calculated for UAS decision systems and displayed for aircrew using one or a combination of visual, audio, and tactile feedback displays. The DAA shall provide maneuver guidance with enough time for individual UAS aircrew to make decisions and take actions.
<p>6. Observation of Common Objects.</p> <ul style="list-style-type: none"> Update rates on decision system state information is inadequate. The real need for coordination is known too late to influence the outcome. 	<p>1, 2.1, 2.4, 2.6, 3, 4.1</p>	<ul style="list-style-type: none"> Update rates shall be adequate for (near) real-time coordination of separation maneuvers.
<p>7. ARA. Authority and Responsibility. Coordination decision authority and responsibility are not established between decision systems. Coordination can still occur without authority, however, it may take more time to reach consensus if consensus can be reached at all.</p> <ul style="list-style-type: none"> Note. Authority for lateral coordination exists in military formation flight operations. There will be a flight lead that is able to make decisions for the formation. With decision authority, lateral coordination may be expedited. Outside of military formation flight, however, coordination decision authority does not appear to exist in protocols for lateral coordination. Cooperation among the DAA/CAS is not coordination authority or responsibility. Establishing coordination authority and responsibility takes time that may not exist when there is a collision scenario potential. With assistance from the DAA, coordination authority and responsibility may not be a significant concern. But in off-nominal conditions or when one decision system does not have a CAS, 	<p>1, 2.1, 2.4, 2.6, 3, 4.1</p>	<ul style="list-style-type: none"> Decision systems shall have coordination authority; regulation shall allow them to engage in lateral coordination as needed for collision avoidance. Decision systems shall establish <i>decision</i> authority and responsibility for lateral coordination decisions in collision avoidance scenarios. Consider: <ul style="list-style-type: none"> First to establish contact (by digital or verbal means) has decision authority. The lowest or highest transponder code (e.g. Mode 3/A identification code). The DAA shall identify and display which decision system has decision authority when in cooperation with another CAS. When not the decision authority, decision systems shall be responsible to engage in coordination and evaluate coordination for feasibility and

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<p>establishing authority and responsibility for collision avoidance coordination is perhaps more important.</p>		<p>acceptability (i.e. does not lead to hazards).</p>
<p>7. ARA. Accountability.</p> <ul style="list-style-type: none"> • Time constraints are not established by decision systems for developing the maneuver strategy. <ul style="list-style-type: none"> ○ (within DS) The DAA does not calculate and display the time remaining to develop and execute a coordination strategy for collision avoidance. ○ Note. This is analogous to the TCAS. When a TCAS RA occurs, there is a calculated 15-35 seconds from the CPA. This is a 20 second difference that pilots may not have awareness on for making decisions. • Time constraints may be established, but are not monitored or forgotten by decision systems when developing strategy. 	<p>1, 2.1, 2.4, 2.6, 3, 4.1</p>	<ul style="list-style-type: none"> • Time constraints on developing a coordination strategy will be established, displayed, and monitored by decision systems. • The DAA shall alert UAS decision systems when time remaining to accomplish collision avoidance maneuvers is low. • The DAA low time alert shall remain active until a maneuver is accomplished or manually acknowledged.
<p>8. Common Understanding.</p> <ul style="list-style-type: none"> • While aware of a collision scenario, the decision systems may have different understanding of the scenario severity and not prioritize developing a maneuver strategy. • At least one of the decision systems is unaware of a collision potential. 	<p>1, 2.1, 2.4, 2.6, 3, 4.1</p>	<ul style="list-style-type: none"> • Consider. Collision avoidance scenarios should use the same thresholds and severity alerts in training and in developing the DAA and CAS.
<p>9. Predictability.</p> <ul style="list-style-type: none"> • Temporal models may be inadequate for collision avoidance coordination, leading to coordination being too late. <ul style="list-style-type: none"> ○ (within DS) The DAA may not account for and have the ability to resolve aggressive maneuvering when in close proximity to other aircraft. The aggressive maneuvering may be from the UAS itself or other highly maneuverable aircraft such as fighters. 	<p>1, 2.1, 2.4, 2.6, 3, 4.1</p>	<ul style="list-style-type: none"> • The DAA shall include temporal factors such as: <ul style="list-style-type: none"> ○ Time to impact or closet point of approach. ○ Time to maneuver to collision free zone. ○ Time for aircraft to respond maneuver input. ○ When aircrew have decision authority, model decisions and action response times. ○ When in cooperation with

Table 26. STPA-Coordination, UAS Decision System Lateral Coordination

Hazardous Lateral Coordination Scenarios	UCA	Recommendations and Considerations
<ul style="list-style-type: none"> ▪ Note. The latest TCAS II logic uses straight line and no acceleration assumptions (M.J. Kochenderfer et al. 2010). ▪ Vertical maneuvers may not be adequately accounted for. Aggressive vertical maneuvers may be observed when overflying military airspaces or during in-flight emergencies. ▪ Turning maneuvers by high performance aircraft such as fighters may be observed in terminal areas or when flying under VFR. 		<p>collision avoidance systems, the DAA shall account for all aircraft maneuvering. For example, to clear a separation bubble with two aircraft maneuvering takes roughly half the time as only one aircraft maneuvering.</p>

5.4.2.3 ATC and Aircraft Decision Systems Vertical Coordination Analysis

Vertical coordination by control methods is an interaction between ATC and UAS decision systems. The vertical coordination relationship is shown in Figure 25a. STPA-Coordination identified flawed vertical coordination scenarios between ATC and the UAS decision systems that may lead to UAS decision system UCAs identified in STPA step 1. Other aircraft decision systems were inherently analyzed in this vertical coordination problem also. Table 27 presents STPA-Coordination results for vertical coordination.

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<p>Flawed Coordination Case 1. Coordination Missing. Coordination missing between UAS decision system (a) and ATC (b), which may lead to UCAs</p>		
1. Coordination Goals. n/a	n/a	n/a
<p>2. Coordination Strategy. Missing</p> <ul style="list-style-type: none"> • ATC near real-time vertical coordination is one of several coordination strategies in the NAS. In some conditions, vertical coordination can be missing. Without coordination, ATC must treat the UAS as a dynamic and unpredictable environmental factor. ATC vertical 	<p>1, 2.1, 2.2, 2.4, 2.6, 3, 4</p>	<ul style="list-style-type: none"> • When ATC coordination by control is missing, there shall be a replacement comprehensive coordination strategy. <ul style="list-style-type: none"> ○ Lateral coordination between aircraft decision systems can replace vertical ATC control coordination.

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<p>coordination can be missing in at least two scenarios:</p> <ul style="list-style-type: none"> ○ UAS are assumed to fly under IFR. In Class G airspace, UAS may fly IFR without ATC control in current regulations. ○ UAS aircrew follow DAA alerts and maneuver guidance (RTCA SC-228 2014), which renders ATC vertical coordination missing. ○ Note. Current ATC policy related to TCAS states: “Once the responding aircraft has begun a maneuver in response to an RA, the controller is not responsible for providing standard separation between the aircraft that is responding to an RA and any other aircraft” (Federal Aviation Administration 2014a) p. 2-1-12. ATC policy may be the same for UAS responding to DAA guidance. 		<ul style="list-style-type: none"> ▪ (within DS) The DAA shall enable comprehensive lateral coordination as prescribed in part by this STPA-Coordination. ○ Coordination by standardization (i.e. rules and regulations) may assist in collision avoidance. There are potential concerns with coordination by standardization: flexibility, reliance on see-and-avoid and limited information integration. <ul style="list-style-type: none"> ▪ (within DS) The DAA maneuver guidance shall be coordinable by vertical coordination by standardization. In the current US NAS, DAA maneuver guidance shall be coordinable by CFR §91.113 and §91.115 Right of way rules. • If UAS is allowed to fly without ATC control, the UAS shall have self-observation capability at least commensurate with established visual requirement for in-situ pilots. • Consider. Automatic collision avoidance maneuvers should be required for aircraft that may fly without ATC coordination, such as military flight operations or flight operations in Class G airspace.
<p>5. Group Decision-Making. Missing</p> <ul style="list-style-type: none"> • Vertical group DM is missing in the following scenarios, which is a concern that involves more than ATC interactions with UAS. <ul style="list-style-type: none"> ○ Aircraft flying under VFR in the same shared airspace as UAS and not in 	<p>1, 2.1, 2.2, 2.4, 2.6, 3, 4</p>	<ul style="list-style-type: none"> • Consider. Aircraft that fly where ATC services exist shall be under ATC control to assist in safe coordination efforts.

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<ul style="list-style-type: none"> communications with ATC. ○ UAS aircraft flying IFR in class G airspace. 		
<p>Flawed Coordination Case 2. Coordination Inadequate. Coordination is inadequate between UAS decision system (a) and ATC (b), which may lead to UCAs.</p>		
<p>1. Coordination Goals. Safety as a primary goal may diverge with time and prioritize efficiency in traffic. Goal divergence can be a problem when unsafe ATC coordination is followed or safe coordination is not followed by UAS decision systems. Goal divergence may occur due to:</p> <ul style="list-style-type: none"> • ATC familiarity with task and environment may foster a belief that they can push the traffic scenarios tighter, but are not able to handle the induced workload or an unusual event. • External pressures on ATC to increase traffic flow beyond individual comfort levels. • UAS aircrew mission accomplishment goals may cause safety goal divergence. 	<p>1, 2, 3, 4</p>	<ul style="list-style-type: none"> • FAA management and leadership shall ensure collision avoidance is a top priority goal. • Training shall ensure human decision systems can meet the expected workload demand in off-nominal conditions, both ATC and aircrew.
<p>2. Coordination Strategy.</p> <ul style="list-style-type: none"> • In current regulations, coordination by control strategy can be ambiguous. There are scenarios where ATC is unsure if they are directing traffic or not. This ambiguity comes at exactly the time clarity is needed—safety-critical outcome in time-pressured and high workload scenarios. The potential for coordination strategy ambiguity in ATC policy is highlighted in the following excerpt: ATC continues to provide control instructions unless aircraft “informs you that it is responding to a TCAS Resolution Advisory.” (Federal Aviation Administration 2014a) p. 2-1-12. <i>Unless informed</i> is a safety concern for UAS operations: <ul style="list-style-type: none"> ○ There is reliance on distressed aircrew to clearly communicate intentions in a 	<p>1, 2.1, 2.2, 2.4, 2.6, 3, 4</p>	<ul style="list-style-type: none"> • ATC coordination by control shall be unambiguous when alternative coordination strategies exist. <ul style="list-style-type: none"> ○ Vertical coordination shall establish adequate accountability in (near) real-time when ATC is responsible for collision avoidance. ○ ATC shall have (near) real-time information on what aircraft decision systems are involved in collision scenarios. • (within DS) To minimize control coordination ambiguity during a collision scenario, the UAS/DAA decision system shall provide ATC with the following as a minimum: <ul style="list-style-type: none"> ○ UAS decision system intentions discussed in <i>enabling conditions</i>

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<p>timely manner. Under such life or death conditions, communications may not occur and ATC continues its instruction.</p> <ul style="list-style-type: none"> ○ If communication did occur, ATC may not receive information. The transmission may not be calm and collected. ATC may continue instruction on the affected UAS or ignore the wrong aircraft. 		<p>previous Table 26. Providing intention information confirms for ATC that lateral coordination between aircraft is in effect.</p>
<p>3. Decision Systems. Inadequate ATC ability and potentially within DS ATC coordination may lead to UCAs.</p> <ul style="list-style-type: none"> • ATC may not be able to handle the workload and time pressure demands needed to control during collision scenarios involving UAS/DAA. • (within DS) ATC instructor/trainer coordination may be inadequate for the coordination by control responsibility. 	<p>1, 2.1, 2.2, 2.3, 2.4, 2.6, 3, 4</p>	<ul style="list-style-type: none"> • ATC shall establish training certification programs for collision avoidance scenarios to include additional UAS/DAA concerns. Some concerns include: <ul style="list-style-type: none"> ○ Remote pilot visual limitations. ○ Communication delays. ○ Limitations in coordination between UAS decision systems, in part established by this STPA-Coordination.
<p>4. Communications</p> <ul style="list-style-type: none"> • Verbal communication channels may be interrupted and not allow information to pass between ATC and UAS decision systems, which may lead to UCAs: <ul style="list-style-type: none"> ○ UAS maneuvering may block line-of-sight communications. ○ External electronic jamming. ○ Internal electromagnetic interference. ○ Failure or degradation of transmit/receive communications equipment. • Single voice communication channels may be in use during time needed to communicate with aircrew in an impending separation violation. Scenarios of high radio communication traffic loads are perhaps more susceptible to this bandwidth limitation, such as during terminal area operations. 	<p>1, 2.1, 2.2, 2.3, 2.4, 2.6, 3, 4.2</p>	<ul style="list-style-type: none"> • The UAS maneuver algorithms shall account for communication limitations and constraints between remote aircrew, UAS, and ATC to ensure uninterrupted communications. • Power, non-interference, and reliability shall be confirmed adequate for communications. • UAS decision systems shall be alerted in (near) real-time when vertical ATC coordination is interrupted. If in or near a collision scenario, aircraft decision systems shall transfer to a lateral coordination strategy. • Consider. An alternative digital communication channel shall exist for ATC-UAS communications, especially in high-density radio traffic environments. • Vertical coordination shall account for

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<ul style="list-style-type: none"> Communication time delays between ATC and remote UAS aircrew may be inadequate for time-critical scenarios. With seconds in delays for transmit and receipt of information, coordination of multiple aircraft for collision avoidance may not be possible inside a time threshold. 		<p>communication time delays in collision avoidance maneuvers.</p> <ul style="list-style-type: none"> Means to measure communication time delays shall be established. ATC and UAS decision systems shall have feedback on communication time delays. Considerations include: <ul style="list-style-type: none"> Calculate and display in real-time communication delays. Only alert decision systems when delays exceed nominal thresholds. (DAA) If DAA is coordinable, the DAA maneuver algorithm shall account for known or predicted communication time delays from ATC instructions.
<p>5. Group Decision-Making. Vertical coordination group DM verbal protocols are adequate. Group DM occurs with a request or instruction that is followed by confirmation of approval or acknowledgment, respectively.</p> <ul style="list-style-type: none"> Group DM by digital means may have inadequate protocols for negotiation of UAS aircrew requests during a time-critical collision avoidance scenario. 	<p>1, 2.1, 2.2, 2.3, 2.4, 2.6, 3</p>	<ul style="list-style-type: none"> Consider. The use of digital means for vertical coordination during collision avoidance scenarios. <ul style="list-style-type: none"> Digital means can send a coordinated maneuver strategy to all decision systems at one time, benefitting common understanding. UAS and aircraft decision systems shall have means to quickly respond in agreement. UAS and aircraft decision systems shall have means to quickly negotiate another acceptable maneuver with ATC should one be deemed necessary.
<p>6. Observation of Common Objects. Observation of common objects may be inadequate, which may</p>	<p>1, 2.1, 2.2,</p>	<ul style="list-style-type: none"> ATC shall provide safety alerts that inform UAS aircrew on the bearing, range, and altitude of collision factor

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<p>lead to UCAs.</p> <ul style="list-style-type: none"> • ATC may observe more objects than individual aircrew having primary and secondary radars. While technologies such as ADS-B are improving observation of objects for aircrew, this technology is not currently ubiquitous. <ul style="list-style-type: none"> ○ In cases where ATC observes airborne objects not observed by aircraft decision systems, the aircrew may not follow ATC instructions when separation violation imminent. • (within DS) DAA observe different objects than the aircrew and ATC. <ul style="list-style-type: none"> ○ Collision trajectory airborne object not observed by DAA. The DAA does not alert nor provide maneuver guidance when a collision scenario is present. If ATC provides required collision avoidance guidance, it may not be received by UAS aircrew as a time-critical and severe situation. ○ Different objects observed by the DAA and provide maneuver guidance not consistent with ATC. With inconsistent and possibly conflicting maneuver guidance, the coordinated action (i.e. the safe action) is unknown by the UAS aircrew. • ATC observation update rates may be inadequate (not necessarily the physical equipment). This may occur during slow or routine enroute navigation flight phases. Equipment malfunction may send UAS off flight plan or instruction, and ATC may not catch in time. 	<p>2.3, 2.4, 2.6, 3, 4.2</p>	<p>airborne objects.</p> <ul style="list-style-type: none"> • ATC shall continue to update aircrew on factor traffic until aircrew acknowledges visual. • UAS aircrew shall acknowledge visual of airborne objects, or request another point out if there is a discrepancy. • UAS aircrew shall know DAA observation limitations against air and ground obstacles encountered during flight operations. • The DAA shall observe or have information on the same objects observed by other decision systems. The technology to send and receive digital information exists in many domains. <ul style="list-style-type: none"> ○ Objects observed by ATC and nearby traffic shall be relayed to the UAS decision system. ○ Consider. Digital means shall be used to assist visual acquisition of ATC safety alert point out. For example, digitally outline obstacles in UAS electro-optic displays that ATC designates. ○ The DAA shall alert UAS aircrew when a discrepancy exists in the display of common objects. This will assist in seeking information and in making decisions. A message check sum or equipment status message may be used determine a discrepancy exists. • ATC shall have adequate observation update rates commensurate with proximity of UAS to other aircraft and active special use airspaces. UAS may experience lost link or other loss of control requiring ATC assistance.
<p>7. Authority, Responsibility, Accountability.</p>	<p>1,</p>	<ul style="list-style-type: none"> • Given lateral coordination

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<p>Authority and Responsibility. While ATC has clear authority to coordinate UAS IFR traffic within their airspace, responsibility to do so can be ambiguous in the following scenarios:</p> <ul style="list-style-type: none"> • When the DAA self-separation or collision avoidance maneuver response is complete, the UAS decision system may: <ul style="list-style-type: none"> ○ Forget to establish coordination under ATC control after the collision scenario and ATC believes they have control. ○ (within DS) Believe they are under ATC control because they made a radio call, but ATC did not receive the maneuver complete information and does not provide separation services. ○ (within DS) The DAA does not broadcast maneuver complete or collision avoidance scenario complete to UAS aircrew and ATC. • (within DS) The DAA alerts and maneuver guidance may be displayed to ATC. The DAA guidance does not equal accountability, however. ATC may stop providing control to aircrew, when aircrew did not intend to follow DAA guidance. <ul style="list-style-type: none"> ○ Note. A comparable scenario exists with TCAS RAs. TCAS RA information is provided to ATC in some international countries, which has professional ATC organizations concerned (Beadle 2010). ○ Note. As an analogy, how often do pilots follow TCAS RAs? The numbers suggest not that often. A 2012 FAA presentation (slide 20) showed data suggesting that pilots do not respond to TCAS climb/descend RAs approximately 30-50% of the time in altitude bands 2-18k feet. In altitude 	<p>2.1, 2.5, 2.6, 3, 4</p>	<p>recommendations above in Table 26, accountability between ATC and aircrew shall be established:</p> <ul style="list-style-type: none"> ○ ATC-UAS accountability shall include strategy in use (i.e. vertical or lateral coordination) and planned maneuver to benefit predictability and common understanding of the scenario. ○ The DAA shall send accountability information to ATC. The digital message protocol shall include as minimum: <ul style="list-style-type: none"> ▪ Confirmation of lateral coordination strategy in use. ▪ UAS and aircraft involved in scenario. ▪ Collision avoidance maneuver intentions. ▪ Updates on maneuver implementation. ▪ Completion of separation and collision scenario indicating when maneuvers may cease. ○ Aircrew shall have methods to confirm the use of lateral coordination strategy with ATC. In other words, aircrew will confirm with ATC that they are no longer under their coordination by control. ○ The DAA shall provide UAS aircrew with simple and error resistant means to confirm with ATC that lateral coordination strategy in use, such as a button push on the flight controls. During time-critical situations,

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<p>bands below 2k and above 18k, the non-response rate increases to 70-80% (Gallo & Tillotson 2012). Non-response and opposite response numbers were also found in analysis of Boston area climb RAs during 2005-2006 (Kuchar & Drumm 2007).</p> <ul style="list-style-type: none"> • (within DS) DAA guidance or alerts may be spurious. For example, ATC may receive DAA alerts that are not displayed to the correlated UAS aircrew. <ul style="list-style-type: none"> ○ Note. A comparable scenario may occur with a TCAS RA. Spurious RAs may be displayed on ATC consoles that are not displayed in the corresponding aircraft. Spurious TCAS RAs is a concern expressed by IFATCA (International Federation of Air Traffic Controllers' Associations). (Beadle 2010) <p>Accountability. In certain scenarios, accountability is not established in the current strategy between ATC-UAS decision systems when the DAA (or any collision avoidance system) is active. ATC may give unnecessary maneuver instructions (i.e. an efficiency or nuisance concern). Perhaps worse, ATC may give instruction that leads to UCAs (i.e. a safety concern). Some examples of inadequate accountability include:</p> <ul style="list-style-type: none"> • Aircrew do not relay to ATC alternative maneuver intentions in response to DAA guidance. Thus, ATC continues to provide instruction to aircrew involved in the separation scenario. ATC may provide instruction with greater amplification and stress given the scenario and being ignored. In doing so, doubts about what maneuvers each decision system is following may persist. • Aircrew clearly and accurately state intentions 		<p>the ability to quickly and accurately relay accountability information to ATC is critical.</p> <ul style="list-style-type: none"> ○ The DAA shall eliminate or mitigate spurious signals that may be interpreted as an alert by ATC when there is none. ○ Consider. Filter spurious DAA alert signals at the ATC receiving end if spurious DAA signals cannot be eliminated. ○ ATC shall confirm receipt of accountability information from aircraft decision systems. Verbal or digital confirmation may suffice. <ul style="list-style-type: none"> ▪ ATC shall confirm receipt of collision avoidance completion. ▪ (within DS) The DAA shall continue to send maneuver completion message until acknowledged by ATC. ATC acknowledgment confirms that ATC coordination is again the coordination strategy. <ul style="list-style-type: none"> • The DAA shall be vertically coordinable by ATC control instruction. Being coordinable means DAA can be part of a vertical coordination solution by ensuring that ATC guidance is integrated into the maneuver guidance. It should be a rare occurrence for ATC and the DAA to provide conflicting guidance when ATC provides maneuver instructions first. <ul style="list-style-type: none"> ○ Note. The technology for digital communication already exists in military tactical aviation domains using Link 16 protocols. In the

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<p>to ATC that they are following DAA guidance, but ATC does not receive or understand aircrew proclamation. ATC continues to provide instructions to UAS or other aircraft.</p> <ul style="list-style-type: none"> • (within DS) Accountability. Missing coordinability. The DAA is not coordinable by ATC vertical coordination strategy. <ul style="list-style-type: none"> ○ The DAA is not coordinable by ATC control coordination. In other words, the DAA decisions cannot be influenced by ATC. If the DAA cannot accept ATC coordination as a decision input, there is potential for conflicting collision avoidance maneuver actions that aircrew must ultimately resolve in current ConOps as they have the decision authority and responsibility. The conflict in control actions from the DAA decision component and ATC may lead to UCAs. ○ [air traffic management coordination] The DAA is not coordinable by standardization, specifically CFR §91.113 and §91.115 Right of way rules. 		<p>US NAS, one of the top four Next Generation initiatives is the development and integration of digital communications between ATC and aircrew, also known as “Data Communications” (FAA 2016). The Data Communications concept has been tested in early development trials.</p> <ul style="list-style-type: none"> • Consider. CAS in general shall be vertically coordinable by ATC and vertical standardization. (DAA coordinable by vertical standardization discussed in Flawed Coordination Case 1)
<p>8. Common Understanding. Where there is discrepancy in common understanding between ATC and aircrew, individual decisions may diverge. A mismatch in common understanding may lead to UCAs.</p> <ul style="list-style-type: none"> • An otherwise safe ATC coordination instruction may not be followed by individual UAS decision systems. • Aircrew may delay or question ATC intentions when an impending separation violation or collision is not known or severity of situation is not obvious. • Aircrew may unintentionally ignore 	<p>1, 2.1, 2.5, 2.6, 3, 4</p>	<ul style="list-style-type: none"> • ATC shall emphasize separation or collision scenario in communications with UAS decision systems to assist common understanding of the situation severity. As an example, “Traffic, your nose, 1 mile, turn right 360, climb 10k feet.” The emphasis by ATC is critical in today’s NAS where aircraft equipment differences are allowed to exist that lead to information divergence. • Consider. Communications shall be on one frequency for high density traffic operations to assist in communications

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<p>instructions as they are not expecting them.</p> <p>Inadequate common understanding may result from the following scenarios:</p> <ul style="list-style-type: none"> • Aircrew can communicate with ATC on UHF and VHF frequencies, which is a common difference between civilian and military flight operations. Thus, while ATC receives verbal information from aircrew, the aircraft decision systems do not receive the same information. Common understanding between ATC and aircrew may be inadequate. ATC may be attempting to reconcile an impending separation violation scenario, but aircraft decision systems are not aware of ATC intentions. • ATC receives additional information than aircraft decision systems from its primary and secondary radars and other systems (e.g. ADS-B). ATC may be responding to an impending separation violation with this information, while aircraft decision systems are not aware of the situation. • (within DS) The DAA does not have the same information as ATC and does not perceive an impending separation violation at all. • (within DS) The DAA fails or degrades. 		<p>(e.g. not stepping on other transmissions) and common understanding.</p> <ul style="list-style-type: none"> • Consider. Compatible information sharing technology shall be mandatory for aircraft in certain shared airspaces, both receive and transmit. The technology exists to send and receive information. • (redundant with lateral coordination) The DAA shall meet minimum reliability requirements. • The DAA shall alert UAS aircrew of degradation where information is uncertain. • The UAS decision system shall relay loss of DAA capability to ATC, like for other IFR equipment failures. • Consider. DAA shall automatically relay failure or degradation to ATC.
<p>9. Predictability.</p> <p>When ATC and aircrew are operating under coordination by control in nominal conditions, there is arguably adequate predictability. Intentions are expressed through flight plans and requests. Standard departure, approach, and landing procedures assist predictability between ATC and aircrew. However, when the DAA issues an alert and maneuver guidance to UAS aircrew, coordination predictability may degrade to a point where ATC instruction or lack of instruction may lead to UCAs. Vertical coordination scenarios that</p>	<p>1, 2.1, 2.5, 2.6, 3, 4</p>	<ul style="list-style-type: none"> • UAS decision systems shall provide ATC with maneuver intentions before and after a collision avoidance maneuver. Intentions may be provided by: <ul style="list-style-type: none"> ○ Aircrew through verbal communication channels. ○ Aircrew through digital communication channels. ○ DAA through digital communication channels, perhaps as an automatic response to DAA derived maneuvers.

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<p>can influence predictability include:</p> <ul style="list-style-type: none"> • ATC does not know if aircrew are responding to ATC control strategy or not, which hinders predictability when UAS aircrew are not following ATC. ATC may not be aware of the DAA alert because: <ul style="list-style-type: none"> ○ The DAA responding aircrew do not communicate status. Aircrew may not communicate intentions because they are correctly prioritizing their efforts and time with aviate and navigate duties to keep themselves and passengers alive—communications is the last priority in aviation (i.e. aviate, navigate, communicate). ○ The DAA responding aircrew expresses intent, but is not understood to ATC. ○ Communication interruptions during transmission or reception. ○ (within DS) DAA alert and guidance information is not provided to ATC. When a collision scenario is forming and ATC does not catch it given their techniques and tools, not receiving a DAA alert may be a lost opportunity to resolve the impending problem. • ATC is aware of a DAA alert and correlated maneuvering aircraft, but maneuver guidance and cooperation information is not received by design or other factor. In this scenario, ATC is still obligated to provide maneuver instructions. The instructions may be opposite to or in conflict with the DAA alert and guidance. • ATC is not aware of aircrew maneuver strategy. Even if ATC received UAS DAA alerts, the intention is not received. <ul style="list-style-type: none"> ○ Will the aircrew follow DAA guidance and its assumptions in part or in 		<ul style="list-style-type: none"> • Under lateral coordination, the DAA/CAS shall provide aircraft system state information to ATC for additional means to correlate aircraft in a collision scenario. • ATC shall receive DAA alerts for informational purposes and to improve coordination predictability. Receiving DAA alerts gives ATC information to predict which aircraft may maneuver and when (i.e. soon) the maneuver may occur. Receiving DAA alerts puts all decision systems on notice and helps focus attention where and when it may be needed. • ATC shall be trained in expected UAS performance characteristics that affect maneuver response. • Consider. Maneuver category (e.g. high, medium, or low) information shall be available for ATC to assimilate in developing coordination maneuver strategy. <ul style="list-style-type: none"> ○ The maneuver category information can come from: <ul style="list-style-type: none"> ▪ The DAA shall transmit UAS maneuver performance. ▪ Flight planning processes gathers UAS maneuver category information and relays it to ATC.

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<p>whole?</p> <ul style="list-style-type: none"> ○ Will aircrew ignore DAA? ○ Or, will aircrew perform a maneuver in the opposite sense as suggested by the DAA? <ul style="list-style-type: none"> ● ATC does not have appropriate UAS performance models to predict response to maneuver instructions. 		
<p>Flawed Coordination Case 3. Coordination Strategy Leads to Hazard. The ATC-Aircrew coordination may lead to UCAs.</p>		
<p>1. Coordination Goals. n/a</p> <p>Note. ATC and aircrew share a primary goal of collision avoidance.</p>	n/a	n/a
<p>2. Coordination Strategy. UAS decision systems may invoke a set of rules to make individual maneuver decisions while in shared airspace. In such scenarios, ATC coordination strategy may lead to UCAs.</p> <ul style="list-style-type: none"> ● Infeasible: ATC gives instructions that are not feasible given constraints. <ul style="list-style-type: none"> ○ Decision system response time (decision and action times) inadequately accounted for in maneuver instruction. <ul style="list-style-type: none"> ▪ Maneuver instruction given too late and followed by aircraft decision system. ▪ Maneuver instruction stopped too late for system response capabilities. ● Unacceptable: ATC gives instruction that is followed leading to an unsafe outcome. <ul style="list-style-type: none"> ○ (within DS) ATC provides instruction to UAS that is in conflict with DAA suggested maneuver. This is a problem should the UAS aircrew follow ATC when the DAA maneuver was in cooperation with another collision 	1, 2.1, 2.2, 2.3, 2.4, 2.6, 3, 4	<ul style="list-style-type: none"> ● (redundant) Only one coordination strategy shall be followed at a time, IAW the coordination framework axiom [3.2]. ● (redundant) ATC shall receive UAS intent information. ● Consider. A priority matrix for collision avoidance maneuver strategy shall be used. I suggest a priority matrix based on comprehensive coordination or not, shown in Table 28. Higher priority should be with comprehensive lateral coordination for the following reasons: <ul style="list-style-type: none"> ○ Coordination between UAS and other aircraft decision systems has the most direct influence on the physical process outcome. ○ In a two aircraft collision scenario, lateral coordination has less communication interactions than vertical coordination: two communication links versus four with ATC. ○ Aircraft under ATC should not get so close to collision potential, thus something may have went wrong with vertical coordination.

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations													
<p>avoidance system.</p> <ul style="list-style-type: none"> ○ ATC provides coordinated maneuvers that inadequately account for time or decision system response. <ul style="list-style-type: none"> ▪ Instruction was given too late for UAS response capability to avoid the separation violation. ▪ Instruction was stopped too soon and the aircraft are still in a collision potential. ▪ Instruction was inadvertently too much leading to other hazards. ○ ATC provides coordinated maneuver that instructs one or more aircraft to maneuver unsafely: <ul style="list-style-type: none"> ▪ Towards the terrain. ▪ Towards additional airborne objects. 		<p>Table 28. Collision Avoidance Coordination Strategy Priority Matrix</p> <table border="1" data-bbox="915 411 1403 709"> <thead> <tr> <th colspan="2" rowspan="2"></th> <th colspan="2">Lateral Coordination</th> </tr> <tr> <th><i>Adequ</i></th> <th><i>Inadequate</i></th> </tr> </thead> <tbody> <tr> <th rowspan="2" style="writing-mode: vertical-rl; transform: rotate(180deg);">Vertical Coord</th> <th><i>Adequ</i></th> <td>Lateral</td> <td>Vertical</td> </tr> <tr> <th><i>Inadequate</i></th> <td>Lateral</td> <td>Independent actions, not coordination</td> </tr> </tbody> </table> <ul style="list-style-type: none"> • Consider. ATC shall have collision avoidance automation similar to DAA/CAS to assist in time-critical situations. The difference from aircraft decision system DAA/CAS would be greater time safety margins. Keeping safe vertical coordination may be preferred to DAA/CAS time-critical collision avoidance scenarios. • The UAS and aircraft decision systems shall revert to adequate lateral coordination should vertical coordination not work (discussed previously as layered coordination). • ATC shall have terrain information as an input to developing a coordination maneuver strategy. • The DAA/CAS shall alert UAS aircrew for potential terrain concerns. • If the DAA is coordinable by ATC, the DAA shall evaluate airborne objects and terrain in the maneuver strategy and suggest alternatives when either is a collision concern for the ATC-derived maneuver coordination strategy. 			Lateral Coordination		<i>Adequ</i>	<i>Inadequate</i>	Vertical Coord	<i>Adequ</i>	Lateral	Vertical	<i>Inadequate</i>	Lateral	Independent actions, not coordination
		Lateral Coordination													
		<i>Adequ</i>	<i>Inadequate</i>												
Vertical Coord	<i>Adequ</i>	Lateral	Vertical												
	<i>Inadequate</i>	Lateral	Independent actions, not coordination												
<p>Flawed Coordination Case 4. Coordination Strategy Established Late. Aircrew-ATC coordination is established late, which may lead to UCAs.</p>															
1. Coordination Goals. n/a	n/a	n/a													

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
<p>2. Coordination Strategy.</p> <ul style="list-style-type: none"> • ATC develops a collision avoidance maneuver strategy too late to influence the outcome. <ul style="list-style-type: none"> ○ Unaware of scenario due to: <ul style="list-style-type: none"> ▪ Observation systems degrade or fail. ▪ Distracted by extraneous concerns. ○ ATC pushes the safe envelope in efforts to improve efficiency (e.g. aircraft volume moved). ○ (within DS) ATC collision awareness systems are ignored. ○ (within DS) ATC collision awareness systems are inadequate. 	<p>1, 2.1, 2.2, 2.4, 2.6, 3, 4</p>	<ul style="list-style-type: none"> • The UAS decision system shall know when ATC coordination can no longer influence a collision outcome and should revert to an alternative coordination strategy. <ul style="list-style-type: none"> ○ (DAA) Consider. The DAA shall alert UAS aircrew when ATC coordination can no longer influence the outcome and to use an alternative strategy. This alert may correspond with cooperative maneuver guidance. For example, 15 seconds might be deemed the minimum time needed to coordinate two aircraft for the current collision. At this point, lateral coordination and DAA guidance may be recommended to aircrew. The ATC coordination time is in addition to the time required to maneuver for collision avoidance. ○ (DAA) Consider. An ATC CAS should alert ATC when vertical coordination efforts can no longer influence the current outcome, which may be the DAA or in cooperation with the DAA.
<p>3. Decision Systems.</p> <ul style="list-style-type: none"> • ATC has inadequate mental capacity for current workload, such as during emergencies and off-nominal, and cannot develop a plan in time. 	<p>1, 2.1, 2.2, 2.4, 2.6, 3, 4</p>	<ul style="list-style-type: none"> • ATC workload shall have adequate safety margin to account for off-nominal conditions.
<p>4. Communications.</p> <ul style="list-style-type: none"> • ATC does not account for communication delays associated with UAS operations. Potential worst case communication delays may be with collision scenario aircraft all 	<p>1, 2.1, 2.2, 2.4, 2.6, 3</p>	<ul style="list-style-type: none"> • In vertical coordination, communication delays shall be accounted for in determining when ATC must begin coordination.

Table 27. STPA-Coordination, ATC and UAS/Aircraft Vertical Coordination

Vertical Coordination Hazardous Scenarios	UCA	Recommendations and Considerations
UAS. In this case, the delays may add up to a significant time delay.		
5. Group Decision-Making. <ul style="list-style-type: none"> • ATC is not directive in nature and group DM takes too long for the scenario. 	1, 2.1, 2.2, 2.4, 2.6, 3	<ul style="list-style-type: none"> • In a collision avoidance scenario, ATC shall be directive in coordination.
6. Observations of Common Objects. n/a	n/a	n/a
7. Authority, Responsibility, Accountability. <ul style="list-style-type: none"> • Authority and Responsibility. n/a • Accountability. <ul style="list-style-type: none"> ○ ATC is not monitoring time constraints in the collision scenario, incorrectly prioritizing other functions. 	1, 2.1, 2.2, 2.4, 2.6, 3	<ul style="list-style-type: none"> • ATC shall be alerted with increasing severity based on time remaining to having no influence.
8. Common Understanding. <ul style="list-style-type: none"> • The time remaining for ATC coordination of two or more aircraft in a collision scenario is not understood by all decision systems. If ATC alone is aware of time remaining, aircrew may not correctly prioritize assisting vertical coordination with listening and responding to maneuver instructions for example. 	1, 2.1, 2.2, 2.4, 3	<ul style="list-style-type: none"> • ATC and aircraft decision systems shall have common understanding of time remaining for engaging in and following ATC coordination instructions.
9. Predictability. <ul style="list-style-type: none"> • ATC is aware of the collision scenario, but does not know time constraints for maneuver strategy development. 	1, 2.1, 2.4, 3	<ul style="list-style-type: none"> • A decision threshold metric shall be established for ATC to develop a separation/collision avoidance coordination strategy and implement it. • ATC shall be given information on the time remaining for coordination strategy development.

5.4.3 STPA-Coordination Frequency Analysis

A descriptive frequency analysis was conducted on the STPA-Coordination results. The frequency analysis counted unique hazardous coordination scenarios and recommendations. The frequency analysis of qualitative data was a manual process and thus inherently subjective. As such, STPA-Coordination quantitative results should be considered approximate; place more emphasis on the data trends and

qualitative observations as they are perhaps more insightful than the absolute numbers. See APPENDIX C. STPA-Coordination Frequency Analysis for further details.

5.4.3.1 Hazardous Scenario Count, Coordination Related

The hazardous scenario count derived from STPA-Coordination is shown in Table 29. Figure 27 graphically represents the combined data. Both representations decompose STPA-Coordination hazardous scenario count by flawed coordination cases and coordination elements.

Observations in the frequency analysis, Table 29 and Figure 27, include:

- There were ~194 unique hazardous coordination scenarios derived using STPA-Coordination.
- Overall, hazardous scenarios were identified for each flawed coordination case and coordination element.
- Flawed Coordination Case 2 (inadequate) represented 73% of the scenarios with 142 identified.
- Coordination elements 2 (strategy) and 8 (common understanding) were most frequent, each representing 24% of the scenarios.

Table 29. STPA-Coordination Hazardous Scenario Count

		Flawed Coordination Cases								Coordination Element Count		
		1. Missing		2. Inadequate		3. Lds to Hazard		4. Late		Lateral	Vertical	Total
		Lateral	Vertical	Lateral	Vertical	Lateral	Vertical	Lateral	Vertical			
Coordination Elements: Missing or Inadequate	1. Coordination Goals	0	0	0	3	0	0	0	0	0	3	3
	2. Coordination Strategy	0	2	12	2	14	8	3	5	29	17	46
	3. Decision Systems	x	x	0	2	x	x	0	1	0	3	3
	4. Communications	x	x	8	6	x	x	1	1	9	7	16
	5. Group Decision-Making	0	2	5	1	x	x	3	1	8	4	12
	6. Observation of Common Objects	x	x	13	4	x	x	1	0	14	4	18
	7. Authority, Responsibility, Accountability	x	x	10	9	x	x	3	1	13	10	23
	8. Common Understanding	x	x	36	7	x	x	2	1	38	8	46
	9. Predictability	x	x	15	9	x	x	2	1	17	10	27
Hazardous Coord Scenario Count		0	4	99	43	14	8	15	11	128	66	
		4		142		22		26		Total Count		194

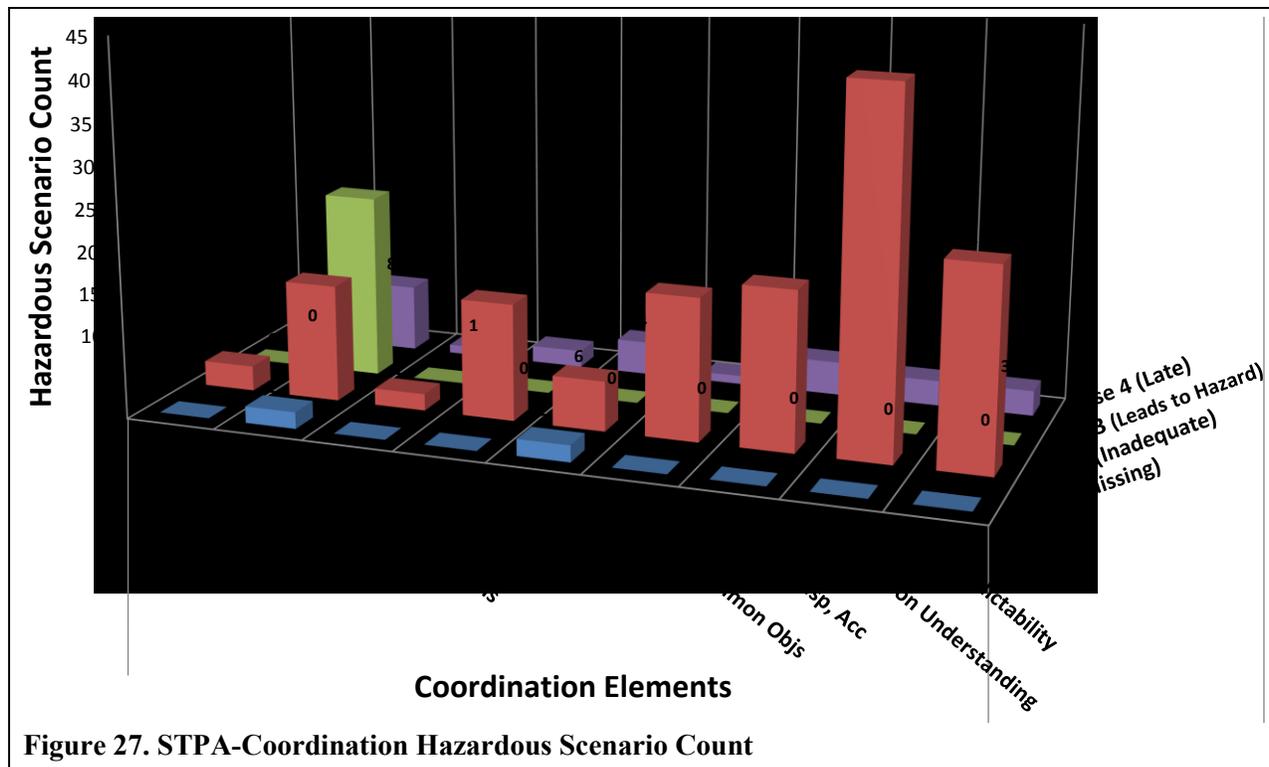


Figure 27. STPA-Coordination Hazardous Scenario Count

Table 30. DAA-Related Hazardous Coordination Scenario Count

Coordination Elements	DAA-Related Hazardous Coordination Scenario Count		
	Lateral Coordination	Vertical Coordination	Total Hazardous Scenarios (DAA)
1. Coordination Goals	0	0	0
2. Coordination Strategy	17	1	18
3. Decision Systems	0	0	0
4. Communications	3	0	3
5. Group DM	2	0	2
6. Observation of Common Objects	9	2	11
7. ARA	5	5	10
8. Common Understanding	23	2	25
9. Predictability	12	5	17
Total Hazardous Coord Scenarios	71	15	86

The DAA unique scenarios are a subset of the overall data, shown in Table 30; observations include:

- Roughly 44% of the overall hazardous coordination scenarios were DAA-related (86 of 194). This reflected the STPA-Coordination focus on within UAS decision system coordination, including the UAS aircrew and the DAA decision components.
- Common understanding was the most frequent coordination element of the DAA hazardous scenarios at 29%, 25 of the 86.

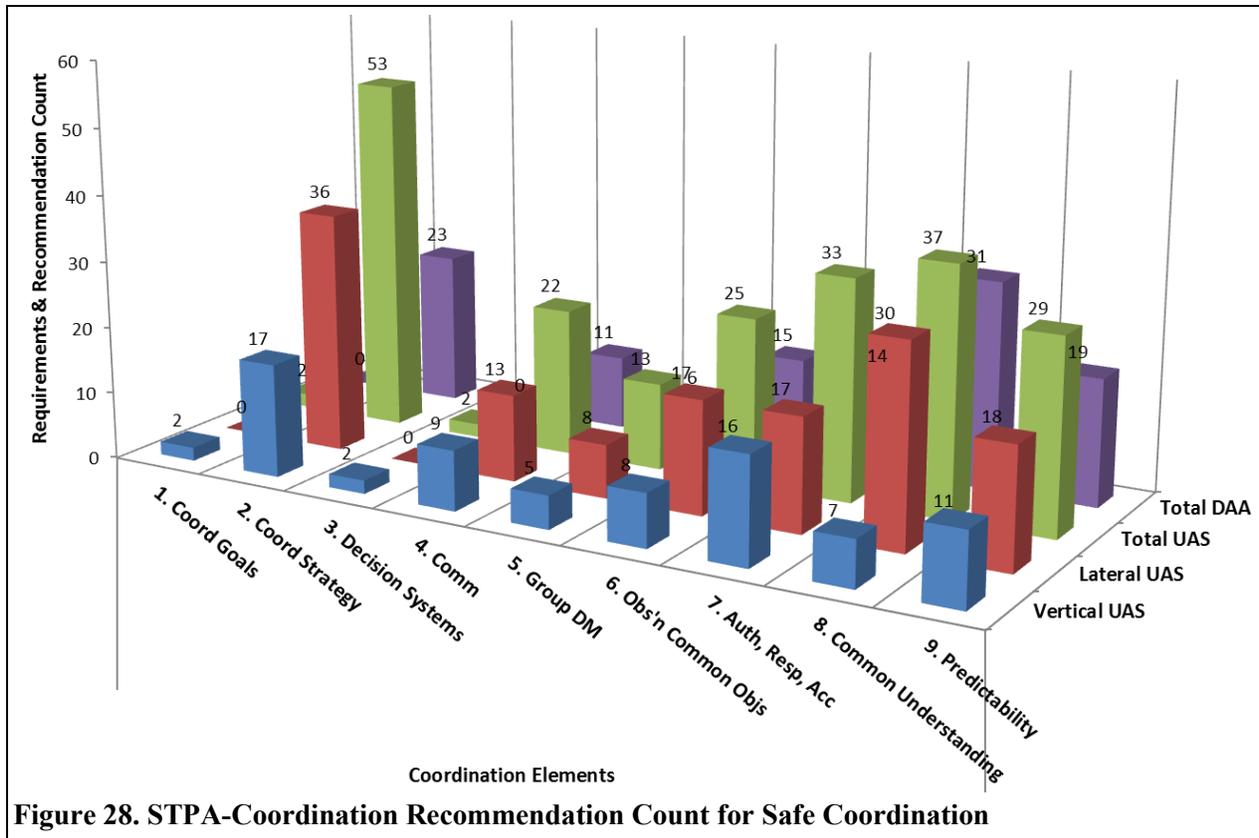
5.4.3.2 Coordination Recommendations and Requirements

Along with the hazardous scenarios are the related safety recommendations, including requirements. A frequency analysis of the recommendations was conducted and summarized in Table 31 and Figure 28. Observations from Table 31 and Figure 28 include:

- There were ~216 unique recommendations derived using STPA-Coordination, which related coordination within and between decision systems for safe coordination between the UAS decision system and other decision systems.
- 55% of the recommendations (119 of 216) were applicable to the design of the DAA, which reflected the focus of inquiry.
- Coordination strategy and common understanding recommendations were the top two frequency counts. Coordination strategy accounted for nearly 25% of the recommendations.

Table 31. STPA-Coordination, Recommendation Count for Safe Coordination

Coordination Elements	STPA-Coordination Recommendation Count					
	Lateral Coordination		Vertical Coordination		Total Coordination	
	UAS DS	DAA	UAS DS	DAA	UAS DS	DAA
1. Coordination Goals	0	0	2	0	2	0
2. Coordination Strategy	36	15	17	8	53	23
3. Decision Systems	0	0	2	0	2	0
4. Communications	13	5	9	6	22	11
5. Group Decision-Making	8	4	5	2	13	6
6. Obs'n of Common Objs	17	12	8	3	25	15
7. ARA	17	5	16	9	33	14
8. Common Understanding	30	28	7	3	37	31
9. Predictability	18	15	11	4	29	19
Total Recommendations	139	84	77	35	216	119



5.5 STPA-Coordination Results Comparison with Previous Work

Formal standards development and safety analysis efforts for UAS integration in the US have been ongoing since at least 2004 with the formation of RTCA SC-203. In 2013, SC-203 disbanded and a new group SC-228 stood up. Whereas SC-203 had UAS as its scope, SC-228 reduced the scope to the DAA and C2 (command and control). Safety analysis was accomplished by SC-203 and published in two volumes of DO-344 (RTCA SC-203 2013a; RTCA SC-203 2013b). While SC-228 efforts are ongoing, the initial Safety Working Group was disbanded late 2015. It is reasonable to deduce the analysis of UAS integration safety is a challenge.

To evaluate the utility of STPA-Coordination, it was compared to the SC-203 safety analysis efforts related to UAS integration. There were two primary reasons for this choice. First, SC-203 had a larger scope than SC-228, which was the UAS versus DAA respectively. This scope was considered analogous to the STPA-Coordination scope in this case study. Second, SC-203 published its FHA and functional requirements analysis in DO-344. In contrast, the SC-228 efforts are ongoing and plans for a published safety analysis are unknown as of this thesis.

In order to compare analysis results, the DO-344 FHA and functional requirements were coded into a set of quantitative and qualitative data related to the coordination framework, in particular the nine coordination elements. The approach used for the comparison included:

- Review SC-203 *DO-344 Operational and Functional Requirements and Safety Objective (OFRSO) for Unmanned Aircraft Systems (UAS) Standards. Volumes 1 and 2*. The comparison focused on two analyses:
 - The Functional Hazard Assessment (FHA), Appendix I in Volume 2.
 - The functional requirements analysis documented in Volume 1.
- Code the FHA (252 pages) to relate identified applicable hazards to the coordination framework developed in this thesis.
- Code the functional requirements guided by the coordination framework.
- Compare frequency (quantitative analysis) and content (qualitative analysis) of STPA-Coordination hazardous scenario results to the DO-344 FHA.
- Compare frequency and content of STPA-Coordination derived coordination safety requirements with the DO-344 functional requirements.

Again, the data trends, observations, and qualitative results are emphasized. The absolute numbers should not be considered significant results. See APPENDIX D. Coding of and Comparison with DO-344 FHA and Requirements Analysis for further details and primary data.

5.5.1 Functional Hazard Analysis

According to (RTCA SC-203 2013b), “The FHA was conducted using experienced safety, engineering and operational expertise” (p. H-1), which consisted of “...manned pilots (general aviation, air carrier and military), unmanned pilots, former air traffic controllers, UAS operators, designated engineering representatives, airworthiness certification authorities, and safety analyst[s]” (p. H-2). The UAS integration FHA had the following scope (RTCA SC-203 2013b):

- In Scope:
 - The FHA focused on UAS failures alone (p. H-2).
 - “...only loss and erroneous failure conditions were assessed” (p. H-5).
 - Erroneous was defined as “...when the operating behavior was anything other than what it should be” (p. H-6).
- Out of Scope:
 - The operational environment was not considered (p. H-2).
 - “Delayed and degraded failure conditions...” were not assessed (p. H-5).
 - Compound failures and cross-functional analysis was not done (p. H-6).

Table 32 shows the STPA-Coordination hazardous scenario comparison with the DO-344 FHA. Included in the comparison are FHA hazards associated with UAS-ATC and UAS-proximate aircraft interactions, which are the same interactions analyzed by STPA-Coordination. The table is red where analysis did not identify a hazardous scenario related to a coordination element, whereas green indicates identification of and having the most coordination related hazardous scenarios for the associated element.

Table 32. Hazardous Coordination Scenarios, Comparison with DO-344 FHA

Coordination Elements	Comparison: Hazardous Coordination Scenarios	
	DO-344 FHA	STPA-Coordination
1. Coordination Goals	0	3
2. Coordination Strategy	0	46
3. Decision Systems	0	3
4. Communications	1	16
5. Group Decision-Making	0	12
6. Observation of Common Objects	7	18
7. Authority, Responsibility, Accountability	0	23
8. Common Understanding	30	46
9. Predictability	10	27
Total Hazardous Coordination Scenarios	48	194

Observations from the hazardous scenario comparison with the FHA in Table 32 include:

- STPA-Coordination identified over four times the unique hazardous coordination scenarios than the SC-203 FHA, 194 to 48 respectively. To provide context, approximately 350 FHA scenarios were included in the comparison, of which 48 scenarios were considered unique.
- STPA-Coordination identified approximately 11 unique failure and degradation scenarios, accounting for roughly 6% of the total hazardous coordination scenarios. This meant that about 94% of the hazardous coordination scenarios identified were related to potential *designed* coordination interactions with the physical process layers (i.e. nothing has failed). In contrast, all the FHA scenarios addressed failures of function or form.
- STPA-Coordination addressed the nine coordination elements identified by the coordination framework, while the FHA addressed four of them.
- STPA-Coordination found more hazardous scenarios in every coordination element category (highlighted by green cells). The largest scenario difference was with coordination strategy where the FHA did not find related scenarios compared to 46 found by STPA-Coordination.
- Common understanding was the most frequent coordination element in each analysis. Common understanding accounted for 24% of the STPA-Coordination scenarios and 63% of the FHA scenarios.
 - Discussion. The FHA focused on failures of UAS DAA and other systems that report state information (e.g. altitude, heading/trajjectory, and position). In addition to

failures, STPA-Coordination identified where missing and inadequate common understanding is or could be designed into the UAS-NAS system.

A qualitative comparison between STPA-Coordination and the DO-344 FHA was conducted. Table 33 is an excerpt of the qualitative comparison, with the full comparison in APPENDIX D, Table 49. FHA Coding and Comparison Results.

Table 33. A Qualitative Comparison with DO-344 FHA Coordination Scenarios

Coordination Elements	FHA Scenarios	Comparison Discussion. <i>NSE (No Safety Effect); MIN (Minimal risk); UA (Unmanned Aircraft)</i>
1. Coordination Goals	Not addressed	<ul style="list-style-type: none"> FHA. Scenarios were not addressed at this level. STPA-Coordination. Goal divergence was addressed as a safety factor for coordination.
2. Coordination Strategy	Not addressed	<ul style="list-style-type: none"> FHA. Coordination strategy was not addressed by the FHA. STPA-Coordination. The strategy can lead to hazards, which is Flawed Coordination Case 3.
3. Decision Systems	Not addressed	<ul style="list-style-type: none"> Both analyses focused on the same decision systems and components, however, only STPA-Coordination addressed how decision systems can impact a safe coordination outcome.
4. Comm	“2.1.1 Loss of external communication with ATC”	<ul style="list-style-type: none"> FHA. NSE (ATC, ATC environment, undetected) “...the controller would take no action, having no effect on normal procedures or workload” (p. I-74, vol. 2). The FHA considered primarily workload impact on the controller. STPA-Coordination. This hazard may occur for many reasons and in worst case conditions could lead to a loss of separation, regardless of likelihood or ATC workload. ATC may not know there is a loss until when the communications are needed.
	“2.2.1 Loss of external communications between UAS pilot and proximate traffic”	<ul style="list-style-type: none"> The FHA classified this hazard as MIN across the failure scenarios categories, with “...negligible effect on safety” (p. I-90, vol. 2) and “...a slight loss of situational awareness” (p. I-89, vol. 2), STPA-Coordination. In nearly complete contrast with the FHA severity assessment, lateral coordination is dependent upon UAS-Proximate Aircraft communications, both verbal and digital means. Without communication, real-time coordination is difficult to impossible.
5. Group DM	Not addressed	<ul style="list-style-type: none"> FHA. Group DM was not addressed in the FHA. For lateral coordination, the FHA acknowledged in lateral communications that the “RTCA Issue Paper ‘UAS control and communications architectures’ recommends that partyline comms are not needed except at non-towered airfields” (p. I-86, vol. 2). STPA-Coordination. Recommended regulations that allow use of

Coordination Elements	FHA Scenarios	Comparison Discussion. <i>NSE (No Safety Effect); MIN (Minimal risk); UA (Unmanned Aircraft)</i>
		ATC frequency for group DM when in collision scenario.
6. Observation of Common Objects	“1.1.1 Loss of ability to sense and avoid traffic”	<ul style="list-style-type: none"> • FHA: NSE (Proximate user, non-ATC environment) “If detected, the UA pilot would work to maneuver the aircraft away from last known position of proximate traffic...having no effect on airspace users as they would have no awareness of the UA” (p. I-5, vol. 2). This was a component perspective on a coordination problem, which was commonly observed throughout this research. The assumption was that the UAS aircrew knows all other decision system actions, which is invalid. • STPA-Coordination. Losing the ability to observe is a hazardous coordination scenario, which was opposite to the FHA NSE risk assessment.
	“1.5.1 Loss of ability to remain clear of unauthorized airspace”	<ul style="list-style-type: none"> • FHA. Coordination discussion: “If undetected by the UAS, military pilots or the restricted airspace controlling agency, the UA could inadvertently enter into restricted airspace and, once the UA pilot is alerted by the sense and avoid system, begin avoidance maneuvers. However, due to high closure speeds ... and unawareness of the military pilots, a near midair collision may result” (p. I-53, vol. 2). • STPA-Coordination. The FHA does not relate this problem to a loss of observation. Being in unauthorized airspace alone does not constitute a hazard. In fact, if the protected airspace is not in use it could be the safest place to fly. Also, closure speed is inherent part of a collision and is accounted for in the DAA/CAS algorithm. In STPA-Coordination, being in a protected airspace may lead to concerns with UAS/other decision systems not observing the collision scenario.
7. ARA	Not addressed	<ul style="list-style-type: none"> • The FHA did not address this coordination concern, while it is a needed element for coordination. Hazard 2.1.2, erroneous or misleading ATC-UAS communications the FHA assessed: “This failure should be evaluated by human factors and not as a system design attribute” (p. I-80, vol. 2). • STPA-Coordination. “Human factors” is a safety concern and is addressed by STPA-Coordination. Instead of HF, however, this is an ARA coordination concern. STPA-Coordination identified many “misleading” hazardous scenarios in vertical coordination between ATC-UAS beyond complete loss of communications. Contrary to the FHA assertion, many UAS/DAA design requirements and considerations were derived from analysis of the ARA coordination element.

Coordination Elements	FHA Scenarios	Comparison Discussion. <i>NSE (No Safety Effect); MIN (Minimal risk); UA (Unmanned Aircraft)</i>
8. Common Understanding	“3.3.1 Loss of UA ground position information”	<ul style="list-style-type: none"> The FHA assessed the hazard NSE (Airspace user, non-ATC environment), “If undetected, pilots in the area would maintain routine see and avoid operations” (p. I-173, vol. 2). STPA-Coordination considers loss of state information a common understanding concern that can lead to unsafe coordination. Again, STPA-Coordination stands in contrast to the FHA.
9. Predictability	“3.5.1 Loss of UA trajectory definition”	<ul style="list-style-type: none"> The FHA and STPA-Coordination both assessed the scenario as hazardous.

Qualitative observations and comparisons in Table 33 include:

- The FHA used “workload” as the primary measure for ATC-related hazards, see Table 33 FHA scenario 2.1.1. The FHA assumption was that workload was negatively correlated to safety (if workload goes up, then safety goes down). Thus, when a failure scenario went “undetected” by ATC, the FHA generally deemed the hazard minimal (MIN) risk or even “no safety effect” (NSE) because ATC workload was not affected by their lack of awareness. In contrast, STPA-Coordination considered lack of knowledge about the actual state a hazardous coordination scenario.
- The FHA decomposed the hazards by arbitrary failure conditions, which made understanding the hazard relationships and whether the hazards were unique difficult. For example, loss of the DAA function was a hazard. Other failure hazards were loss of altitude, position, or heading information, which were also refinements to the DAA functions loss. Although a dependency existed for this risk assessment, each hazard was identified as unique. In contrast, STPA-Coordination provided a framework to understand hazardous scenario relationships and how each may lead to hazards.
- The FHA focused on failure conditions and related them to the UAS perspective. Many FHA scenarios were assessed Minimal risk or even No Safety Effect because the other interdependent decision system (ATC or other aircraft) would not be aware. STPA-Coordination, in contrast, recognized the interdependency between decision systems; a failure condition of one decision system can absolutely affect the coordination safety problem. In addition to failures, STPA-Coordination focused on identification of flawed coordination *behavior* that can lead to hazards.

5.5.2 UAS Functional Requirements, DO-344

STPA-Coordination results can be used to create recommendations and requirements to eliminate or mitigate the identified hazardous coordination scenarios. To compare the STPA-Coordination recommendations, a frequency analysis and qualitative comparison was accomplished on the DO-344

“functional requirements” found in DO-344 (vol. 1) Chapter 3 and Appendix C (RTCA SC-203 2013a). SC-203 identified four top level UAS functions to include: 1) avoid hazards, 2) communicate, 3) navigate, and 4) control (RTCA SC-203 2013a). Each function was further decomposed into sub functions that were in most cases traced to a safety objective addressed by the FHA. In some cases, the functional requirement was not traced to a safety objective, but was traced back to an “Operational Requirement”.

The frequency analysis first required coding the functional requirements using the coordination framework. Not every DO-344 functional requirement was traced to the FHA, but all within and between decision system coordination functions were considered in the comparison. This approach was considered a reasonable coordination requirements comparison. See APPENDIX D for further analysis details on comparison with DO-344 functional requirements.

Table 34 summarizes the frequency analysis comparison of STPA-Coordination with DO-344 functional requirements.

Table 34. Coordination Requirements, Comparison with DO-344 Functional Requirements

Coordination Elements	Comparison: Coordination Recommendations	
	DO-344 Functional Requirements	STPA-Coordination
1. Coordination Goals	0	2
2. Coordination Strategy	4	53
3. Decision Systems	0	2
4. Communications	2	22
5. Group Decision-Making	0	13
6. Observation of Common Objects	4	25
7. Authority, Responsibility, Accountability	0	33
8. Common Understanding	19	37
9. Predictability	3	29
Total Coordination Recommendations	32	216

Observations from the requirements comparison in Table 34 include:

- STPA-Coordination recommendations addressed the nine coordination elements, while the DO-344 functional requirements addressed five of nine. This suggests STPA-Coordination provides additional insights not analytically derived by the FHA for the coordination safety problem.
- STPA-Coordination analytically derived over six times the number of coordination related recommendations than published in the DO-344 functional requirements.

- The largest difference in recommendations occurred with the coordination strategy element with a difference of 49. The implications are that STPA-Coordination may better assist in the design of functional interactions (i.e. coordination) needed for safety.
- Coordination goals and decision system elements had the smallest gap in derived recommendations. This was intuitive as the goals and decision systems can be assumed established for UAS integration. While training of decision systems was an important safety concern, it was not the focus of STPA-Coordination or the FHA in this case study.

5.5.3 STPA-Coordination Comparison with DO-344 Summary

Overall, the quantitative and qualitative comparison to the DO-344 FHA and functional requirements analysis suggests benefits from using STPA-Coordination.

Quantitative results had a few notable trends supported by the data. One was that STPA-Coordination provided additional insights into analysis of coordination and safety. The FHA identified hazardous scenarios related to four of the nine coordination elements described by the framework and recommended requirements that related to five coordination elements. In contrast, STPA-Coordination addressed the nine coordination elements in hazardous scenario identification and in coordination recommendations. The frequency analysis trends also suggested that STPA-Coordination might be most beneficial for addressing coordination strategy and accountability, responsibility, and accountability coordination elements.

Qualitatively, STPA-Coordination results identified flawed coordination scenarios that can be used to develop recommendations for coordination (i.e. addressing the nine coordination elements) that lead to safe outcomes. The same cannot be claimed from the DO-344 FHA and requirements analysis. The FHA can be used to determine a “safety objective” (i.e. failure or reliability requirement), but how this relates to coordination behavior is ambiguous. Assessing interactions for the UAS integration problem using the FHA was difficult as evidenced by this DO-344 quote (RTCA SC-203 2013b):

To assist in this [SC-203] effort the Safety Workgroup developed a cross-functional matrix. A number of associations were identified but, when assessing the effects of failures, it became apparent that it was not practical from a purely system-agnostic approach to proceed. Without an understanding of functional allocations to a system design, the assessment would remain too speculative as it would be based on assumptions of functional relationships rather than intended relations. For this reason, a decision was made to defer an assessment of cross-functional associations until the ASOR [allocation of safety objectives and requirements] phase. (pp. H-6 to H-7).

It is interesting to note that certifying aircraft systems by specifying design requirements (for example, as was done for TCAS) rather than failure rates was the approach to certification used prior to the current emphasis on performance-based regulation.

Comparison results suggest that STPA-Coordination is better suited to address coordination for analysis and design of UAS integration than the FHA and functional requirements analysis used by SC-203.

5.6 A Process Comparison for Safety Analysis of UAS Integration

In addition to an analytical comparison against the SC-203 safety analysis results as documented in DO-344 (2013), the safety analysis processes used for UAS integration efforts can be compared.

5.6.1 Overview of Safety Analysis Processes

RTCA SC-203 and SC-228 safety analysis efforts used similar approaches to characterizing the safety of UAS integration into the NAS. SC-203 was guided in part by:

- RTCA DO-264 *Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications* (RTCA SC-189 2000). This document outlines an analysis and approval framework for developing operational, safety, performance, and interoperability requirements.
- The FAA-ATO (Air Traffic Organization) Safety Management System (SMS) Manual. Version 2.1 (2008) was specifically mentioned, which has since been updated.

Guidance for the current RTCA SC-228 safety process is outlined in the SC-228 DAA White Paper (RTCA SC-228 2014). In part, safety analysis would include:

- Use of the FAA-ATO (Air Traffic Organization) Safety Management System approach.
- Use of 1) Target Level of Safety and 2) Risk Ratio metric as defined in the SAA (sense-and-avoid) Second Caucus Workshop report (2013).

- The Sense-and-Avoid workshop report recommended:

(R 3.1) TLS is the key metric for substantiating the safety level of UAS in the NAS ATM system, but TLS does not easily lend itself to describing the levels of mitigation that an UAS SAA system needs to achieve. The TLS should be broken down into UAS SAA system mitigating components and should express those components in the form of a risk ratio.

(R 3.2) The safety metric for UAS SAA Target Level of Safety should be expressed in terms of Catastrophic Collision Event per flight hour (CCE/FH), where one (1) MAC [mid-air collision], regardless of fatalities or damage to either aircraft, is defined to comprise two (2) Catastrophic Collision Events, and the quantitative values and methodologies described in ICAO Doc 9689-AN/953³ should be retained as the safety substantiation for UAS SAA. (Federal Aviation Administration 2013b) p. vii

- The Risk Ratio may be used for the “technical assumption” identified in the SC-228 DAA white paper: “DAA functions will be proven not to degrade the safety of

³ ICAO Doc 9689 describes planning methodology for aircraft separation minima determination.

aircraft equipped with TCAS II for applicable airspace classes” (p. 13). The Risk Ratio can be used to compare accident rates with and without the DAA.

Former and current RTCA UAS integration safety efforts are united in safety analysis goals and in analysis processes used. The goal of safety analysis is to show that “The introduction of UAS to the NAS should have no greater effect than the integration of any other aircraft” (RTCA SC-203 2013a) p. 10. As discussed, accident rates and reliability measures are used to characterize the UAS integration risk. The common analysis process used is the FAA’s Safety Management System, in particular the Safety Risk Management process.

5.6.2 Comparison to the FAA Safety Risk Management Process

The FAA Safety Management System (SMS) Manual provides guidance for the safety validation of changes to the NAS and its operations (Federal Aviation Administration 2014c). While the SMS discusses traditional safety analysis methods such as Fault Tree Analysis and hazard analysis, it is not a how-to manual. Rather, the FAA SMS provides a system safety analysis framework that is grounded in the Safety Risk Management (SRM) five-step process. The SRM process and description is reprinted in Figure 29 from the SMS Manual.

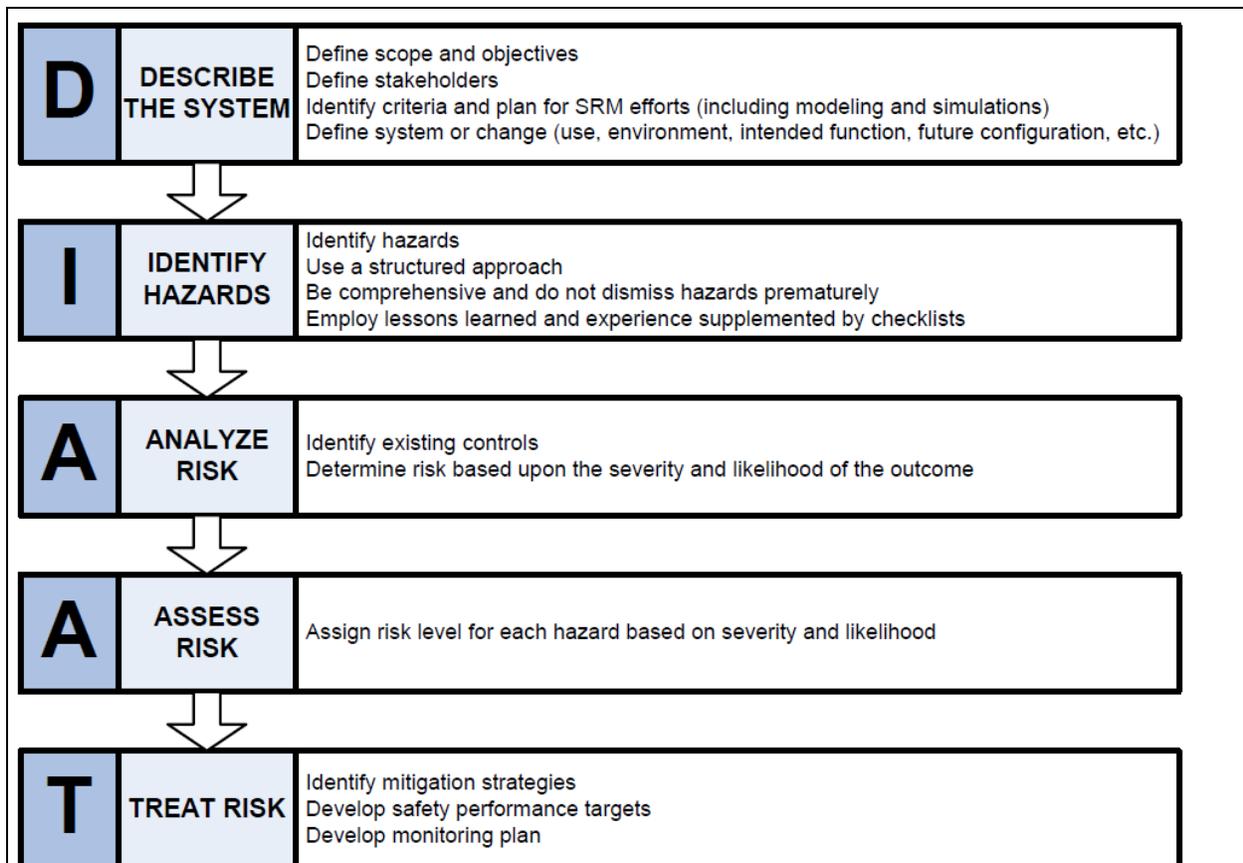


Figure 29. FAA Safety Risk Management Analysis Phases

Reprinted from (Federal Aviation Administration 2014c), p. 19. Figure in public domain.

A comparison of the FAA’s Safety Risk Management and extended STPA processes is given in Table 35. The comparison is largely a comparison to STPA, which by association is a comparison to STPA-Coordination.

Table 35. Extended STPA Comparison with the FAA Safety Risk Management

	FAA Safety Risk Management (SRM)	Extended STPA (with STPA-Coordination)
Safety Definition	<ul style="list-style-type: none"> “...the state in which the risk of harm to persons or property damage is acceptable” (p. 1). Safety is a likelihood. 	<ul style="list-style-type: none"> Freedom from conditions which cause accidents Safety is a state (lack of accidents) that is controlled top-down in a system.
Accident Model and Assumptions	<ul style="list-style-type: none"> Accidents occur from a chain of failure events, which the SMS labels “defense in depth.” Assume: <ul style="list-style-type: none"> Independent and stochastic events. Reliability is equivalent to safety. 	<ul style="list-style-type: none"> STAMP. Accidents occur from inadequate controls and enforcement of system safety constraints.
Identify Hazards	<ul style="list-style-type: none"> Hazards are defined as failures. 	<ul style="list-style-type: none"> Hazards are defined as a system state or set of conditions that can lead to accidents given a worst-case scenario. Hazards as defined by the FAA are considered hazardous scenarios in STAMP, or a cause of unsafe control.
Analysis	<ul style="list-style-type: none"> Determine and assess risk of hazards in terms of severity and likelihood. A significant concern is lack of data on the future airspace system and UAS/DAA technology needed for quantitative assessment (US Department of Transportation 2014; US Government Accountability Office 2013). Limited to no guidance for analysis of system behavior and interactions beyond failures, to include coordination behavior. 	<ul style="list-style-type: none"> Worst case analysis. Identify hazardous behavior and interaction scenarios that can lead to unsafe control actions. Analytical guidance provided with four flawed coordination cases and nine coordination elements. Likelihood is not assessed. Analysis is not hindered by lack of data as behaviors and interactions are analyzed. STPA-Coordination is a functional analysis. In contrast to the FAA’s SRM, loss and failures are only one of many hazardous conditions addressed.
Design	<ul style="list-style-type: none"> Mitigate risk. Examples include redundancy and “System design that ensures that critical functionality is 	<ul style="list-style-type: none"> Design recommendations seek to eliminate hazardous scenarios identified by STPA and STPA-

	FAA Safety Risk Management (SRM)	Extended STPA (with STPA-Coordination)
	<p>maintained in degraded mode if individual elements fail” (p. 12). Design recommendations seek to improve reliability to decrease accident rates and meet an identified TLS.</p> <ul style="list-style-type: none"> • Set safety targets. According to an FAA workshop report, UAS integration accident rate objectives may need to meet 1E-7 to 1E-9 MAC/FH, which is an arbitrary yet accepted threshold for MACs (Federal Aviation Administration 2013b). • When the risk is too high, the SRM process recommends “revise objective/scope or abandon project” (p. 64 in Figure 4.1). 	<p>Coordination.</p> <ul style="list-style-type: none"> • Otherwise, mitigate the effects of the hazardous scenario and document for monitoring. • Design recommendations do not try to meet quantitative safety objectives. Rather, recommendations address requirements for system functions and interactions that assist in the design of accident free systems.
Coordination Behavior	<ul style="list-style-type: none"> • Explicit is analysis of failure conditions. Analysis of coordination behavior is not. 	<ul style="list-style-type: none"> • Use of STPA-Coordination derives requirements for safe coordination within and between decision systems.

Sheridan critiques “Quantitative modeling as sorcery for the powerful” in his observation that cultures have a perhaps irrational affinity towards wanting to reduce highly complex concepts such as safety of sociotechnical systems into numbers (Sheridan 2002) p. 167. STPA-Coordination and in general STPA does not reduce safety to a number. STPA-Coordination provides guidance to identify flawed coordination behavior within and between decision systems that may lead to unsafe control actions (i.e. hazards) in the worst-case scenarios. Systems reliant on the FAA’s Safety Risk Management processes may benefit from the use of extended STPA.

5.7 Summary, STPA-Coordination Case Study

The case study demonstrated the utility of the coordination framework and STPA-Coordination to analyze coordination in the UAS integration system, which is a system in design phase. The coordination framework was useful in developing the safety control structure and defining the roles and responsibilities of decision systems. STPA-Coordination and flawed coordination guidance successfully identified hazardous coordination scenarios that can lead to unsafe control actions and derived safety requirement for use in the design of safe coordination, including the design of the DAA technology suite.

STPA-Coordination was compared with safety analysis results documented in official RTCA DO-344 reports. STPA-Coordination results suggest quantitative and qualitative benefits in both hazardous

scenario identification and in development of coordination safety recommendations. In this case study, a qualitative benefit to STPA-Coordination is that derived recommendations holistically address coordination (i.e. the nine coordination elements of the framework) among UAS and NAS stakeholders, which if implemented may assist in preventing coordination-related accidents. The same claim is difficult to make from implementing the ad-hoc functional requirements documented in DO-344.

As outlined in this case study, UAS integration safety is largely a coordination problem that must address shared airspace interdependency to avoid collisions. To not assess the safety of coordination behavior between the primary decision systems is a mistake. The traditional safety analysis techniques being used as prescribed by the FAA's Safety Risk Management process have limited analytical means to conduct such a coordination safety analysis. Analysis of UAS integration safety may benefit from an alternative system-theoretic paradigm using extended STPA.

6 CAST-COORDINATION CASE STUDY. PATRIOT FRIENDLY FIRE SHOOT DOWN

“The Patriot system, CRC [Control and Reporting Center], AWACS [Airborne Warning and Control Center] and friendly fighters have become interdependent, but without each player understanding the needs, concerns or requirements of the other” (US Central Command 2004) p. 37.

On 22 Mar 2003 and then again on 2 April 2003, Patriot missile systems shot down friendly aircraft that were supporting Operation Iraqi Freedom (OIF). In another friendly fire incident, 24 March 2003, an F-16 fighter aircraft engaged a Patriot battery with an anti-radiation missile; there were fortunately no injuries. Within a two-week period, three unsafe incidents unambiguously demonstrated that coordination among interdependent decision systems was inadequate and in some cases potentially missing. This chapter investigates how coordination influenced the Patriot and aircrew friendly fire incidents.

This chapter first introduces CAST-Coordination, which extends CAST (Causal Analysis based on STAMP) with additional steps for analysis of coordination. The chapter then presents the CAST-Coordination case study on the Patriot friendly fire incident involving a British GR-4 Tornado aircraft. CAST-Coordination results are compared to the findings and recommendation in two official accident reports, one by the US Central Command (USCENTCOM) and the other by the United Kingdom (UK) Ministry of Defence (MOD). To provide another perspective, the case study also reviews and compares a Defense Science Board report (2005) discussing Patriot system operations during OIF.

The case study scope for analysis and comparison is coordination alone in order to evaluate the additional insights gained from using CAST-Coordination and the flawed coordination analysis guidance. See APPENDIX E. CAST-Coordination Case Study Background for more information on joint military operations and the case study approach.

6.1 CAST-Coordination

CAST-Coordination *extends* CAST with additional steps to accomplish CAST Step 7: “Examine overall coordination and communication contributors to the loss” (Leveson 2012) p. 351. CAST-Coordination was developed from this chapter’s case study and the coordination framework. The same flawed coordination guidance used in STPA-Coordination is used for CAST-Coordination. Table 36 summarizes CAST-Coordination.



Figure 30. Patriot Missile System Launch

Image from (US Army Aviation and Missile Life Cycle Management Command n.d.). Image in public domain.

Table 36. CAST-Coordination Steps

CAST Step 7. Examine Overall Coordination
CAST-Coordination <ul style="list-style-type: none">• Identify decision system interdependency.• Use guidance provided by flawed coordination cases and coordination elements to analyze:<ul style="list-style-type: none">○ Physical process level coordination, between (or within) decision systems.○ Top-level coordination and its influence on the physical process coordination.○ Supporting coordination. Decision-making hierarchy coordination from top to bottom and within decision system coordination.

First, identify the interdependency that existed to establish when and where coordination was required.

Second, analyze the physical process layer coordination, which is most directly involved with the accident. A thorough understanding of coordination influences most directly involved with the accident provides context for analysis of coordination in the decision-making hierarchy. In this case study, lateral coordination between the aircrew and Patriot decision systems was most directly involved with the aircraft and missile physical systems shared airspace interdependency.

Next, analyze coordination at the highest level. The top-level coordination transforms the system goals and safety constraints into a refined set of goals and constraints. The case study example is lateral coordination between the Joint Force Air and Joint Force Land Component Commanders, which are responsible for providing theater-level coordination strategy that meets the Joint Force Commander's intent. Particular for this case study was analysis of the coordination required to develop and implement a safe coordination strategy for integrated air defense artillery and flight operations.

Last is to analyze *supporting* coordination efforts, from the top-down. The decision-making hierarchy coordination supports the decision systems controlling the physical process layer. The supporting coordination provides the safety constraints and coordination strategy to the physical layer decision systems, among other coordination information. The decision-making hierarchy coordination may be extensive in large sociotechnical systems, such as in joint military operations. This case study addressed the supporting coordination from an Air Component perspective, the Land Component vertical hierarchy, and lateral coordination between mid-level air and land decision systems.

Supporting coordination also includes within decision system coordination. Analysis of within decision system coordination can occur at any time given the context for between decision system coordination is known. For example, this case study addresses the Air Component Command within decision system coordination.

CAST-Coordination is recommended to be accomplished in the order discussed because it was found useful for this case study. In addition, there is not one correct analysis. CAST-Coordination abstraction levels for analysis and results are influenced by the intended audience and the accident information details for example. CAST-Coordination also relies on the expertise of those using it for accident investigation.

Application of CAST-Coordination follows, starting with the systems engineering baseline.

6.2 Systems Engineering Baseline

System safety is conceived within the systems engineering efforts. Taking a top-down approach, a systems theoretic hazard analysis starts with the identification of goals, hazards, and constraints. For this accident, the following apply:

- Sociotechnical System: Joint Military Operations, consisting of Air Defense and Airspace Controls systems.
- Goal: Safe coordination of air defense systems and coalition aircraft flight operations.
- Accident (A) of interest:
 - A1. Shoot down of friendly aircraft by Patriot system (fratricide).
- System Hazards (H):
 - H1. Patriot system engagement of friendly aircraft.
 - H2. Missile reaches lethal radius of friendly aircraft.
- System Safety Constraints (SC):
 - SC1. The Patriot system shall not engage friendly aircraft.
 - SC2. The Patriot system shall abort launched missiles on friendly aircraft prior to reaching lethal radius.

6.3 The Safety Control Structure

“...the ability to comprehensively execute AMD [Air and Missile Defense] operations requires detailed planning, coordination and control of air defense fires” (US Department of the Army 2016) p. 3-10.

A safety control structure is developed, which represents the decision systems involved in the Patriot friendly fire, shown in Figure 31. The decision systems are represented at abstraction levels commensurate to the level of detail found in the accident investigation reports and deemed useful to demonstrate CAST-Coordination. The command, coordination, and engagement authority relationships shown were responsible for defensive counter air and airspace operations. The relationships identified are considered representative of what existed during the accident and consistent with the accident investigation reports, Service doctrine, and Joint military doctrine.

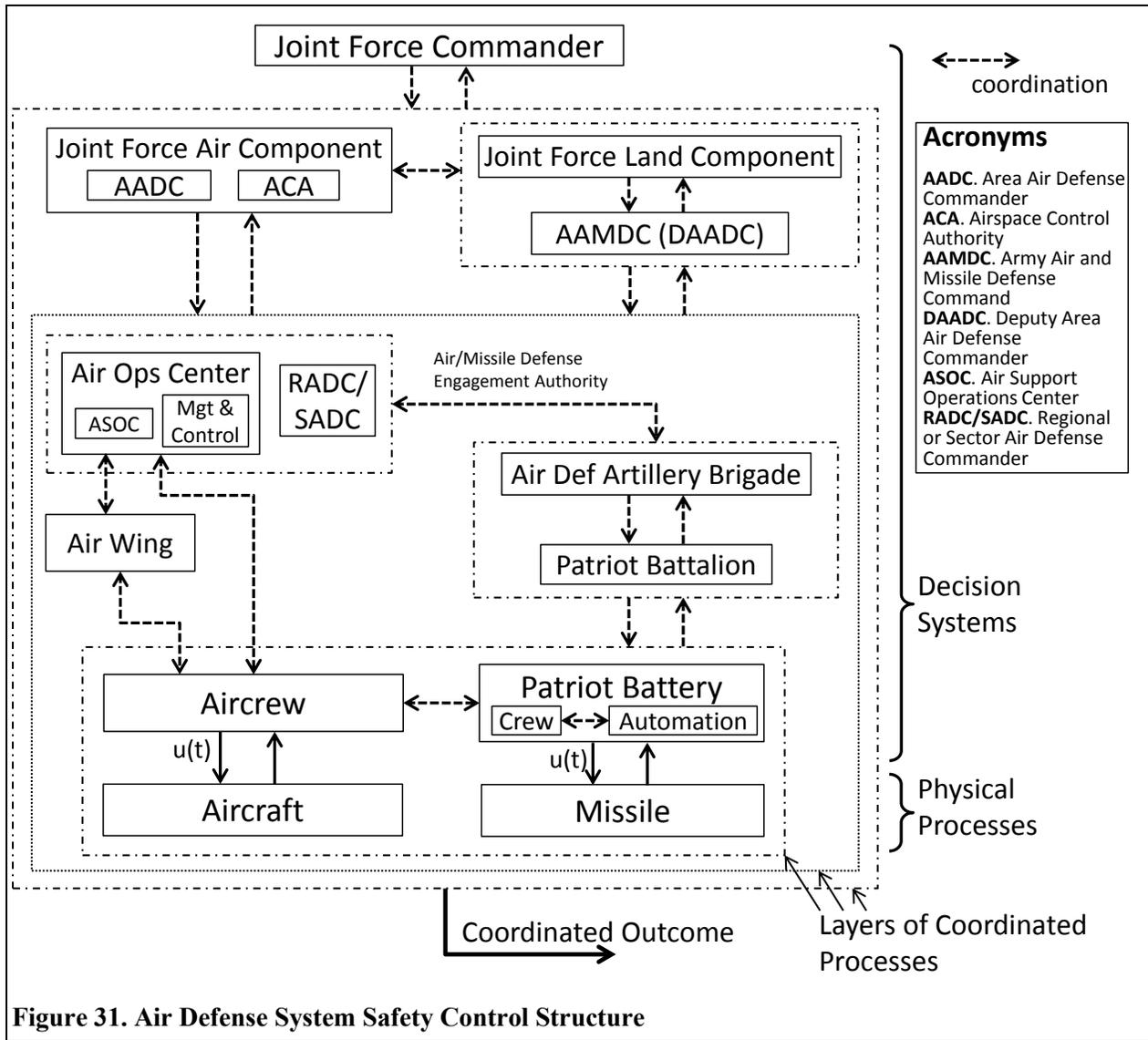


Figure 31. Air Defense System Safety Control Structure

In part, the roles and responsibilities of the decision-making hierarchy were to ensure 1) adequate coordination between decisions systems in control of the Patriot system and friendly aircraft were accomplished and 2) that the coordination leads to safe outcomes (i.e. no fratricides). Table 37 gives an overview of individual decision system roles and responsibilities pertaining to the fratricide avoidance in executing defensive counterair and airspace control.

Table 37. Joint Operations Decision System Roles and Responsibilities

Decision System	Role and Responsibility Related to Fratricide Avoidance
Joint Force Commander (JFC)	The staff of the Joint Force Commander is responsible for overall strategic decisions and guidance of the joint operations in Iraq. The JFC approves high level coordination strategy documents for defensive counterair (i.e. the Area Air Defense Plan) and airspace control (i.e. the Airspace Control Plan).

Decision System	Role and Responsibility Related to Fratricide Avoidance
Joint Force Air Component Commander (JFACC)	<p>The component commanders are responsible for carrying out the strategic vision of the JFC, developing the overall coordination strategy, and developing the rules of engagement for prosecuting the war.</p> <ul style="list-style-type: none"> • The JFACC has operational control (OPCON) over assigned air forces. The JFACC normally holds two additional commands pertinent to the case study. <ul style="list-style-type: none"> ○ AADC (Area Air Defense Commander) is responsible for coordination of the entire theater air defense effort. The AADC develops the AADP (Area Air Defense Plan) coordination strategy document. ○ ACA (Airspace Control Authority) is responsible for the control and coordination of airspace usage that affect the Patriot system and aircrew. The ACA develops the ACP (Airspace Control Plan) coordination strategy document. • The JFACC uses the Joint Air Operations Center (JAOC) as the central C3 (command, control, and communications) node to plan, coordinate and execute the mission, including defensive counterair. <ul style="list-style-type: none"> ○ Subordinate to the AOC is the ASOC (Air Support Operations Center), which is the “primary control agency...for execution of air power in direct support of land operations” (US Department of Defense Joint Staff 2014a) p. II-9. ○ The AOC may delegate battle management and airspace control—“Mgt & Control”—functions to other C2 decision systems, such as AWACS (Airborne Warning and Control System) and CRC (Control and Reporting Center) (US Air Force 2015).
Joint Force Land Component Commander (JFLCC)	<p>Similar to the JFACC. The JFLCC exercises OPCON over assigned joint ground forces, including air defense artillery.</p>
Army Air and Missile Defense Command (AAMDC)	<ul style="list-style-type: none"> • The AAMDC is normally assigned three roles. <ul style="list-style-type: none"> ○ The “...Army forces (ARFOR) operational lead for counterair operations who ensures the ARFOR contribution is properly planned, coordinated, integrated, and synchronized” (US Department of Defense Joint Staff 2012) p. II-4. ○ Is the JFLCC’s principle advisor on the counterair mission and use of air defense artillery (ADA) forces, called the Theater Army Air and Missile Defense Coordinator (TAAMDCOORD). ○ Designated the Deputy Area Air Defense Commander in support of theater defensive counter air operations.
Regional or Sector Air Defense Commanders (RADC, SADC)	<p>The JFACC/AADC can delegate air defense engagement authority to RADC/SADC as needed. “Normally” air defense engagement authority is not delegated lower (US Air Force 2015). “The RADC (or SADC) executes air defense operations through the CRC [Control and Reporting Center], or through an AWACS [Airborne</p>

Decision System	Role and Responsibility Related to Fratricide Avoidance
	Warning and Control System] until a CRC arrives in the area of operations” (US Department of the Army 2016) p. 3-9.
Air Defense Artillery (ADA) Chain of Command	<p>The ADA Brigade, Battalion, and Battery represent a typical chain of command for Patriot systems units. Delegated engagement authority depends on the rules of engagement and individual scenario.</p> <p>(US Department of the Army 2016) defined the ADA brigade interactions with higher level decision systems:</p> <ul style="list-style-type: none"> • “JOA [joint operating area] ADA brigades follow the weapon control procedures and measures established by the AADC for conducting JOA air and missile defense” (p. 3-5). • “The ADA brigade is under the command of the AAMDC. ... The brigade will always follow the measures established by the AAMDC when conducting AMD operations” (p. 3-8).

Lateral coordination efforts existed for: 1) the Joint Air and Land Component Commander level, and 2) the aircrew and Patriot decision system. Coordination by control methods are implied in the hierarchical arrangement, including the air defense engagement authority from the RADC/SADC to the Patriot Battery chain of command. While not explicitly shown in the control structure, there is a complex set of interactions needed for AMD to be effective. According to the US Army Air Defense Artillery manual (2013), coordination between the following decision systems “must be accomplished between the following organizations:

- The AAMDC to the JFC, host nation, allies[,] JFACC, AADC, ACA, JFLCC, Army Forces commander, BCD [Battlefield Coordination Detachments], ADA brigades, and ADA battalions.
- The ADA brigade to the AAMDC, AADC, ACA, CRC, JFLCC, Army forces Commander, and subordinate ADA battalions. If the AAMDC is not present, then the JOA brigade coordinates as the AAMDC.” (p. 3-13)

The safety control structure is a model and a representation that was considered useful for conducting and comprehending CAST-Coordination results. See APPENDIX E for further explanations of joint military operations and coordination relationships represented in the safety control structure and analyzed by CAST-Coordination.

6.4 Proximate Events

Table 38 summarizes the known events and approximate timeline provided in the MOD accident report (United Kingdom Ministry of Defence 2004). The timeline reads from top to bottom, with rows grouping GR-4 and Patriot events that are proximate in time.

Table 38. Timeline, Patriot Shoot Down of GR-4

GR-4 Tornado Aircrew	Patriot Battery Crew
The GR-4 aircrew were tasked for mission in accordance with doctrine and rules.	The Patriot battery was operating autonomously to protect the ground troops from incoming missiles. They were focused on theater ballistic missile coming from Iraq.
The GR-4 planned in accordance with rules.	
Ground operations through takeoff uneventful and included confirmation that the IFF worked correctly prior to engine start.	
The aircrew were returning to Ali Al Salem Air Base, Kuwait and “completed appropriate checks” to include “noting that the IFF switches were set correctly” (p. 2). ⁴	The GR-4 was tracked and Patriot algorithms identified the GR-4 as an Anti-Radiation Missile with a vector directly towards them (p. 2). It was deduced that the GR-4 had IFF degradation (p. 4). Based on the information and rules-of-engagement, the Patriot crew launched a missile at the GR-4.
The aircrew started descent to base at about 18k feet.	
2348 hours, 22 March 2003: Patriot missile shot down GR-4 aircraft and crew did not attempt to eject.	

6.5 CAST-Coordination Applied

Given interdependency, multiple decision units stand to benefit from coordination. The CAST steps prior to Step 7 investigate from controller’s perspective. CAST-Coordination was used to investigate the accident and coordination relationships in the safety control structure, which was in part inspired by the accident reports reviewed.

6.5.1 Identify Decision System Interdependency

The joint military operations interdependencies relevant to the accident included:

1. Pooled interdependency to avoid fratricide of coalition aircraft by friendly air defense units. In other words, there was a shared coordination goal.
2. Shared resource interdependency with the defended airspace. The Patriots defend the airspace against hostile targets and the aircrew use the same airspace for transit and mission execution.

⁴ The USCENTOM report (2004) noted that some device was “active on” and “may have contributed to its classification as an ARM [anti-radiation missile]” (p. 23).

6.5.2 Aircrew and Patriot Decision System Lateral Coordination

First, CAST-Coordination evaluated lateral coordination between decision systems directly in control of the physical processes. Evaluation of the physical process coordination provides context for all other decision-making hierarchy coordination efforts investigated next. In this case study, the Patriot decision system and the aircrew lateral coordination was evaluated. This coordination was characterized as lateral coordination of independent physical processes, shown in Figure 32.

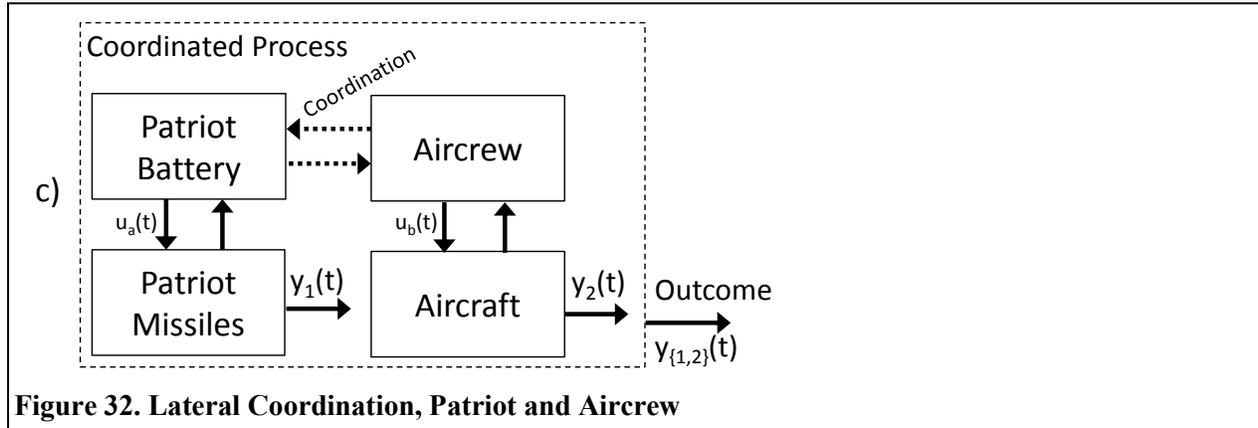


Figure 32. Lateral Coordination, Patriot and Aircrew

Decision System Descriptions:

- Patriot Battery Decision System
 - Decision Components
 - Tactical Control Officer (TCO). Responsible for identification and engagement decisions.
 - Tactical Control Assistant (TCA). Fire missiles and aids TCO in track information.
 - Automation. Classify targets as hostile, friendly or unknown, and in certain modes may automatically launch missiles (management by exception).
 - Common Outputs Related to the Accident
 - Missile launch.
 - Abort launched missile.
- GR-4 Tornado Decision System
 - Decision Components
 - Pilot. Responsible for aircraft movement and employment of weapons and self-defense systems.
 - Navigator/Weapons System Officer. Responsible for operating mission systems and assisting pilot in tactical and navigational decisions.

- Common Outputs Related to the Accident
 - Navigation of aircraft.
 - Operation of communications equipment.

Context for Coordination:

- Patriot system
 - Patriot system crews are under pressure to protect ground forces from theater ballistic missiles.
 - Patriot crew training (United Kingdom Ministry of Defence 2004).
 - React quickly, seconds up to about one minute for engagement decisions.
 - Trust the Patriot system automation.
 - Patriot systems had successfully intercepted enemy theater ballistic missiles on 20 March 2003 (US Central Command 2004).
 - Patriot system crew was allowed to operate autonomously, with degraded communication to Patriot Battalion Headquarters (HQ).
- Aircrew
 - Aircrew were mission complete and flying back to base following return to base procedures for Ali Al Salem Air Base, Kuwait.
 - Accident reports deduced the GR-4 Tornado IFF Mode 4 was not working. If this was the case, aircrew may not have known IFF was malfunctioning. Aircrew accomplished return to base checks, including checking the IFF switch after mission complete.
 - The IFF Mode 4 pre-engine start check was satisfactory. Once started and throughout the mission there were many opportunities for IFF checks, however, the MOD report (2004) noted “there is no firm evidence that the ZG710 [GR-4] responded to any IFF interrogations throughout the entire mission” (p. 4).
- Coordination efforts included
 - Coordination Strategy:
 - IFF reliability strategy. The Patriot system relied on electronic identification of friendly aircraft using encrypted IFF mode 4.
 - The MOD report (2004) indicated a safe passage procedure existed to handle the IFF failure, although further details on the procedures were not found.

- Communication Channels: Radio communication channels were used for electronic identification—IFF interrogator and transponder. It does not appear other communication channels were used at the time.

Flawed Lateral Coordination Evaluation:

Flawed lateral coordination CAST-Coordination results are presented in Table 39. The “Eval” column in Table 39 is color coded per the following legend for a quick visualization and summary of the CAST-Coordination evaluation:

Coordination behavior was:

- Adequate
- Inadequate
- Missing

Where multiple accident influences were identified, the evaluation color represents the worst case scenario.

Table 39. Flawed Coordination Influences, Patriot and Aircrew Lateral Coordination

Eval	Patriot/Aircrew Flawed Coordination Influences	Patriot/Aircrew Lateral Coordination Recommendations
	<p>1. Coordination Goals.</p> <ul style="list-style-type: none"> The motivations to engage objects may not have been adequately calibrated. There were nine missiles that threatened coalition forces, and nine were engaged and destroyed (eight were attributed to Patriot missiles). But, two friendly aircraft within a two-week period were engaged and destroyed including the GR-4 Tornado. The fratricide rate was 2 of 11 engagements, or 18% for a relatively low missile threat environment (Defense Science Board 2005). 	<p>Patriot systems shall prioritize fratricide avoidance.</p>
	<p>2. Coordination Strategy (case 2 inadequate).</p> <ul style="list-style-type: none"> When the stakes are life and death, standardization (safe passage routes) and component reliability (IFF working) coordination strategies were inadequate. Standardization may be acceptable for more routine operations or when off-standardization does not lead to death. However, early warfare is dynamic and the coordination strategy had limited flexibility to adapt in this case to 	<ul style="list-style-type: none"> Coordination by standards alone shall be the exception and last resort when life is at stake and conditions are uncertain. Coordination methods that favor mutual adjustment are recommended given 1) a relatively low-intensity conflict environment and 2) dynamic warfare operations during initial phase.

Table 39. Flawed Coordination Influences, Patriot and Aircrew Lateral Coordination

Eval	Patriot/Aircrew Flawed Coordination Influences	Patriot/Aircrew Lateral Coordination Recommendations
	<p>unreliable IFF communications.</p> <ul style="list-style-type: none"> • The Patriot correctly identifying friendly aircraft by IFF means alone was inadequate: <ul style="list-style-type: none"> ○ Concerns with the electronic identification strategy using the encrypted IFF: <ul style="list-style-type: none"> ▪ IFF transmitter may fail or degrade (aircraft). ▪ Patriot IFF interrogator may fail or malfunction (Patriot) ▪ IFF may intermittently degrade during transit through protected airspace, even if good initially. ▪ IFF interrogation/transmit signals may be jammed. ▪ IFF signals may be too low energy. ▪ IFF encryption may be invalid. ▪ IFF encryption may expire during mission. ▪ IFF signals may be electromagnetically incompatible with aircraft or external signals. ▪ The Patriot crew or aircrew may not be aware their IFF equipment was inoperative or degraded. ○ Concerns with alternative routing strategy, such as safe passage for non-IFF conditions. <ul style="list-style-type: none"> ▪ Aircrew must know the IFF or applicable system that necessitates the safe passage route was degraded. ▪ Knowledge and understanding of current safe passage routes by aircrew. For example, new aircrew or aircrew diverting 	

Table 39. Flawed Coordination Influences, Patriot and Aircrew Lateral Coordination

Eval	Patriot/Aircrew Flawed Coordination Influences	Patriot/Aircrew Lateral Coordination Recommendations
	<p>from other bases may have little to no knowledge of local procedures.</p> <ul style="list-style-type: none"> ▪ Updates to alternative procedural strategy were inadequately dispersed to forces. Maybe some got the update and others did not; or, updates were not understood by forces because the Patriot crew are not familiar with air operations. ▪ Patriot crew may not know or recognize safe passage routes on displays. 	
	<p>3. Decision Systems.</p> <p>Patriot crew expertise may not have matched the level of responsibility needed for autonomous operations as a Patriot crew for one of the friendly fire incidents was certified “just prior to deployment” and assessed not ready for joint military operations (US Central Command 2004) p. 33.</p>	<ul style="list-style-type: none"> • Evaluation methods shall be established to confirm Patriot crew capability to handle lethal decisions and coordinate in dynamic and ambiguous joint military operations. • Certification levels shall be commensurate with increased responsibility up to autonomous Patriot operations.
	<p>4. Communications.</p> <p>Communication channels were missing for needed coordination. Passive communication channels existed: electronic identification (i.e. IFF) and aircraft using safe passage routing. However, active verbal or digital communications were not used between decision systems.</p>	<ul style="list-style-type: none"> • Recommend direct communication channels between the Patriot Battalion HQ and aircrew. • In more routine cases or when Battalion HQ does not have the workload bandwidth for direct communication with aircrew, direct communication channels between the Patriot Battery and aircrew are recommended. • If the workload may be too high for aircrew, then assign a communication node to facilitate real-time coordination efforts, such as AWACS or a Control and Reporting Center (CRC). The communication node can confirm accountability established. • Communication channels must handle the data load and information update rates

Table 39. Flawed Coordination Influences, Patriot and Aircrew Lateral Coordination

Eval	Patriot/Aircrew Flawed Coordination Influences	Patriot/Aircrew Lateral Coordination Recommendations
		<p>needed for Patriot and aircrew coordination. Predictability and common understanding need robust communication channels.</p> <ul style="list-style-type: none"> • Real-time information display and integration of battlefield operations was not a reality of the time. To compensate, additional vertical and lateral communication channels between decision systems shall be developed to facilitate information flow to Patriot-Aircrew coordination.
	<p>5. Group Decision-Making.</p> <p>Without language communications, verbal or digital, group decision-making could not occur.</p>	<p>There shall be protocols for Patriot and aircrew group decision-making for transit through protected airspace.</p>
	<p>6. Observation of Common Objects.</p> <p>Common objects may include the Patriot Battery, aircraft, and the air and ground order of battle. The Patriot radar was able to observe an airborne object. It is not clear to what level of detail Patriot and aircrew decision systems were able to observe the order of battle from mission materials or in real-time. One assessment of information integration during the Patriot incident came from a Defense Science Board (DSB) report (2005) claiming battlefield information was “a long way” from integration (p. 4).</p>	<ul style="list-style-type: none"> • Aircrew shall observe Patriot interactions, such as with radar warning receivers or data link information. • Patriot system must observe friendly coalition aircraft. Strategy protocols shall confirm Patriot and aircraft electronic systems and their operating modes are compatibility for observation. For example, a GR-4 “device” in “active on” mode may have contributed to their anti-radiation missile classification.
	<p>7. Authority, Responsibility, Accountability.</p> <p>Note: The aircrew did not know if they were safe to transit—there was no coordination accountability. Aircrew were nervous about the Patriots; an F-16 pilot stated, “The Patriots scared the Hell out of us” (Axe 2014).</p> <ul style="list-style-type: none"> • While the Patriot had an individual role and responsibility to protect ground forces and friendly aircrew, lateral coordination roles and responsibilities were not found in the literature. For example, aircrew were not proactively trying to establish their friendly identity with 	<ul style="list-style-type: none"> • Roles and responsibilities for Patriot and aircrew in lateral coordination shall be established, either with high level strategy (i.e. the AADP) or with lower level coordination strategy. <ul style="list-style-type: none"> ○ Coordination standards may dictate assignment of roles and responsibilities, such as first to establish two-way contact is responsible for coordination decisions. ○ Coordination by mutual adjustment may assign roles and responsibilities

Table 39. Flawed Coordination Influences, Patriot and Aircrew Lateral Coordination

Eval	Patriot/Aircrew Flawed Coordination Influences	Patriot/Aircrew Lateral Coordination Recommendations						
	<p>Patriot systems that covered airspace they may transit through. Relying on the IFF to work does not establish authority or responsibility for coordination.</p> <ul style="list-style-type: none"> Accountability that coordination was established was inadequate. Responsible for <i>lethal</i> decisions against potentially friendly airborne targets and the Patriot did not need to establish accountability with the aircraft. Accountability requires confirmation. For example, one may argue that electronic identification of the aircraft by the Patriot system established accountability. But, the aircrew do not have confirmation that they were indeed identified as friendly. 	<p>in real-time based on conditions.</p> <ul style="list-style-type: none"> There shall be confirmation from each decision system of the assignment of roles and responsibilities for transit through protected airspace. <ul style="list-style-type: none"> Confirmation can occur directly between aircrew and the Patriot from verbal or digital means, or can occur through a common communication node such as AWACS. Confirmation increases confidence in the coordination since each decision system gets a chance to demonstrate their understanding to the other. For example, the following verbal exchange establishes coordination accountability (read a1-b1, a2-b2): <table border="1" data-bbox="850 1020 1432 1417"> <thead> <tr> <th data-bbox="850 1020 1192 1079">(a) Viper 1 (aircrew)</th> <th data-bbox="1192 1020 1432 1079">(b) Patriot</th> </tr> </thead> <tbody> <tr> <td data-bbox="850 1079 1192 1325">(a1) “Patriot, Viper 1, 100 miles north of Kuwait inbound for arrival at checkpoint Charlie” (e.g. a pre-established checkpoint)</td> <td data-bbox="1192 1079 1432 1325">(b1) “Viper 1, Patriot has contact and tracking you southbound 20 thousand feet. Report Delta.”</td> </tr> <tr> <td data-bbox="850 1325 1192 1417">(a2) “Patriot, Viper 1, good contact, will report Delta.”</td> <td data-bbox="1192 1325 1432 1417">(b2) “Patriot copy”</td> </tr> </tbody> </table>	(a) Viper 1 (aircrew)	(b) Patriot	(a1) “Patriot, Viper 1, 100 miles north of Kuwait inbound for arrival at checkpoint Charlie” (e.g. a pre-established checkpoint)	(b1) “Viper 1, Patriot has contact and tracking you southbound 20 thousand feet. Report Delta.”	(a2) “Patriot, Viper 1, good contact, will report Delta.”	(b2) “Patriot copy”
(a) Viper 1 (aircrew)	(b) Patriot							
(a1) “Patriot, Viper 1, 100 miles north of Kuwait inbound for arrival at checkpoint Charlie” (e.g. a pre-established checkpoint)	(b1) “Viper 1, Patriot has contact and tracking you southbound 20 thousand feet. Report Delta.”							
(a2) “Patriot, Viper 1, good contact, will report Delta.”	(b2) “Patriot copy”							
	<p>8. Common Understanding.</p> <ul style="list-style-type: none"> The Patriot crew fired upon a target following standard arrival procedures to a friendly air base—common understanding was missing. The Patriot was allowed to operate autonomously from and with degraded communications to its Battalion HQ, which may have impacted its ability to receive updated and timely information. Some examples of missing or inadequate information for common understanding include: 	<ul style="list-style-type: none"> Common understanding shall be addressed with a common picture of the battlespace operations and airspace layout. Some examples include: <ul style="list-style-type: none"> Air and Ground Order of Battle: <ul style="list-style-type: none"> Location and movement of friendly aircraft, routes and targets, supported ground forces location and movement. Current and future Patriot Battery locations and 						

Table 39. Flawed Coordination Influences, Patriot and Aircrew Lateral Coordination

Eval	Patriot/Aircrew Flawed Coordination Influences	Patriot/Aircrew Lateral Coordination Recommendations
	<ul style="list-style-type: none"> ○ Air bases and standard departure and arrival routes. The GR-4 was shot on descent to home base, for example. ○ Location of friendly aircraft missions, and ingress/egress routes. The F/A-18 was shot and destroyed returning back to the ship, for example 	<ul style="list-style-type: none"> defended airspace coverage. <ul style="list-style-type: none"> ▪ Airbase locations. ▪ Overlap of aircrew and Patriot mission airspace coverages. ○ Airspace Control <ul style="list-style-type: none"> ▪ Safe passage corridors. ▪ Departure and arrival procedures. ▪ Patriot defended airspace restrictions and other prohibited airspaces. ▪ Pre-established checkpoints and airspace corridors for more secure communications (not giving away specific locations). ○ Abnormal Procedures <ul style="list-style-type: none"> ▪ Aircraft emergency routing ▪ Divert routing from other bases. ▪ Weather airspace routing ● A means to ensure updated and consistent information is received by Patriot and aircrew shall be established.
	<p>9. Predictability.</p> <p>For mutual adjustment coordination applicable to the accident, predictability is important. It is not clear that either decision system had information or knowledge to predict when and where coordination was needed, or what each other were doing. When the Patriot crew engaged a friendly aircraft returning to land at a friendly base and using normal arrival procedures, information and predictability were inadequate.</p>	<ul style="list-style-type: none"> ● Direct planning between decision systems shall be considered, such as direct interactions between Patriot Battalion HQ or Battery and aircrew prior to aircrew mission step. ● Adequate information update rates and communication channels needed to ensure changes in plans are received by appropriate decision systems. Information useful for predictability is: <ul style="list-style-type: none"> ○ Aircrew and Patriot systems mission information. ○ Theater level events that may impact coordination, such as based closures. ○ Weather for impact to air operations

Table 39. Flawed Coordination Influences, Patriot and Aircrew Lateral Coordination

Eval	Patriot/Aircrew Flawed Coordination Influences	Patriot/Aircrew Lateral Coordination Recommendations
		and potential divert scenarios that may impact prescribed routing.

6.5.3 Lateral Coordination Between Air and Land Component Command

Next, Joint Component Commander level lateral coordination was analyzed, which is represented in Figure 33. CAST-Coordination treated the process below Component Commander level coordination as one “Air Defense Coordinated” process.

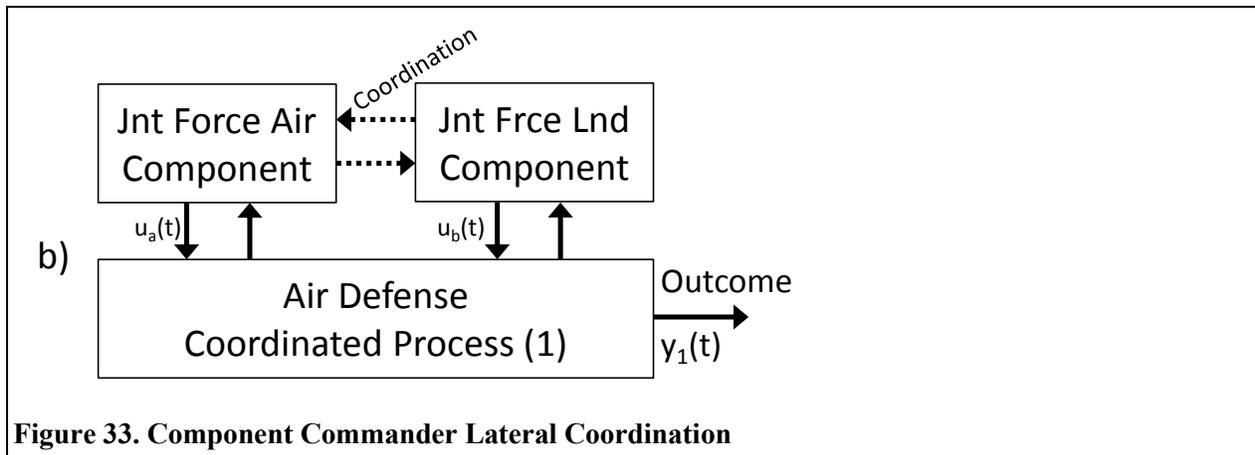


Figure 33. Component Commander Lateral Coordination

The Component Commanders must operationalize the Joint Force Commander’s and national level goals into implementable coordination strategy for the warfighters to execute. The lateral coordination at the highest level sets the constraints and coordination strategy for the supporting coordination in the decision-making hierarchy and ultimately for the physical process layer coordination that must occur for safe air defense coordination.

Decision System Descriptions:

- Joint Force Air Component Commander (JFACC). The JFACC is normally assigned Airspace Control Authority and Area Air Defense Commander, pertinent commands to air defense operations in this case study.
 - Decision Components (this was a typical JFACC description)
 - Airspace Control Authority (ACA). Responsible for control of airspace operations and development of procedures for control of the joint operational area.

with the requirements for theater level air defense should they exist. The AAMDC is the air defense operations coordination focal point for the JFLCC.

- Army Air and Missile Defense Command (AAMDC)
 - The commander AAMDC commands all Army theater level AMD forces.
 - May act as the TAAMDCOORD (Theater Army Air and Missile Defense Coordinator), which is the principal advisor and coordinator of counterair and missile defense operations for the JFLCC.
 - Is “normally” OPCON to the JFLCC and direct supports the JFACC/AADC (US Department of Defense Joint Staff 2012) p. II-6.
 - Acts as “...the Army forces (ARFOR) operational lead for counterair operations who ensure the ARFOR contribution is properly planned, coordinated, integrated, and synchronized” (US Department of Defense Joint Staff 2012) p. II-4.
 - Establishes liaison elements for coordination with major C2 elements, including the JFACC/AADC staff.
- Common Outputs Related to the Accident
 - Coordination strategy to ensure assigned air forces and ADA forces implement and execute the AADP and ACP as intended.

Context for Coordination:

- Joint Force Air Component Commander
 - Air operations tempo was high during first six weeks of war, with over 41,000 coalition sorties (Moseley 2003).
 - The coordination strategy at the time was reliant on electronic identification, with backup non-IFF safe passage procedures.
- Joint Force Land Component Commander
 - Early OIF had Patriot system elements still in transit to theater.
 - There were eventually over 60 Patriot fire units from US and coalition forces, which was considered “substantial” (Defense Science Board 2005) p. 1.
 - Patriot systems were the only way to counter the ballistic missile threat, anticipated to be massive like the Gulf War Scud volleys during 1991 (Anderson 2004).
- Lateral Coordination efforts included
 - Organizational integration of the functional component commands existed, but to what degree and the details were ambiguous in the literature.

- Liaison elements were established at the component levels, for example at the JFACC/AADC level in developing the AADP.

Flawed Lateral Coordination Evaluation:

Table 40 summarizes the evaluation of flawed coordination at the component command level that potentially influenced the Patriot friendly fire incident. The CAST-Coordination recommendations are given in the last column.

Table 40. Flawed Coordination Influences, Component Commander Lateral Coordination

Eval	Component Commander Flawed Coordination Influences	Component Command Coordination Recommendations
	<p>1. Coordination Goals (case 2 inadequate).</p> <ul style="list-style-type: none"> ● Fratricide avoidance was perhaps not a primary top-down goal at the onset of OIF. Observations that indicate inadequate safety goal priority: <ul style="list-style-type: none"> ○ The Defense Science Board (2005) commented that Patriots were not assigned an air defense role, which was ambiguous, but perhaps indicated inadequate integration with theater air defense. ○ At least initially in OIF, Patriot batteries were allowed to operate autonomously and allowed to operate in this case with degraded communication channels to battalion HQ. ○ Three separate friendly fire incidents (one against a Patriot battery) within a two-week timeframe. 	<p>Avoiding fratricide shall be a Component Commander priority coordination goal. The Services and lower level commanders must ensure fratricide prioritization is maintained down to the physical process decision systems.</p>
	<p>2. Coordination Strategy (case 2 inadequate).</p> <ul style="list-style-type: none"> ● A coordination strategy based on reliability of a physical system (i.e. the IFF) was inadequate. ● There may have been alternative non-IFF strategies (i.e. the safe passage routes), but when to use them was clearly ambiguous as alternative strategy attempts were not made by either the Patriot Battery or the GR-4 aircrew. ● High level direction on when lower-level commanders should or were authorized to refine coordination strategies was inadequate. For 	<p>Inadequate coordination strategy at this level directly influenced inadequate coordination at the lowest physical level (Patriot system crew and aircrew). Coordination strategy at Component level referred to air defense and airspace control systems.</p> <ul style="list-style-type: none"> ● Strategy to develop the AADP (Area Air Defense Plan) and ACP (Airspace Control Plan) shall be flexible to needs of the campaign and account for system and environmental uncertainty.

Table 40. Flawed Coordination Influences, Component Commander Lateral Coordination

Eval	Component Commander Flawed Coordination Influences	Component Command Coordination Recommendations
	<p>example, USCENTCOM confirmed that higher level coordination efforts did not develop local geographic-based coordination measures related to the Patriot: “[higher level coordination] did not promulgate any active Air Control Measures (ACM), Missile Engagement Zones (MEZ) or Restricted Operating Areas (ROA)/Restricted Operating Zones (ROZ) regarding Patriot” (p. 17).</p>	<ul style="list-style-type: none"> • The AADP and ACP shall be evaluated for conflicts in strategy. • A layered approach to coordination is recommended, with Patriot/aircrew coordination predominantly by mutual adjustment until standards can replace more routine warfare operations. • Coordination strategy shall provide unambiguous guidance related to the degrees of freedom that shall be addressed by lower level supporting coordination efforts.
	<p>3. Decision Systems.</p> <ul style="list-style-type: none"> • Inadequate decision systems involved in developing theater level coordination strategy may have influenced the accident. • Note. The literature suggested that AAMDC (Army Air and Missile Defense Command members), air component staff including AADC staff, and land component liaisons were responsible for developing the Area Air Defense Plan. It is unclear if technical experts on the fighter aircraft and Patriot systems, such as engineers and operators (e.g. pilots and Patriot operators) were participants in the decision-making coordination needed to develop the defended airspace strategy (i.e. the AADP). 	<p>Decision systems. The decision components needed for component lateral coordination should include those familiar with tactics, limitations, and joint staff authority and administrative functions:</p> <ul style="list-style-type: none"> • Air and land staff familiar with joint operations and establishing joint coordination strategy. • Theater air defense command staff familiar with air defense doctrine. • Expert pilots familiar with aircraft limitations and defensive system operations. • Expert patriot operators familiar with tactics and systems. • Patriot system technical experts (e.g. engineers, radar specialists, etc.).
	<p>4. Communications.</p> <p>By doctrine, communications and group decision-making were part of joint staff planning and operations. At this level, communications involved verbal and written communications channels. Communications were deemed acceptable at the Component Commander lateral coordination level.</p>	<p>No recommendations.</p>
	<p>5. Group Decision-Making.</p> <p>By doctrine, group decision-making occurred with</p>	<p>A coordination framework shall be used for development and evaluation of air defense</p>

Table 40. Flawed Coordination Influences, Component Commander Lateral Coordination

Eval	Component Commander Flawed Coordination Influences	Component Command Coordination Recommendations
	<p>developing the joint area air defense plan, accomplished with AAMDC experts. However, the conceptual framework used to develop the joint Area Air Defense Plan was potentially inadequate for coordination of joint operations. Safe coordination was needed, but not achieved in execution of coordination strategy that was used. The USCENTCOM report observed at echelons above brigade (i.e. higher level): "...when the [friendly fire] engagements occurred, the effort to prevent another seemed to focus on the Patriot unit or system vice taking a holistic approach to the problem" (p. 36).</p>	<p>(AADP) and airspace control (ACP) coordination strategies to ensure adequate and safe coordination between ADA and aircrew in theater operations.</p>
	<p>6. Observation of Common Objects.</p> <p>Inadequate observation of within decision system Component Commands and of the Service command chains may have influenced the accident. It is not clear that Component Commanders had internal observation channels of their respective component staff, let alone observation channels of external common objects. Observation channels were needed to ensure development, management, and distribution of the coordination strategy was accomplished.</p>	<ul style="list-style-type: none"> • Observation channels of the coordinated processes and outcomes shall be established. • Observation update rates shall be commensurate with system dynamics. Onset of wartime or release of new coordination strategy may require higher update rates than required four years into sustained combat operations. Higher update rates may provide more timely assessments of coordination implementation and execution. • Air and land component hierarchies shall ensure their observation channels on the coordinated process are of common objects. <ul style="list-style-type: none"> ○ Observe airspace operations where interdependency exists to ensure established strategy matches initial assumptions. ○ Staff liaison officers shall observe Service deficiencies in the implementation and execution of the AADP and ACP. Deficiencies shall be reported with recommendations to the liaised component leadership.

Table 40. Flawed Coordination Influences, Component Commander Lateral Coordination

Eval	Component Commander Flawed Coordination Influences	Component Command Coordination Recommendations
	<p>7. Authority, Responsibility, Accountability.</p> <ul style="list-style-type: none"> • Roles and responsibilities for the coordination of protected airspace. There was potential for overlapping and ambiguous coordination responsibility implementing the Area Air Defense Plan. • Authority and responsibility were inadequate for development of theater level and more refined airspace control strategy. For example (US Central Command 2004): "...unfortunately no ACOs [Airspace Control Orders] were used as risk mitigations for mixing aircraft and Patriot in a dynamic situation, both initially and ... when the Blue-on-Blue incidents occurred" (p. 36). 	<ul style="list-style-type: none"> • The authority chain and responsibility for the implementation of the area air defense plan shall be unambiguous. • Responsibility and authority shall be assigned to lower supporting coordination to develop strategy where degrees of freedom were afforded in the AADP or ACP. This recommendation helps ensure the high level strategy is refined as it reaches implementation at the physical layer. • Accountability. Confirmation of receipt and implementation of the coordination strategy from each joint force level is needed. • Authority and Responsibility shall be assigned to manage the coordination strategy and ensure it is updated to meet theater coordination goals and requirements.
	<p>8. Common Understanding.</p> <p>Common understanding was perhaps inadequate.</p> <ul style="list-style-type: none"> • In developing coordination strategy, the area air defense command decision components need to be aware of Patriot, aircrew, and decision component limitations. For example, what are the IFF limitations, aircraft limitations, or Patriot limitations such as knowing how aircraft may be identified as hostile missiles. • Information may have been inadequate to develop appropriate coordination strategy, such as Patriot unit locations and coverage areas. 	<ul style="list-style-type: none"> • Ensure scheduled opportunities exist (e.g. weekly meetings) to update staff on the coordination strategy implementation status and provide evaluation of the AADP in execution. • Experts shall be involved in coordination to assist in common understanding of system operations and coordinated defended airspace operations.
	<p>9. Predictability.</p> <p>Note. Predictability at the component level influenced coordination strategy development and may identify when strategy should change.</p> <ul style="list-style-type: none"> • Predictive models and understanding of the interactions between air force operations and 	<ul style="list-style-type: none"> • Developing the high level strategy shall use liaison elements and subject matter experts to help predict the consequences of current and alternative air defense strategies. • Maintaining and updating the air defense and air control coordination strategy shall refer to theater level near and far term plans

Table 40. Flawed Coordination Influences, Component Commander Lateral Coordination

Eval	Component Commander Flawed Coordination Influences	Component Command Coordination Recommendations
	<p>Patriot Corps air defense roles was inadequate. Predictive models that were perhaps inadequate for developing the coordination strategy include:</p> <ul style="list-style-type: none"> ○ Predicting when Patriot automation would classify aircraft as hostiles. For example, when departing or arriving Kuwait air base could aircraft appear hostile. ○ Predicting when overlap of airspace occurs for executing the missions. For example, the Patriot may defend airspace that F-16s are engaging enemy forces. ○ Movement of Patriot systems relative to Army and JFLCC Corps movements and the potential impact to aircraft operations. 	<p>to help identify when the coordination strategy may be inadequate.</p>

6.5.4 Evaluation of Supporting Coordination

Lateral coordination at the component command level produce the strategy needed for safe defended airspace operations and in some cases refine the Joint Force Commander goals for specific coordination goals. Lateral coordination is also needed to ensure common understanding at the given level and below in the decision-making hierarchy. Vertical and within decision system coordination played a part as well in the accident.

The Context for Coordination:

- The Joint Force Land Component Commander had Operational Control (OPCON) over Patriot systems, which meant the JFLCC had authority to organize and employ the Patriot systems as needed.
- The Joint Force Air Component Commander (JFACC) set the air defense coordination strategy for the Patriot Battalions as the AADC (Area Air Defense Commander) through the AADP (Area Air Defense Plan). Airspace control coordination strategy was also integral to safe coordination.

6.5.4.1 Within Decision System Coordination, Air Component

The Air Component Commander internal coordination was important to this incident, a relationship highlighted in Figure 34 by the dashed (blue) box. The Air Component is the top-level of the vertical hierarchy for joint air forces. The Air Component must work within the constraints and degrees of freedom afforded them by AADP and ACP to achieve coordination goals through development of a refined coordination strategy.

For example, electronic identification using the secure IFF Mode 4 was the given air defense coordination strategy. The air component decision system then had the responsibility to establish a safe coordination strategy for confirmation that the IFF is operating satisfactorily before entering and for the duration of transit through Patriot engagement zones.

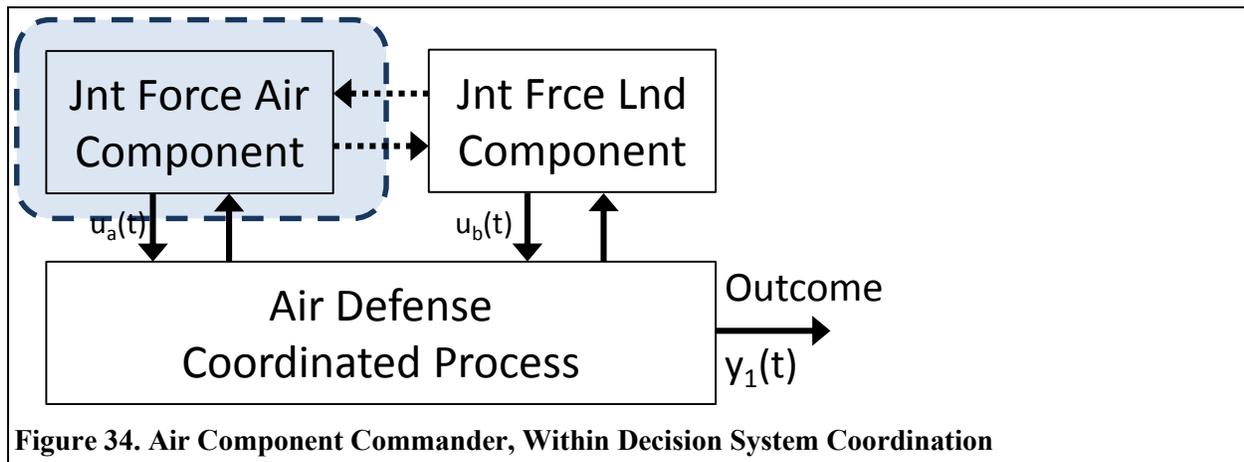


Figure 34. Air Component Commander, Within Decision System Coordination

Inadequate coordination (case 2):

- 2. Coordination Strategy. The air component command within decision system coordination inadequately addressed the overall coordination strategy. While the IFF reliability coordination strategy was in place, execution of it was ambiguous. The lynchpin of executing the coordination strategy was the IFF and the IFF send/receive functions were not checked for adequate operations prior to entering and during transit through a defended airspace.
- 5. Group Decision-Making (missing or inadequate). Group DM problem solving framework was perhaps inadequate to transform the joint AADP into a safe air component strategy. Another potential influence was Air Component staff did not have (flawed case 1) an organization to refine the AADP and ACP into air forces coordination strategy (JFACC staff discussions were not found in the investigations). The AADP provided the highest-level guidance, which then needed to be evaluated for implementation where degrees of freedom were afforded for air operations. In this case, there was flexibility on the IFF reliability strategy implementation which group DM did not address.
- 7. Authority, Responsibility, Accountability. JFACC staff needed to assign responsibility and authority to refine the AADP/ACP for implementation by the joint air forces.

6.5.4.2 Vertical Coordination, Land Component

Joint land forces vertical hierarchy coordination was evaluated, a relationship highlighted in Figure 35 by a dashed (green) box. Coordination in the vertical sense must ensure each successive layer in the land component decision-making hierarchy was passed the higher-level air defense goals and strategy; this was coordination by control implementing theater air defense strategy. In addition to goals and strategy, the information needed for physical process coordination must pass through the vertical coordination communication channels.

Inadequate coordination (case 2):

- 1. Coordination Goal. Goal priority potentially inadequate to avoid fratricide. Two decisions that suggested inadequate goal priority were:
 - Patriot batteries were allowed to operate independently with potentially limited air battle information from friendly forces.
 - The Patriot battery responsible for the fratricide was allowed to operate with degraded communications to Battalion HQ.
- 7. Authority, Responsibility, Accountability. There was inadequate accountability and confirmation that the Patriot algorithms and fire protocols were integrated with known threat and friendly information.
 - Arrival/departure procedures for Ali Al Salem, Kuwait air base.
 - Friendly versus hostile aircraft, and anti-radiation missile characteristics were inadequately integrated into Patriot automation.
- 8. Common Understanding. Common understanding of friendly air forces by the Patriot Battalion and Battery was inadequate due to the content, accuracy, and timeliness of needed information for safe air defense coordination.

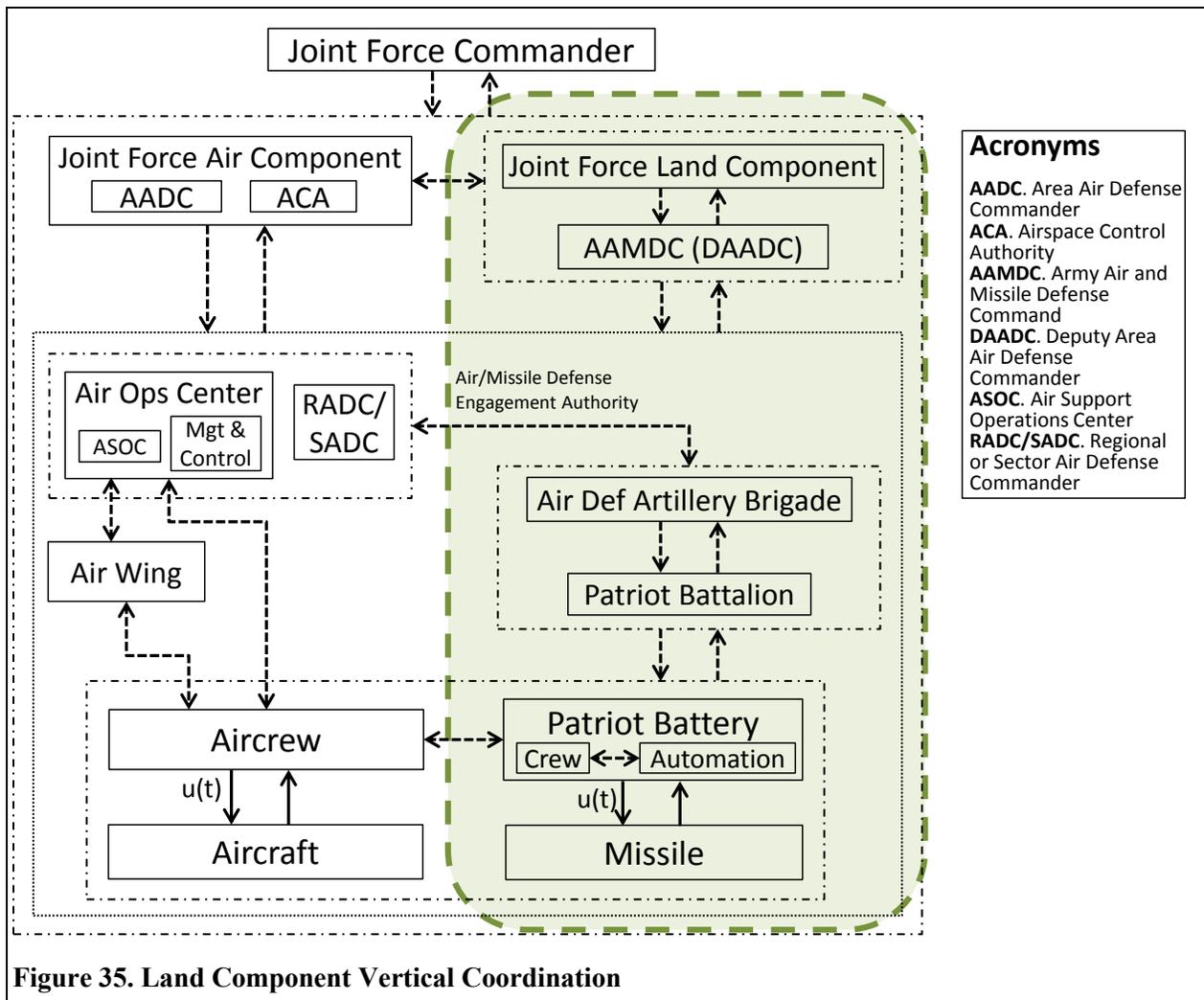


Figure 35. Land Component Vertical Coordination

6.5.4.3 Missing Lateral Coordination

Lateral between decision system coordination was evaluated below the Joint Component Command, highlighted in Figure 36 by the dashed (purple) box.

Lateral coordination used for airpower in offensive operations was well established. There were Ground Liaison Officers (GLO) and Air Liaison Officers (ALO) embedded in the tactical air and ground units respectively. The liaison elements coordinate to ensure lethal force was effectively and efficiently employed to meet the ground commanders' intent and to minimize friendly casualties.

The equivalent coordination for air defense operations was not documented for this accident; although as USCENTCOM (2004) noted, the GLO or aircrew could receive Patriot location information provided in the Airspace Control Order (p. 37). Formal lateral coordination efforts may not have existed between the Patriot Division/Battalion and Air Wing at the time. Current ADA doctrine (US Department of the Army 2016) singled out ADA Brigade coordination between the Control and Reporting Center and other higher level Air Component decision systems, but not coordination between the Air Wing or below to the aircrew (see section 6.3 above).

Formal lateral coordination air defense efforts may only have existed at the component command level, which was a problem for receiving needed coordination information. First, time constants generally increase the further away from the physical process a decision system coordinates (Mesarović et al. 1970). Second, the information becomes more susceptible to noise the longer the distance traveled and more decision system involved in interpreting the information. The timeliness and accuracy of information may be degraded in the round trip travel from physical process (e.g. Patriot) up to component command and again back down to the other physical process (e.g. aircrew).

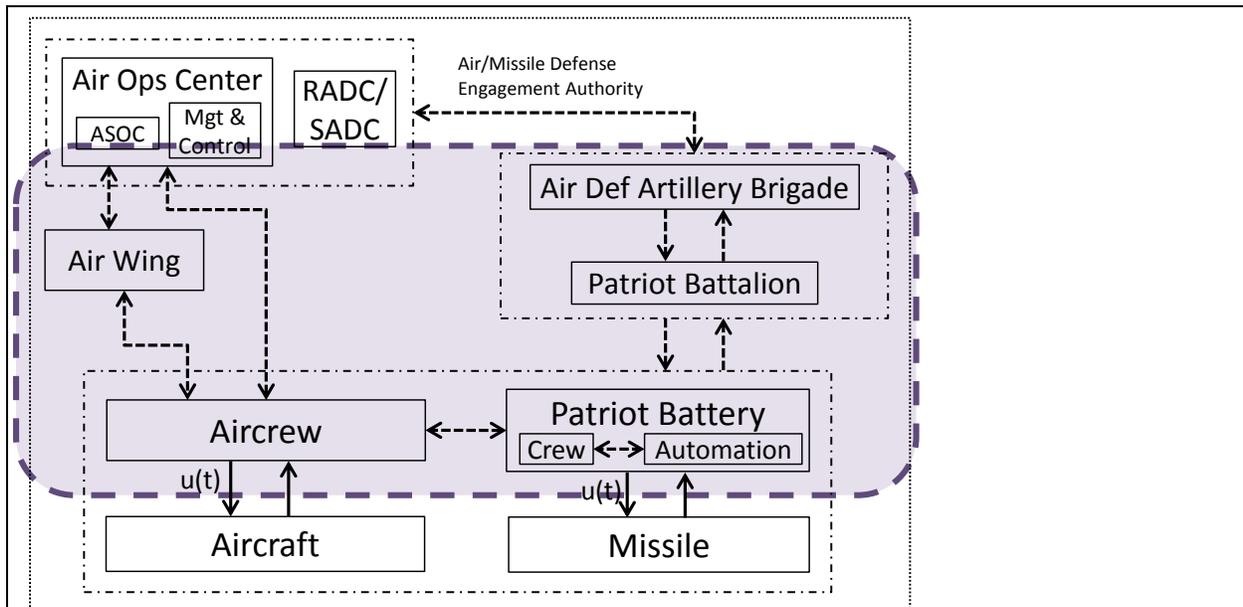


Figure 36. Lateral Supporting Coordination, Below Component Command

Missing lateral coordination can affect coordination of air and ground order of battle information, which hindered common understanding and predictability at the Patriot Battery-Aircrew coordination level.

Coordination Missing (case 1):

- 5. Group Decision-Making (and 2. Coordination Strategy)
 - Patriot Division/Battalion HQ and Air Wing lateral coordination may have been missing that would assist in local coordination planning and information flow needed for physical process layer coordination.
 - Patriot Division/Battalion HQ lateral coordination with Airspace control and Aircrew was largely missing. Lateral coordination at this level may assist in more real time coordination.

6.5.4.4 Supporting Coordination Recommendations

Table 41 describes recommendations to address flawed supporting coordination.

Table 41. Recommendations for Supporting Coordination

Coordination Elements	Recommendations for Supporting Coordination
1. Coordination Goals	<ul style="list-style-type: none"> • Vertical coordination of goals <ul style="list-style-type: none"> ○ The vertical coordination channels shall establish coordination goal priority within their hierarchy to assist in the survival of friendly aircrew coming back from offensive operations in Iraq. ○ Vertical coordination shall confirm receptions of goals and strategy by lower level decision systems.
2. Coordination Strategy	<ul style="list-style-type: none"> • Vertical coordination strategy <ul style="list-style-type: none"> ○ Vertical coordination strategy shall confirm component level coordination strategy: 1) disseminated to decision systems, 2) understood, 3) executed. ○ Vertical coordination shall ensure update and confirmation procedures are in place. ○ (within DS) There shall be a means to independently evaluate the Patriot automation was correctly modified in accordance with theater air defense coordination strategy, air operations information, and threat information.
3. Decision Systems	no recommendations
4. Comms	<ul style="list-style-type: none"> • Unambiguous vertical communication channels shall be established in each Service component hierarchy from top to bottom. This may assist in the implementation, execution, and evaluation of the coordination strategy.
5. Group DM	<ul style="list-style-type: none"> • Establish formal lateral coordination at a hierarchical level closer to the physical process. Lateral coordination closer to the physical process may improve information timeliness and accuracy. Common understanding, predictability, and confidence in coordination information may benefit as well. Coordination that is more flexible is possible with faster decision time constants than with component level decisions. <ul style="list-style-type: none"> ○ Lateral coordination shall be implemented between Air Wing and Patriot Division or Battalion levels for information exchange and local coordination strategy refinements if needed and authorized by the AADP. ○ Lateral coordination shall be implemented between the airspace control operations and the Patriot Battalion. The coordination assists in more real-time flow of order of battle information. This level of lateral coordination and information flow may suffice for safe coordination in more standard air defense operations.
6. Observation of Common Objects	<ul style="list-style-type: none"> • Vertical Coordination. Information of the physical processes must flow to and from Patriot and aircrew decision systems. Each Service component shall observe or have knowledge of each other, in particular aircrew and Patriot movements. <ul style="list-style-type: none"> ○ Liaison elements can assist with cross observation and information flow of

Coordination Elements	Recommendations for Supporting Coordination
	<p>slower time constant information.</p> <ul style="list-style-type: none"> ○ In current and future operations, data link information shall assist in cross observation of decision systems and other needed external information.
7. Authority, Responsibility, Accountability	<ul style="list-style-type: none"> ● The Patriot automation must be coordinable, which means vertical coordination with the Patriot system influences its decisions. The Patriot automation shall integrate: <ul style="list-style-type: none"> ○ Theater air defense and airspace coordination strategy. ○ Coordination constraints, such as rules-of-engagement. ○ Air and ground order of battle. ○ Friendly flight profiles. ○ Relevant air base arrival, departure and emergency flight procedures. ○ Coordination strategies that are geographically based, such as safe passage routes (e.g. IFF inoperative or loss of radio) or airspace control measures. ● Confirmation that Patriot algorithms were successfully modified to integrate current theater air defense and airspace control considerations shall be established through air defense coordination. Patriot automation may be coordinable, but this does imply it was coordinated with necessary information and theater air defense restrictions. ● Confirmation of coordination information shall be received at each decision system level. ● Autonomous Patriot operations shall have approval from authority that has a theater level perspective and influence. A recommendation would be approval from the delegated air defense engagement authority, whom may subsequently modify theater-level coordination strategy.
8. Common Understanding	No recommendations
9. Predictability	No recommendations

6.5.5 CAST-Coordination Recommendations, Summary

The Patriot friendly fire accident was largely a coordination problem and CAST-Coordination was used to develop recommendations that can lead to safe coordination. The following summarizes key coordination recommendations and insights derived from CAST-Coordination.

- There were two vertical hierarchies, the ground component and air components chains. Lateral coordination was needed to address safe coordination goals and strategy for theater operations. While component level lateral coordination was needed to provide coalition wide standards for coordination, the coordination was inadequate and unsafe for the environment. The higher-level decision systems can use a systems-theoretic approach, such as STPA-Coordination, to analyze and design safe coordination.

- Avoiding fratricide needed a commitment from the top Component Command levels starting with coordination goal priorities and in developing a safe coordination strategy for the air defense interdependencies.
 - A coordination goal shall be emphasized from the top-down—avoid fratricide.
 - The component command lateral coordination output needs to be: 1) a safe physical process coordination strategy and 2) a vertical coordination strategy for each Component decision system hierarchy that is clear on their roles and responsibilities for implementing and refining the high-level coordination strategy.
- The Patriot system engagement automation and friend/foe identification algorithms shall be coordinable. There shall be confirmation that air defense strategy, airspace control measures, and friendly and threat information were correctly integrated into Patriot automation. There shall also be means for confirming automation updates are current.
- The Patriot and aircrew decision systems must have a safe coordination strategy and means for establishing the enabling conditions.
 - The air defense coordination strategy should favor mutual adjustment given the internal and external uncertainty faced during early OIF. Communications between Patriot and aircrew decision systems was necessary to enable adequate and flexible coordination. Flexible coordination should have the ability to establish accountability, common understanding, and predictability in real-time if standards do not. Use of IFF for electronic identification was not a flexible coordination strategy.
 - A layered coordination strategy approach is prudent. Non-verbal IFF identification and safe passage routes are suggestions for alternatives that employ coordination by standardization. These strategies relied upon decision systems making isolated engagement decisions, which is perhaps best left to a last resort coordination strategy. If the circumstances were different, such as no communications and a missile defense Armageddon from Iraqi forces then a primary strategy reliant upon correct IFF identification may be reasonable; but those conditions were not the case.
- Creating lateral coordination between the Air Wing and ADA Brigade/Patriot Battalion level may benefit common understanding and predictability with reduced time delays of needed information. There is also potential to reduce loss of information from noise induced by travel distance up to the Component level for lateral communication before being coordinated back down. Reduced noise may increase information accuracy and assist in Patriot and aircrew confidence that the information is correct.

6.6 CAST-Coordination Results Comparison with Official Accident Reports

CAST-Coordination results are compared to the UK MOD (United Kingdom Ministry of Defence 2004) and the USCENTCOM official investigation reports. This section presents qualitative and quantitative

comparisons that provide numerous perspectives on key findings and recommendations. While the USCENTCOM report discusses all the Patriot friendly fire incidents, many of the general flawed coordination discussions are relevant to analysis of the British GR-4 incident. See APPENDIX F. Coding Results, CAST-Coordination Case Study for further details on the comparison analysis approach and primary data used in the comparisons.

6.6.1 US Central Command Accident Investigation

CAST-Coordination was qualitatively compared with selected excerpts from the USCENTCOM report (2004), described in Table 42.

Table 42. Qualitative Comparison with USCENTCOM Accident Investigation Report

Selected Findings and Recommendations	A Comparison with USCENTCOM Report
(US Central Command 2004) GR-4 Tornado Incident Recommendations (p. 23)	
<p>2. Coordination Strategy</p> <ul style="list-style-type: none"> • Airspace control measures “are activated to enable safe transit”. • “All forms of airspace control must be applied to ensure the potential risk of a friend-on-friend engagement is mitigated to the maximum extent possible.” 	<p>The statements provide a sense for the limited depth of recommendations related to coordination.</p> <ul style="list-style-type: none"> • The first statement implies that if you have a coordination strategy, it would be safe. The details of making the strategy safe are left to the reader. • The second statement claims “all forms” were needed, which is perhaps not actionable. <p>In contrast, CAST-Coordination recommendations address the coordination elements to implement that can lead to safe coordination outcomes.</p>
<p>2. Coordination Strategy</p> <ul style="list-style-type: none"> • “Leaders, who place units in this situation [Patriot autonomous operations] because of operational need, must ensure they have provided the maximum number of procedural and process checks to ensure the potential for a friend-on-friend engagement is minimized; and should ensure this unit is manned by their 	<p>The quote implies acceptance of independent Patriot operations as long as “maximum number of” prescriptions were in place. Even if one could determine the “maximum number,” it is not clear what the relationship is between the quantity of procedures and safe coordination in the incident. Rather procedures that implement adequate (or holistic) coordination can influence safe coordination outcomes. Substance over quantity is the recommended measure of a procedure’s value. In addition, coordination should be used and autonomous operations perhaps left as a last resort alternative.</p>

Selected Findings and Recommendations	A Comparison with USCENTCOM Report
most experienced crews”	
<p>General Recommendations</p> <ul style="list-style-type: none"> • Checklists “should be modified to ensure activation of all IFF modes” • Information on independent (or autonomous) Patriot battery operations needed to be distributed. • Airspace controllers advise aircrew to follow rules. 	<ul style="list-style-type: none"> • Inadequate coordination may not be solved with component solutions such as checklists to “ensure activation” or that the IFF meets some reliability threshold. • Releasing information about Patriot battery autonomous operations inadequately addresses the coordination problem. It is not clear how knowing the Patriot operated independently would change coordination or the outcome in this case study. • The MOD report claims the GR-4 “...followed the published speed and height procedures for a return to Ali Al Salem” (p. 5). The Patriot followed the rules-of-engagement. CAST-Coordination highlighted that standards (i.e. the coordination strategy) may inadequately address safe coordination.
<p>(US Central Command 2004) Coordination Efforts (e.g. Airspace Control Measure) Recommendations (p. 30-31)</p>	
<p>2. Coordination Strategy</p> <ul style="list-style-type: none"> • “ensure positive control of transiting aircraft” 	<p>Positive control may assist aircrew in following established procedures. However, control of aircraft does not ensure coordination with the Patriot system, which was the problem. The problem was not an aircraft problem or a Patriot problem alone.</p>
<p>4. Communications</p> <ul style="list-style-type: none"> • Ensure “connectivity to Patriot units” 	<p>One of the few coordination related recommendations was connectivity to Patriot units. Connectivity between Patriot systems and 1) Area Air Defense Engagement Authority (EA) and 2) airspace controllers were discussed. An important connection for consideration is <i>direct</i> Patriot and aircrew connectivity; however, this discussion was not found.</p>
<p>4. Communications</p> <ul style="list-style-type: none"> • “In all operations, airspace controllers...must be positioned and resourced with adequate communications equipment (to include Patriot units) to ensure reliable, responsive command and control can be applied” 	<ul style="list-style-type: none"> • CAST-Coordination recommended airspace controllers as a potential communication node for lateral coordination between Patriot and aircrew. Some coordination related concerns include: <ul style="list-style-type: none"> ○ A consideration is that adding a layer of communication protocols compared to mutual adjustment coordination between Patriot and aircrew directly may serve to delay coordination efforts and increase complexity. When decisions are made in seconds up to a minute (United Kingdom Ministry of Defence 2004), extra coordination processes may not be the best answer. ○ “Reliable, responsive command and control” should establish authority, responsibility, and accountability for

Selected Findings and Recommendations	A Comparison with USCENTCOM Report
	<p>coordination. Aircrew need confirmation that the Patriot identified and correlated their track as a friendly, initially and throughout transit to make sure they are not later tagged hostile. The Patriot system needs confirmation that a specific track is a friendly, especially if Patriot algorithms show differently.</p>

Coordination was not a primary focus of the investigation. Insightful into the local (component) versus holistic focus of the report was the executive summary on the F/A-18 friendly fire incident from (US Central Command 2004):

The ultimate conclusion of the investigation... is that a PATRIOT Air Defense Artillery (ADA) Battery erroneously identified two F/A-18s when its system failed to properly classify and correlate friendly aircraft and the system operators failed to properly execute their friendly protection responsibilities. A principal failure was a lack of human oversight and knowledge of system capabilities by ADA operators (p. 2).

There was perhaps a missed opportunity to address the airspace interdependency with a more holistic coordination solution and not use a Patriot- or aircrew-centric paradigm, similar to the GR-4 incident. Beyond the obligatory *improve coordination* and equivalent phrases there was limited substance in the recommendations to assist those responsible for taking actions. Further, how the recommendations integrated and lead towards more adequate and safe coordination was ambiguous. The qualitative comparison underscores a limited conceptual framework for identifying the need for and evaluating coordination in accident investigation involving Joint Military systems.

6.6.2 United Kingdom Ministry of Defence Accident Report

Selected excerpts from the UK MOD report were evaluated for a qualitative comparison to CAST-Coordination, given in Table 43.

Table 43. Qualitative Comparison to UK Ministry of Defense Accident Investigation Report

Selected Findings and Recommendations (United Kingdom Ministry of Defence 2004) pp. 4-5	A Comparison to CAST-Coordination
<p>2. Coordination Strategy</p> <ul style="list-style-type: none"> “If the position of the Patriot batteries and the likely ‘arcs’ of their missiles had been taken into account in writing the procedures, ZG710 [GR-4] might have 	<ul style="list-style-type: none"> Accounting for Patriot weapon engagement zones is a coordination strategy, but inadequately backed up with coordination enabling conditions. Under many scenarios, this coordination strategy can lead to unsafe outcomes. For example, Patriots change coverage and this is not updated in new routing or aircrew are not

Selected Findings and Recommendations (United Kingdom Ministry of Defence 2004) pp. 4-5	A Comparison to CAST-Coordination
taken a different route.”	able to follow routing due to aircraft emergency conditions.
2. Coordination Strategy and 4. Communications <ul style="list-style-type: none"> • “The Board concluded that airspace routing, airspace control measures and a breakdown in planning and communication were contributory factors in the accident.” 	<ul style="list-style-type: none"> • The contributing factors listed in the quote are most akin to the coordination framework. However, the level of detail is perhaps too broad to be useful. • Inadequate communication is highlighted by both CAST-Coordination and the MOD. Communication is an enabling process and simply needed to exist. It did not exist at the Patriot crew and aircrew level.
2. Coordination Strategy <ul style="list-style-type: none"> • An additional recommendation from the Commander-In-Chief, Royal Air Force: “A positive challenge and response IFF check be completed after take-off between every aircraft and an appropriate control authority.” 	<ul style="list-style-type: none"> • The recommendation inadequately addresses the air defense interdependency critical to the GR-4 shoot down. The lynchpin to the entire IFF reliability coordination strategy was that it must be working prior to entering <i>and</i> for the duration of transit through a Patriot engagement zone. Checking the IFF at any other time, from engine start and throughout a mission, may be inadequate.
5. Group Decision-Making <ul style="list-style-type: none"> • Recommend (of 12 recommendations): “Closer co-ordination is implemented between planning and operations organisations regarding airspace usage.” 	<ul style="list-style-type: none"> • The recommendation for “closer co-ordination” is a typical recommendation and ambiguous. “Closer” may be difficult to operationalize and measure. The recommendation was chosen to show that some abstractions are too broad for comparison to CAST-Coordination.

6.6.3 Defense Science Board Report

The Defense Science Board (DSB) reported on Patriot OIF operations and its results were similar to the accident investigations. They are discussed in this section to provide an independent perspective on causation and recommendations.

The Board concluded: “Two of the main shortfalls seen in OIF performance transcend just the Patriot system; they involve combat identification and situational awareness” (Defense Science Board 2005) p. 1. Related to the combat identification, the DSB discussed how the IFF Mode 4 “performed very poorly” (p. 2), which in safety terms was a reliability assessment. However, CAST-Coordination results had numerous examples where even having perfect IFF reliability, the Patriot friendly fire shoot down can still occur. The DSB report recommendation stated: “We have to fix Mode IV and institute additional

protection measures such as safe return corridors for our aircraft” (p. 2); this highlights the use of a traditional failure chain paradigm for accident causation.

The DSB concluded a “significant” lack of situational awareness was a factor and assessed the “Patriot battery on the battlefield can be very much alone” (p. 2). The term was used in the other accident investigations. USCENTCOM concluded “...the key concept was increasing situational awareness of joint warfighters” (US Central Command 2004) p. 41. The MOD report acknowledged inadequate situational awareness. The DSB recommendation was “...we must improve the situational awareness of air defense systems” (p. 3), which was a valid recommendation but perhaps too broad to be useful. CAST-Coordination associated situational awareness with the coordination element predictability.

Relative to the coordination framework, the DSB report addressed two of nine elements: coordination strategy (i.e. IFF component reliability) and predictability (i.e. situational awareness).

6.6.4 CAST-Coordination Comparison, Frequency Analysis

A frequency analysis was performed on each accident investigation and CAST-Coordination for comparison. Efforts were made to be consistent in the abstraction level used for the frequency analysis of accident influences and recommendations across the comparisons. As such, absolute numbers are approximate and more emphasis should be placed on the data trends and qualitative observations in the comparison. The comparison results for accident influences are in Table 44 and for coordination recommendations in Table 45.

Table 44. Comparison to CAST-Coordination Accident Influences

Coordination Elements	Coordination Contributing Factors		
	USCENTCOM	UK MOD	CAST-Coordination
1. Coordination Goals	0	0	2
2. Coordination Strategy	3	3	6
3. Decision Systems	1	0	2
4. Communications	1	1	1
5. Group Decision-Making	0	0	5
6. Observation of Common Objects	0	0	2
7. Authority, Responsibility, Accountability	0	0	8
8. Common Understanding	1	2	5
9. Predictability	1	1	4
Total Coordination-Related Influences	7	7	35

Observations from comparison of accident influences related to coordination in Table 44 include:

- CAST-Coordination found potential accident influences related to the nine coordination elements identified in the coordination framework, while the official investigation reports each addressed less than nine elements.
- Authority, responsibility, accountability was one of the major coordination influences on the accident, but was not acknowledged in the official reports.
- Each investigation report acknowledged the coordination strategy was an influence. However, CAST-Coordination suggested that the coordination strategy itself was inadequate versus the more obvious influence that the GR-4 IFF potentially failed.
- Communications was recognized by each investigation. However, CAST-Coordination recommended a more direct communication channel between the aircrew and the Patriot Battalion HQ or even Battery unit.
- CAST-Coordination found a majority of potential contributing factors related to the coordination enabling conditions, which were largely ignored by the accident investigation reports except for acknowledgement of low situational awareness.
- CAST-Coordination identified prioritization of fratricide avoidance, the coordination goal, was perhaps inadequate. Political limitations may have prevented such a claim in the official reports.

Table 45. Comparison to CAST-Coordination Recommendations

Coordination Elements	Coordination Recommendations		
	USCENTCOM	UK MOD	CAST-Coordination
1. Coordination Goals	0	0	2
2. Coordination Strategy	5	2	9
3. Decision Systems	1	1	7
4. Communications	2	0	6
5. Group Decision-Making	0	1	4
6. Observation of Common Objects	0	0	8
7. Authority, Responsibility, Accountability	0	0	11
8. Common Understanding	4	1	6
9. Predictability	2	0	6
Total Coordination Recommendations	14	6	59

Observations from comparison of coordination-related recommendations in Table 45 include:

- CAST-Coordination recommendations addressed holistic and safe coordination between the Patriot and aircrew. The same cannot be determined from the USCENTCOM and MOD recommendations.
- CAST-Coordination had recommendations for observation of common objects in several coordination relationships of the Joint structure, which was not addressed in the accident investigations. An example is Component Command observations of their respective vertical hierarchies for implementation and execution of the air defense and airspace control coordination strategy.
- Authority, responsibility, and accountability was noticeably absent from the official accident reports. CAST-Coordination placed emphasis on improving accountability at the physical process layer (e.g. aircraft have confirmation they are tracked as a friendly) and in higher-level coordination (e.g. Component responsibility to refine theater coordination strategy to address degrees of freedom).
- The quantitative and qualitative trends suggest a potential benefit from using CAST-Coordination as a framework to develop recommendations for safe coordination in comparison with the techniques used by SC-203 and USCENTCOM experts.

6.7 Summary, CAST-Coordination for Accident Investigation

The Patriot friendly fire accident investigation case study demonstrates that CAST-Coordination can derive additional insights not documented in official accident reports. The comparisons suggest that CAST-Coordination improves explanatory power for coordination-related causal factors and improves ability to generate detailed and actionable recommendations for safe coordination.

USCENTOM (2004) wrote in their Patriot friendly fire investigation report: “Any finding or inference that inadequate Airspace Control Measures (ACMs) were a factor in these accidents [Patriot friendly fire] has to be considered in the total context of the combat operation (p. 11).” While the dictum suggests using systems-theoretic principles, USCENTCOM was perhaps ahead of its time given the limited analysis methods available for accident investigations during the early 2000s.

There were human error taxonomies, such as HFACS, ad-hoc investigation and brainstorming techniques as former state-of-the-art. In this case study, a new system-theoretic approach was successfully demonstrated with CAST-Coordination. Using extended CAST, interested stakeholders can now analytically derive results and recommendations from analysis of system functions, including coordination, “in the total context.”

In summary, the case study suggests that the coordination framework and CAST-Coordination are a useful and valid means for accident analysis of fratricide incidents in joint military operations. Implementing CAST-Coordination recommendations may assist in the design of coordination to avoid fratricide in joint military operations.

[Page intentionally left blank]

7 CONCLUSIONS

Coordination is the behavior to address interdependency between decision systems. In many complex work domains, success depends on cooperation among many participating decision systems, which may include multiple humans and autonomous technologies. In these work domains, coordination is essential for safety.

This thesis introduced STPA- and CAST-Coordination extensions that can be used for analysis and design of safe coordination behavior in sociotechnical systems. To assess their utility, two case studies were accomplished. One case study applied STPA-Coordination to UAS integration investigating collision avoidance. The second case study applied CAST-Coordination to air defense operations investigating friendly aircrew fratricide by Patriot missile systems during Operation Iraqi Freedom. Both case studies demonstrated: 1) the successful application of respective extensions and 2) the beneficial insights gained over the results documented in the official reports, which are results derived from using traditional safety analysis methods.

Across case studies and comparisons, the results are promising. The results suggest the coordination framework and analysis extensions are useful and support an argument towards their validation. Analysis and design of within and between decision system coordination in other safety-critical complex work domains may benefit from the use of STPA- and CAST-Coordination.

7.1 Contributions to Knowledge

The state-of-the-art for safety analysis methods have limited to no guidance for analysis of coordination influences on safety. With this thesis, state-of-the-art safety analysis methods can now address coordination behavior. The overall thesis contribution to knowledge is the introduction of STPA-Coordination and CAST-Coordination, which extend current STPA and CAST to address hazardous coordination behavior. There are several significant contributions introduced in the thesis.

7.1.1 Introduced a Coordination Framework

The concept of coordination for safety analysis is limited in the literature. A framework was needed to provide explanatory power for coordination observed in sociotechnical systems. This thesis presents one, which was inspired by theoretical literature. The following four points summarize the decisions and decomposition assumptions used to guide the observations and analysis of coordination:

- **Decision Systems.** A decision system is introduced. The decision system is responsible for making decisions for a common output, such as actions, and can be composed of one or more decision components. The decision system is a fundamental unit for analysis of coordination.
- **Coordination Elements.** Coordination behavior is decomposed into three categories: basic components, processes, and enabling conditions. Each category is further refined into nine coordination elements, including: 1. Coordination goals; 2. Coordination strategy; 3. Decision

systems; 4. Communications; 5. Group decision-making; 6. Observation of common objects; 7. Authority, responsibility, and accountability; 8. Common understanding; 9. Predictability.

- Set of Fundamental Coordination Relationships. Coordination relationships can exist within and between decision systems, and in the vertical and lateral dimensions. When also accounting for the process controlled by decision systems, a set of four fundamental coordination relationships are derived. The relationships are used to guide analysis.
- Internal and External Coordination Perspectives. The coordination problem can be viewed using internal and external perspectives. The internal perspective addresses whether coordination consisted of needed coordination elements or not. The external perspective addresses the coordination strategy relative to safe outcomes, including temporal factors. Safe coordination requires the necessary elements, a coordination strategy that leads to safe outcomes, and a coordination strategy that is established in time to influence an outcome.

The coordination framework is the theoretical foundation for STPA- and CAST-Coordination.

7.1.2 Extended STPA with STPA-Coordination

STPA-Coordination is introduced, which extends STPA with additional steps to identify coordination scenarios that may lead to unsafe control actions (i.e. hazards). STPA-Coordination steps include:

1. Identify the interdependency.
2. Identify the coordination relationship.
3. Use flawed coordination guidance (i.e. four flawed coordination cases and nine coordination elements) to identify coordination scenarios that can lead to unsafe control actions.

7.1.3 Introduced Analytical Guidance for STPA-Coordination

Flawed coordination guidance is introduced for use with STPA-Coordination consisting of four flawed coordination cases and nine coordination elements. The flawed coordination cases include: 1) missing coordination; 2) inadequate coordination; 3) coordination strategy directly leads to hazards; and 4) coordination strategy established late. Flawed coordination guidance is used to identify coordination scenarios that can lead to unsafe control actions.

7.1.4 Extended CAST with CAST-Coordination

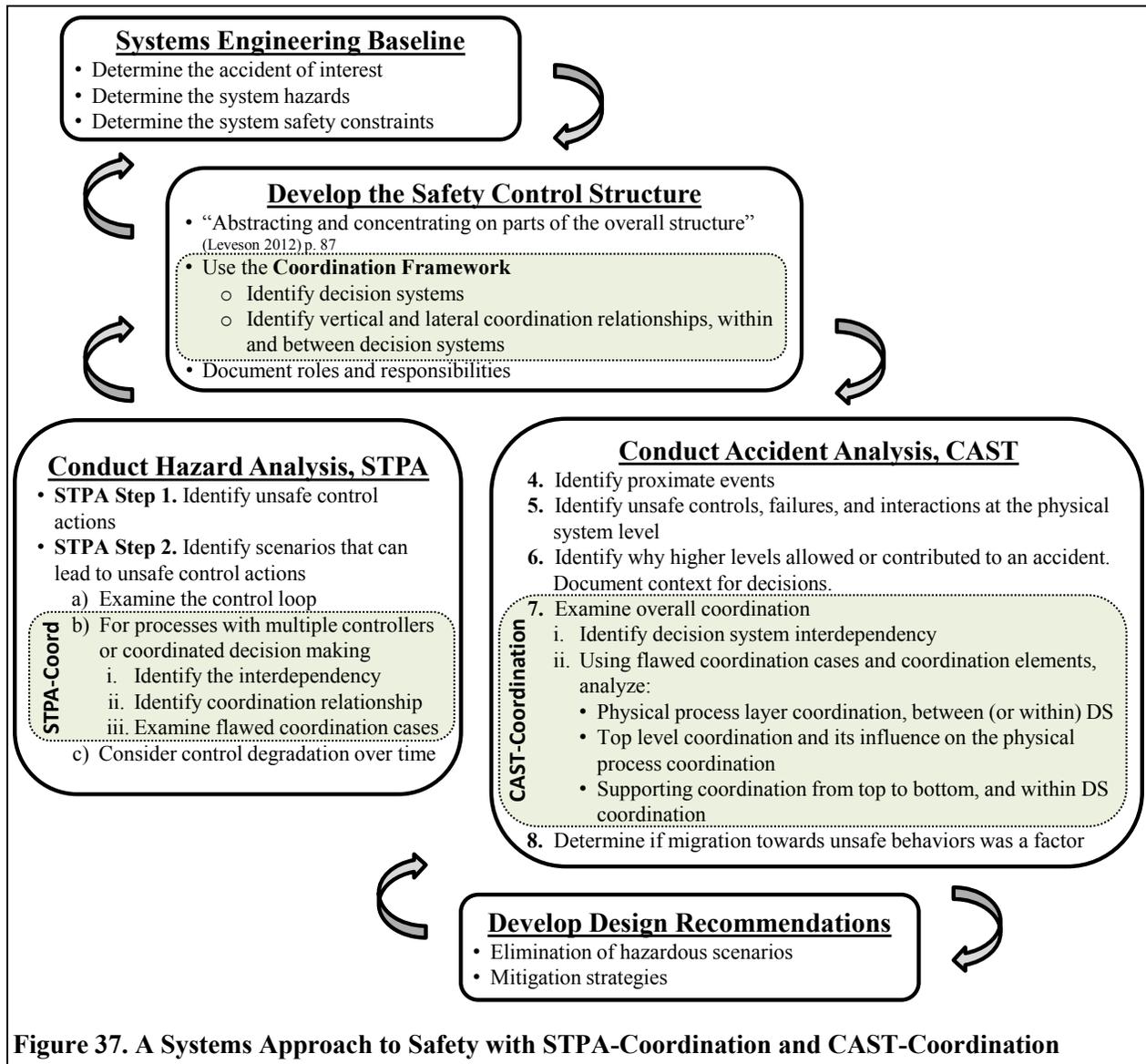
CAST-Coordination is introduced to provide accident analysis guidance focused on coordination, which is guidance derived from the coordination framework and STPA-Coordination. CAST-Coordination extends CAST with additional steps for analysis of coordination, including:

- Identify decision system interdependency.
- Use guidance provided by the flawed coordination cases and coordination elements to analyze:
 - Physical process level coordination, between (or within) decision systems.

- Top-level coordination and its influence on the physical process coordination.
- Supporting coordination. Decision-making hierarchy coordination from top to bottom and within decision system coordination.

7.1.5 Guidance for a Systems Approach to Safety Engineering

A systems approach to safety is embedded in systems engineering efforts. The coordination framework and analysis extensions can be used to guide safety engineering efforts as highlighted (green) in Figure 37. STPA- and CAST-Coordination extensions assist in deriving design recommendations for coordination that leads to safe outcomes, through either elimination or mitigation of hazardous scenarios.



7.2 Limitations and Future Work

The overall research objective was met: to develop systems-theoretic safety analysis extensions for coordination. However, there are limitations for discussion, which lead into future work.

First, the case study comparisons were subject to researcher bias. Bias would be most apparent in the coding of the other official analyses and reports, which can directly influence the assessed benefits from using STPA and CAST extensions. To minimize bias, a structured approach to coding was used as documented in the thesis and appendices. In addition, the coordination framework itself provided guidance and clear descriptions with its coordination elements, which was the primary comparison. All coding was done by the author, which assisted in having consistent results. Last, the results were qualified with the precision commensurate to the comparison rigor, which was mostly qualitative. Comparison of quantitative results was qualified as being approximate and not statistically significant. Rather, emphasis was placed on the evaluation of data trends across comparisons and case studies, and from qualitative comparisons.

Second, unintentional errors of fact in omission or commission may be in the CAST-Coordination case study as information in some cases was ambiguous, potentially conflicting, and heavily redacted (e.g. USCENTCOM report). To minimize potential errors, self-study used accident and related reports, and Service and Joint Doctrine. Discussion with an experienced Air Defense Artillery US Army officer was accomplished, as well as drawing from personal Iraq combat experiences. Analysis descriptions used qualifying statements where appropriate to acknowledge the ambiguity. In addition, CAST-Coordination abstraction levels were used commensurate with the known information. The higher-level abstraction results would then apply to the details whatever they were, are currently, or will be in the future.

Next, the coordination framework was derived from selected literature and perspectives deemed integral to understanding coordination behavior holistically. The coordination framework is one way to approach coordination in analysis and design of safety in complex sociotechnical systems; it is not the only way or the correct way. It is possible that additional factors were left out of the framework that may be important for safety analysis and design. Other frameworks may find different coordination representations and relationships not addressed by the one presented in this thesis. For example, there may be additional coordination elements or broader coordination categories than components, processes, and enabling conditions.

The last limitation is that STPA- and CAST-Coordination validation is in nascent stages. However, the demonstrated utility and beneficial comparison results in the two real-world case studies are promising and suggest further validation is warranted.

Not a limitation, but important discussion is that CAST- and STPA-Coordination are extensions that can be used by anyone. However, the extensions alone cannot derive hazardous scenarios and system design recommendations. Expert knowledge of functions, interactions, and understanding of internal and external context is information needed to accomplish the analysis and derive recommendations. The extensions provide analytical guidance to analysis that as demonstrated can provide improved results over other methods, including ad-hoc brainstorming.

Future work has several exciting research paths in the application of the coordination framework and STPA/CAST-Coordination, and in the refinement of coordination analysis guidance. The extensions were

developed for analysis of coordination and future work should apply them to the coordination problems observed in many sociotechnical systems. Further applications would serve to improve validation of the coordination framework and STPA/CAST extensions. Such application research would also have practical implications of assisting in the safety analysis of real-world accident and engineering design problems.

Future work can also refine the developed methods and analysis guidance. The analysis guidance, particularly use of the flawed coordination cases and nine coordination elements, may improve with more formal research methods. Expert and user studies and other qualitative inquiry may evaluate the general guidance presented in this thesis or may develop more local coordination analysis guidance for particular domains and systems.

Coordination safety analysis guidance for within decision systems is a potential broad area for research. Human-human coordination, human-automation coordination, and larger team combinations are areas for future investigation of the flawed coordination analysis guidance. Coordination interactions that were typically framed as a component problem, such as analysis of a single human or automation alone, now have an analysis framework to address the interdependency within context. Future work may investigate how the coordination framework and flawed coordination guidance may assist in the design and evaluation of safe human-automation interfaces. The design and evaluation of automation-automation (i.e. robot-robot) or human-robot between decision system coordination is another area for inquiry. How can the coordination framework and flawed coordination guidance assist in the analysis of and safe design of human-robot interactions?

STPA has analysis guidance for identifying unsafe control actions using the control feedback loop and using flawed coordination guidance introduced in this thesis. Decisions are the other goal-directed behavior, which is applicable to humans and automation decision systems and components. Decisions were not explicitly addressed by this thesis. Future research opportunities exist to extend STPA analysis guidance to address group and individual decision-making influences on unsafe control actions. The use of decision theory may provide insights into framing and analyzing the decision problem.

Last, the coordination framework was the theoretical foundation for this thesis, but its utility may be beneficial to more than safety. Future work may look more broadly at the coordination framework and its application to theory of management and organizational sciences from which it was derived. Similarly, the flawed coordination guidance is in theory applicable to any system emergent outcome that can be defined by acceptable outcomes. While this thesis focused on safe outcomes, other stakeholders can define acceptable outcomes more broadly.

[Page intentionally left blank]

LIST OF DEFINITIONS AND ACRONYMS

A. Accident	BCD. Battlefield Coordination Detachment
AADC. Area Air Defense Commander	BDS. Between Decision Systems
AADP. Area Air Defense Plan	C2. Communications and Control, or Command and Control
AAMDC. Army Air and Missile Defense Command	CA. Collision Avoidance
ACA. Airspace Control Authority	CAS. Collision Avoidance System
ACM. Airspace Control Measure	CAST. Causal-Analysis based on STAMP
ACO. Airspace Control Order	CAT. Collision Avoidance Threshold
ACP. Airspace Control Plan	CCE/FH. Catastrophic Collision Event per Flight Hour
ACS. Airspace Control System	CFR. Code of Federal Regulations
AD. Air Defense	ConOps. Concept of Operations
ADA. Air Defense Artillery	Coord. Coordination
ADS-B. Automatic Dependent Surveillance-B	CPA. Closest Point of Approach
AGL. Above Ground Level	CRC. Control and Reporting Center
AH. Abstraction Hierarchy	CSE. Cognitive Systems Engineering
AMD. Air and Missile Defense	CSS. Complex Sociotechnical System
AMDC. Air and Missile Defense Commander	DAA. Detect-and-Avoid
AOC. Air Operations Center	DCA. Defensive Counterair
AOD. Air Operations Directive	DM. Decision-Making
ARA. Authority, Responsibility, Accountability	DOD. Department of Defense
ARFOR. Army Forces	DS. Decision System
ARM. Anti-Radiation Missile	DSB. Defense Science Board
ASOC. Air Support Operations Center	EPU. Emergency Power Unit
ATC. Air Traffic Control	FDC. Fire Direction Center
ATM. Air Traffic Management	FH. Flight Hour
ATO. Air Tasking Order	FHA. Functional Hazard Analysis/Assessment
AWACS. Airborne Warning and Control System	

fpm. Feet per Minute	NMAC. Near Mid-Air Collision
GA. General Aviation	NSE. No Safety Effect
H. Hazard	OP. Operational Control
HALE. High Altitude, Long Endurance	OPCON. Operational Control
HF/E. Human Factors/Ergonomics	PHA. Preliminary Hazard Analysis
HFE. Human Factors Engineering	PHL. Preliminary Hazard List
ICAO. International Civil Aviation Organization	RA. Resolution Advisory
ID. Identification	RADC. Regional Air Defense Commander
IFATCA. International Federation of Air Traffic Controllers' Associations	RR. Risk Ratio
IFF. Identification, Friend or Foe	RTB. Return-to-Base
IFR. Instrument Flight Rules	RTF. Return-to-Force
IMC. Instrument Meteorological Conditions	SADC. Sector Air Defense Commander
JAOC. Joint Air Operations Center	SC. Safety Constraint
JFACC. Joint Force Air Component Commander	SMS. Safety Management System
JFC. Joint Force Commander	SPINS. Special Instructions
JFLCC. Joint Force Land Component Commander	SRM. Safety Risk Management
JOA. Joint Operations Area	SST. Self-Separation Threshold
JP. Joint Publication	ST. Strategic Control
MABA-MABA. Men are better at, Machines are better at	STAMP. Systems-Theoretic Accident Model and Processes
MAC. Mid-Air Collision	STPA. Systems-Theoretic Process Analysis
MIL-STD. Military Standard	STPA-Coord. STPA-Coordination
MIN. Minimal (Risk)	TA. Traffic Advisory
MMS. Man-Machine System	TAAMDCOORD. Theater Army Air and Missile Defense Coordinator
MOD. Ministry of Defence	TACON. Tactical Control
NAS. National Airspace System	TCA. Tactical Control Assistant
NDM. Naturalistic Decision-Making	TCAS. Traffic Collision and Avoidance System
	TCO. Tactical Control Officer

TD. Tactical Director
TDA. Tactical Director Assistant
TLS. Target Level of Safety
UA. Unmanned Aircraft
UAS. Unmanned Aircraft System or Unmanned
Aerial System
UAV. Unmanned Aircraft Vehicle
UCA. Unsafe Control Action
UK. United Kingdom
US. United States
VFR. Visual Flight Rules
VMC. Visual Meteorological Conditions
WCV. Well Clear Violation

[Page intentionally left blank]

BIBLIOGRAPHY

- Anderson, C.C.A., 2004. Air and Missile Operation Defense: Iraqi Freedom. *Army*, (January), pp.40–47.
- Annett, J. & Duncan, K., 1967. Task Analysis and Training Design. *Occupational Psychology*, 41(July), pp.211–221. Available at: <http://eric.ed.gov/?id=ED019566> [Accessed December 16, 2014].
- Antoine, B., 2013. *Systems Theoretic Hazard Analysis (STPA) Applied to the Risk Review of Complex Systems: An Example from the Medical Device Industry*. Massachusetts Institute of Technology.
- Argote, L., 1982. Input Uncertainty and Organizational Coordination in Hospital Emergency Units. *Administrative Science Quarterly*, 27(3), pp.420–434. Available at: <http://www.jstor.org/stable/2392320>.
- Ashby, W.R., 1956. *An Introduction to Cybernetics*, London, UK: Chapman & Hall. Available at: <http://pcp.vub.ac.be/books/IntroCyb.pdf>.
- Ashby, W.R., 1981. Information flows within co-ordinated systems. In R. Conant, ed. *Mechanisms of Intelligence: Ashby's Writing on Cybernetics*. Seaside, CA: Intersystems Publications, pp. 127–134.
- Ashby, W.R., 1958. Requisite Variety and Its Implications for the Control of Complex Systems. *Cybernetica*1, 1(2), pp.83–99. Available at: <http://pcp.vub.ac.be/books/AshbyReqVar.pdf>.
- Axe, D., 2014. That Time an Air Force F-16 and an Army Missile Battery Fought Each Other: Fighter pilots feared flawed air-defense system. *War is Boring*. Available at: <https://medium.com/war-is-boring/that-time-an-air-force-f-16-and-an-army-missile-battery-fought-each-other-bb89d7d03b7d#.iv9ezsz02> [Accessed March 14, 2016].
- Beadle, A., 2010. Problems When Displaying TCAS RA's at Controller Working Positions. , (1), p.2.
- Bell, B.J. & Swain, A.D., 1983. *A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants (NUREG/CR-2254)*, Albuquerque, NM.
- Bernstein, N., 1967. *The Co-ordination and Regulation of Movements* First Engl., Oxford: Pergamon Press Ltd.
- Bertalanffy, L. von, 1968. *General System Theory. Foundations, Development, Applications* Revised., New York: George Braziller, Inc.
- Bertalanffy, L. Von, 1972. The History and Status of General Systems Theory. *Academy of Management Journal*, 15(4), pp.407–426. Available at: <http://amj.aom.org/content/15/4/407.short> [Accessed August 10, 2014].
- Blanchard, B.S., 2006. *Systems Engineering and Analysis* 4th ed., Upper Saddle River, NJ: Pearson Prentice Hall.
- Brehmer, B., 1992. Dynamic Decision Making: Human Control of Complex Systems. *Acta Psychologica*, 81(3), pp.211–241.
- Cataldo, M. et al., 2006. Identification of Coordination Requirements: Implications for the Design of Collaboration and Awareness Tools. In *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*. Banff, Alberta, Canada: ACM, pp. 353–362.
- Celik, M. & Cebi, S., 2009. Analytical HFACS for investigating human errors in shipping accidents. *Accident Analysis and Prevention*, 41(1), pp.66–75.
- Checkland, P., 1981. *Systems Thinking, Systems Practice*, Chichester: John Wiley & Sons, Inc.
- Conant, R.C. & Ashby, W.R., 1970. Every Good Regulator of a System Must Be a Model of

- That System. *International Journal of Systems Science*, 1(89), pp.511–419.
- Cowlagi, R. V. & Saleh, J.H., 2013. Coordinability and Consistency in Accident Causation and Prevention: Formal System Theoretic Concepts for Safety in Multilevel Systems. , 33(3), pp.420–433.
- DARPA, 2016. Gremlins Takes Flight to Provide Air-Recoverable Unmanned Air Systems. *DARPA News And Events*. Available at: <http://www.darpa.mil/news-events/2016-03-31> [Accessed September 5, 2016].
- Defense Science Board, 2005. *Report of the Defense Science Board Task Force on Patriot System Performance*, Washington, DC.
- Dekker, S., 2003. Failure to adapt or adaptations that fail: contrasting models on procedures and safety. *Applied Ergonomics*, 34(3), pp.233–238.
- Dekker, S., 2006. *The Field Guide to Understanding Human Error*, Aldershot, England: Ashgate Publishing Company.
- Eckberg, C.R., 1963. *WS-133B Fault Tree Analysis Program Plan*, Seattle, WA.
- FAA, 2016. NextGen Data Communications. Available at: https://www.faa.gov/nextgen/update/progress_and_plans/data_comm/ [Accessed May 19, 2016].
- Fannin, W.R. & Rodrigues, A.F., 1986. National or Global?--Control vs Flexibility. *Long Range Planning*, 19(5), pp.84–88.
- Faraj, S. & Xiao, Y., 2006. Coordination in Fast-Response Organizations. *Management Science*, 52(8), pp.1155–1169. Available at: <http://www.scopus.com/inward/record.url?eid=2-s2.0-33748304172&partnerID=tZOtx3y1>.
- Federal Aviation Administration, 2014a. *Air Traffic Organization Policy: Air Traffic Control Order JO 7110.65V*,
- Federal Aviation Administration, 2013a. *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*,
- Federal Aviation Administration, 2012. *Integration of Unmanned Aircraft Systems into the National Airspace System Concept of Operations V2.0*,
- Federal Aviation Administration, 2011. *Introduction to TCAS II Version 7.1*, Washington, DC. Available at: [http://www.faa.gov/documentLibrary/media/Advisory_Circular/TCAS II V7.1 Intro booklet.pdf](http://www.faa.gov/documentLibrary/media/Advisory_Circular/TCAS%20II%20V7.1%20Intro%20booklet.pdf).
- Federal Aviation Administration, 2014b. *Notice JO 7210.873. Unmanned Aircraft Operations in the National Airspace System (NAS)*,
- Federal Aviation Administration, 2014c. *Safety Management System Manual Version 4.0* , p.127.
- Federal Aviation Administration, 2013b. *Sense and Avoid (SAA) for Unmanned Aircraft Systems (UAS). Second Caucus Workshop Report*,
- Federal Aviation Administration, 2014d. Title 14 Code of Federal Regulations Part 91. *Federal Aviation Regulations*. Available at: <http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=3efaad1b0a259d4e48f1150a34d1aa77&rqn=div5&view=text&node=14:2.0.1.3.10&idno=14> [Accessed August 24, 2014].
- Fischhoff, B., 1975. *Hindsight ≠ Foresight: The Effect of Outcome Knowledge on Judgment Under Uncertainty (Report AD-A008 580)*, Eugene, OR. Available at: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA008580>.
- Flach, J.M. et al., 1998. An Ecological Approach to Interface Design. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 42(3), pp.295–299. Available at:

- <http://pro.sagepub.com/content/42/3/295.short>.
- Flach, J.M., 2012. Complexity: Learning to Muddle Through. *Cognition, Technology and Work*, 14(3), pp.187–197.
- Flach, J.M. et al., 2013. Coordination and Control in Emergency Response. In A. Badiru & L. Racz, eds. *Handbook of Emergency Response: Human Factors and Systems Engineering Approach*. CRC Press, pp. 533–548.
- Flach, J.M., 2015. Supporting Productive Thinking: The Semiotic Context for Cognitive Systems Engineering (CSE). *Applied Ergonomics*, In Press. Available at: <http://www.sciencedirect.com/science/article/pii/S0003687015300739>.
- Flach, J.M., 2016. Supporting Self-Designing Organizations. *She Ji: The Journal of Design, Economics, and Innovation*, In Press, p.9.
- Flach, J.M. & Voorhorst, F.A., 2016. *What Matters? Putting Common Sense to Work*, Dayton, OH: Wright State University Libraries.
- Fleming, C.H., 2015. *Safety-Driven Early Concept Analysis and Development*. Massachusetts Institute of Technology.
- Fleming, C.H. et al., 2013. Safety Assurance in NextGen and Complex Transportation Systems. *Safety Science*, 55, pp.173–187. Available at: <http://www.sciencedirect.com/science/article/pii/S0925753512002871> [Accessed September 16, 2014].
- Fleming, C.H. & Leveson, N., 2015. Integrating Systems Safety into Systems Engineering during Concept Development. In *25th Annual INCOSE International Symposium (IS2015)*. Seattle, WA: INCOSE.
- Gallo, W. & Tillotson, D., 2012. Traffic Alert and Collision Avoidance System (TCAS); FAA Flight Standards Pilot Outreach Program. , p.47. Available at: <https://www.nbaa.org/ops/cns/tcas/20120625-faa-tcas-awareness.pdf>.
- Gray III, W.R., 2016. *Time Safety Margin: Theory and Practice (412TW-TIH-16-01)*, Edwards AFB, CA. Available at: http://flighttestsafety.org/images/TSM_Theory_and_Practice.pdf.
- Grote, G. et al., 2009. Coordination in High-Risk Organizations: The Need for Flexible Routines. *Cognition, Technology and Work*, 11, pp.17–27.
- Grote, G., 2004. Uncertainty management at the core of system design. *Annual Reviews in Control*, 28, pp.267–274.
- Gulati, R., Wohlgezogen, F. & Zhelyazkov, P., 2012. The Two Facets of Collaboration: Cooperation and Coordination in Strategic Alliances. *The Academy of Management Annals*, 6(1), pp.531–583. Available at: <http://www.tandfonline.com/doi/abs/10.1080/19416520.2012.691646>.
- Harkleroad, E. et al., 2013. *Risk-based Modeling to Support NextGen Concept Assessment and Validation*, Lexington, MA.
- Heinrich, H.W., 1931. *Industrial Accident Prevention: A Scientific Approach* 1st ed., New York, NY: McGraw-Hill Book Company, Inc.
- Helmreich, R.L., 1997. Managing Human Error in Aviation. *Scientific American*, 276(5), pp.62–67.
- Hollnagel, E. & Woods, D., 1983. Cognitive Systems Engineering: New Wine in New Bottles. *International Journal of Man-machine Studies*, 18, pp.583–600. Available at: <http://www.sciencedirect.com/science/article/pii/S0020737383800340> [Accessed December 31, 2014].
- Hollnagel, E. & Woods, D., 2005. *Joint Cognitive Systems: Foundations of Cognitive Systems*

- Engineering*, Boca Raton, FL: CRC Press.
- Hollnagel, E., Woods, D.D. & Leveson, N.G. eds., 2006. *Resilience Engineering: Concepts and Precepts*, London, UK: Ashgate Publishing Company.
- Jarzabkowski, P.A., Lê, J.K. & Feldman, M.S., 2012. Toward a Theory of Coordinating: Creating Coordinating Mechanisms in Practice. *Organization Science*, 23(4), pp.907–927.
- Kamienski, J. et al., 2010. Study of Unmanned Aircraft Systems Procedures: Impact on Air Traffic Control. *Digital Avionics Systems Conference (DASC), 2010 IEEE/AIAA 29th*, pp.1–10.
- Keller, W. & Modarres, M., 2005. A Historical Overview of Probabilistic Risk Assessment Development and Its Use in the Nuclear Power Industry: A Tribute to the Late Professor Norman Carl Rasmussen. *Reliability Engineering and System Safety*, 89(3), pp.271–285.
- Kerzner, H.R., 2009. *Project Management: A Systems Approach to Planning, Scheduling, and Controlling* 10th ed., Hoboken, NJ: John Wiley & Sons, Inc.
- Kleinbaum, A.M., Stuart, T.E. & Tushman, M.L., 2009. *Communication (and Coordination?) in a Modern, Complex Organization*, Cambridge, MA.
- Kochenderfer, M.J. et al., 2008. A Comprehensive Aircraft Encounter Model of the National Airspace System. *Lincoln Laboratory Journal*, 17(2), pp.41–53. Available at: https://www.ll.mit.edu/publications/journal/pdf/vol17_no2/17_2_2Kochenderfer.pdf.
- Kochenderfer, M.J. et al., 2010. Airspace Encounter Models for Estimating Collision Risk. *Journal of Guidance, Control, and Dynamics*, 33(2), pp.487–499. Available at: <http://arc.aiaa.org/doi/abs/10.2514/1.44867> [Accessed December 17, 2014].
- Kochenderfer, M.J. et al., 2010. *Model-Based Optimization of Airborne Collision Avoidance Logic*, Springfield, VA.
- Kuchar, J. & Drumm, A., 2007. The Traffic Alert and Collision Avoidance System. *Lincoln Laboratory Journal*, 16(2), pp.277–296. Available at: https://www.ll.mit.edu/publications/journal/pdf/vol16_no2/16_2_04Kuchar.pdf [Accessed October 20, 2014].
- Lee, J.D. & See, K. a, 2004. Trust in Automation: Designing for Appropriate Reliance. *Human factors*, 46(1), pp.50–80.
- Lenné, M.G. et al., 2012. A systems approach to accident causation in mining: An application of the HFACS method. *Accident Analysis and Prevention*, 48, pp.111–117. Available at: <http://dx.doi.org/10.1016/j.aap.2011.05.026>.
- Leplat, J., 1998. About Implementation of Safety Rules. *Safety Science*, 29, pp.189–204.
- Leplat, J., 1987. Occupational accident research and sysetms approach. In J. Rasmussen, K. Duncan, & J. Leplat, eds. *New Technology and Human Error*. New York: John Wiley & Sons, pp. 181–191.
- Leveson, N. et al., 2012. Applying System Engineering to Pharmaceutical Safety. *Journal of Healthcare Engineering*, 3(September), pp.391–414. Available at: <http://multi-science.metapress.com/index/178681U841P2XMT2.pdf> [Accessed September 16, 2014].
- Leveson, N.G., 2004. A New Accident Model for Engineering Safer Systems. *Safety Science*, 42(4), pp.237–270. Available at: <http://www.sciencedirect.com/science/article/pii/S092575350300047X> [Accessed December 17, 2014].
- Leveson, N.G., 2015. A systems approach to risk management through leading safety indicators. *Reliability Engineering and System Safety*, 136, pp.17–34. Available at: <http://dx.doi.org/10.1016/j.ress.2014.10.008>.

- Leveson, N.G., 2013. *An STPA Primer*, Available at: sunnyday.mit.edu/STPA-Primer-v0.pdf [Accessed July 21, 2016].
- Leveson, N.G., 2012. *Engineering a Safer World: Systems Thinking Applied to Safety*, Cambridge, MA: The MIT Press. Available at: <http://mitpress.mit.edu/books/engineering-safer-world> [Accessed January 12, 2015].
- Leveson, N.G., 2000. Intent Specifications: An Approach to Building Human-Centered Specifications. *IEEE Transactions on Software Engineering*, 26(1), pp.15–35.
- Leveson, N.G., 1995. *Safeware: System Safety and Computers*, Reading, MA: Addison-Wesley Publishing Company.
- Malone, T.W. & Crowston, K., 1994. The Interdisciplinary Study of Coordination. *ACM Computing Surveys*, 26(1), pp.87–119. Available at: <http://portal.acm.org/citation.cfm?id=174668&dl=GUIDE&coll=GUIDE&CFID=39091014&CFTOKEN=55426743>.
- Malone, T.W. & Crowston, K., 1990. What is Coordination Theory and How Can It Help Design Cooperative Work Systems? In *Proceedings of the 1990 ACM Conference on Computer-Supported Cooperative Work*. Los Angeles, CA: ACM, pp. 357–370.
- March, J.G. & Simon, H.A., 1958. *Organizations*, New York: John Wiley & Sons, Inc. Available at: <http://doi.apa.org/psycinfo/1958-15040-000>.
- McCarthy, S., 2013. *A System Theoretic Safety Analysis of Friendly Fire Prevention in Ground Based Missile Systems*. Massachusetts Institute of Technology.
- McEvily, B., Perrone, V. & Zaheer, A., 2003. Trust as an Organizing Principle. *Organization Science*, 14(1), pp.91–103.
- Mesarović, M.D., 1970. Multilevel Systems and Concepts in Process Control. *Proceedings of the IEEE*, 58(1), pp.111–125. Available at: <http://ieeexplore.ieee.org/ielx5/5/31128/01449475.pdf?tp=&arnumber=1449475&isnumber=31128>.
- Mesarović, M.D., Macko, D. & Takahara, Y., 1970. *Theory of Hierarchical, Multilevel, Systems*, Academic Press. Available at: http://www.worldcat.org/title/theory-of-hierarchical-multilevel-systems/oclc/78075&referer=brief_results.
- Mindell, D.A., 2000. *Cybernetics: Knowledge domains in Engineering systems*, Massachusetts Institute of Technology.
- Montes, D.R., 2016. *Using STPA to Inform Developmental Product Testing*. Massachusetts Institute of Technology.
- Moseley, T.M., 2003. *Operation IRAQI FREEDOM -- By The Numbers*, Prince Sultan Air Base, Saudi Arabia. Available at: <http://www.afhso.af.mil/shared/media/document/AFD-130613-025.pdf> [Accessed July 14, 2016].
- National Oceanic and Atmospheric Administration, 2016. Space Weather Impacts. *Space Weather Prediction Center (webpage)*. Available at: www.swpc.noaa.gov/impacts [Accessed July 8, 2016].
- de Neufville, R. & Scholtes, S., 2011. *Flexibility in Engineering Design* J. Moses et al., eds., Cambridge, MA: The MIT Press.
- Okhuysen, G.A. & Bechky, B.A., 2009. Coordination in Organizations: An Integrative Perspective. *The Academy of Management Annals*, 3(1), pp.463–502.
- Placke, M.S., 2014. *Application of STPA to the Integration of Multiple Control Systems: A Case Study and New Approach*. Massachusetts Institute of Technology.
- Pyle, J.D., 2004. F-16 Launch (Photograph). www.eucom.mil. Available at:

- <http://www.eucom.mil/media-library/photo/19149/staff-sergeant-robert-sandoval-a-crew-chief-with-the-182nd-fighter-squadron-texas-air-national-guard-lackland-air-force-base-san-antonio-texas-prepares-to-launch-an-f-16-34fighting-falcon34> [Accessed July 13, 2016].
- Rasmussen, J., 1982. Human Errors: A Taxonomy for Describing Human Malfunctions in Industrial Installations. *Journal of Occupational Accidents*, 4, pp.311–333. Available at: <http://www.sciencedirect.com/science/article/pii/0376634982900414> [Accessed January 12, 2015].
- Rasmussen, J., 1997a. Merging Paradigms: Decision making, Management, and Cognitive Control. In R. Flin et al., eds. *Decision Making Under Stress*. Aldershot, England: Ashgate Publishing Ltd, pp. 67–81.
- Rasmussen, J., 1997b. Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*, 27(2–3), pp.183–213. Available at: <http://www.sciencedirect.com/science/article/pii/S0925753597000520> [Accessed January 6, 2015].
- Rasmussen, J., 1983. Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and other Distinctions in Human Performance Models. *IEEE Transactions On Systems, Man, And Cybernetics*, SMC-13(3), pp.257–266. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6313160 [Accessed February 19, 2014].
- Reason, J., 1990. *Human Error*, Cambridge, England: Cambridge University Press.
- Reason, J., 2000. Human Error: Models and Management. *British Medical Journal*, 320(March), pp.768–770.
- Risser, D.T. et al., 1999. The Potential for Improved Teamwork to Reduce Medical Errors in the Emergency Department. *Annals of Emergency Medicine*, 34(3), pp.373–383.
- Rothrock, L. et al., 2006. Applying the Proximity Compatibility and the Control-Display Compatibility Principles to Engineering Design Interfaces. *Human Factors and Ergonomics in Manufacturing*, 16(1), pp.61–81. Available at: <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Human+Motion+Simulation+for+Vehicle+and+Workplace+Design#1>.
- RTCA SC-189, 2000. *RTCA DO-264. GUIDELINES FOR APPROVAL OF THE PROVISION AND USE OF AIR TRAFFIC SERVICES SUPPORTED BY DATA COMMUNICATIONS*, Washington, DC.
- RTCA SC-203, 2013a. *DO-344 Operational and Functional Requirements and Safety Objective (OFRSO) for Unmanned Aircraft Systems (UAS) Standards. Volume 1*, Washington, DC.
- RTCA SC-203, 2013b. *DO-344 Operational and Functional Requirements and Safety Objective (OFRSO) for Unmanned Aircraft Systems (UAS) Standards. Volume 2*, Washington, DC.
- RTCA SC-203, 2010. *Special Committee (SC) 203 Minimum Performance Standards for Unmanned Aircraft Systems Revision 2*, Washington, DC.
- RTCA SC-228, (DRAFT) *Minimum Operational Performance Standards (MOPS) for Unmanned Aircraft Systems (UAS) Detect and Avoid (DAA) Systems*, Washington, DC.
- RTCA SC-228, 2014. *Detect and Avoid (DAA) White Paper*, Washington, DC.
- SAE Aerospace, 2010. *SAE ARP4754 Guidelines for Development of Civil Aircraft and Systems*, Sage, A.P. & Cuppan, C.D., 2001. On the Systems Engineering and Management of Systems of Systems and Federations of Systems. *Inf. Knowl. Syst. Manag.*, 2(4), pp.325–345. Available at:

- http://dl.acm.org/citation.cfm?id=1234195.1234200%5Cnhttp://datafedwiki.wustl.edu/images/7/7a/Sage-On_the_Systems_Engineering_and_Management_of_Systems_of_Systems.pdf.
- Scarborough, A., Bailey, L. & Pounds, J., 2005. *Examining ATC Operational Errors Using the Human Factors Analysis and Classification System*, Washington, DC.
- Shappell, S.A. & Weigmann, D.A., 2000. *The Human Factors Analysis and Classification System--HFACS (Report DOT/FAA/AM-00/7)*, Washington, DC. Available at: https://www.nifc.gov/fireInfo/fireInfo_documents/humanfactors_classAnly.pdf.
- Shattuck, L.G., 2000. Communicating Intent and Imparting Presence. *Military Review*, (March-April), pp.66–72. Available at: <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA522123>.
- Sheridan, T.B., 2002. *Humans and Automation: System Design and Research Issues*, New York: John Wiley & Sons, Inc.
- Sheridan, T.B., 2008. Risk, Human Error, and System Resilience: Fundamental Ideas. *Human Factors*, 50(3), pp.418–426.
- Stout, R.J. et al., 1999. Planning, Shared Mental Models, and Coordinated Performance: An Empirical Link Is Established. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 41(1), pp.61–71.
- Stringfellow, M., 2010. *Accident Analysis and Hazard Analysis for Human and Organizational Factors*. Massachusetts Institute of Technology.
- Stringfellow, M. V, Leveson, N.G. & Owens, B.D., 2010. Safety-Driven Design for Software-Intensive Aerospace and Automotive Systems. *Proceedings of the IEEE*, 98(4), pp.515–525.
- Suchman, L., 1987. *Plans and Situated Actions*, New York: Cambridge University Press. Available at: http://books.google.com/books?id=AJ_eBJtHxmsC.
- Thomas, J., 2013. *Extending and Automating A Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis*. Massachusetts Institute of Technology.
- Thompson, J.D., 1967. *Organizations in Action: Social Science Bases of Administration*, New York: McGraw-Hill Book Company, Inc.
- Thornberry, C.L., 2014. *Extending the Human-Controller Methodology in Systems-Theoretic Process Analysis (STPA)*. Massachusetts Institute of Technology.
- United Kingdom Ministry of Defence, 2004. *Aircraft Accident to Royal Air Force Tornado GR MK4A ZG710*, London, UK.
- US Air Force, 2015. ANNEX 3-01 COUNTERAIR OPERATIONS. *LeMay Center for Doctrine*, p.42. Available at: <https://doctrine.af.mil/download.jsp?filename=3-01-ANNEX-COUNTERAIR.pdf> [Accessed July 15, 2016].
- US Army Aviation and Missile Life Cycle Management Command, PATRIOT. Available at: https://history.redstone.army.mil/miss/patriot/patriot_1989_01.jpg [Accessed September 5, 2016].
- US Central Command, 2015. *Investigation Report of the Airstrike on the Médecins Sans Frontières / Doctors Without Borders Trauma center in Kunduz, Afghanistan on 3 October 2015*, MacDill Air Force Base, FL. Available at: [https://www6.centcom.mil/foia_rr/FOIA_RR.asp?Path=/5 USC 552\(a\)\(2\)\(D\)Records&Folder=1](https://www6.centcom.mil/foia_rr/FOIA_RR.asp?Path=/5 USC 552(a)(2)(D)Records&Folder=1). Airstrike on the MSF Trauma Center in Kunduz Afghanistan - 3 Oct 2015 [Accessed July 28, 2016].
- US Central Command, 2004. *PATRIOT Shootdown of US Navy FA-18*, Macdill Air Force Base,

- FL. Available at: [https://www6.centcom.mil/foia_rr/FOIA_RR.asp?Path=/5 USC 552\(a\)\(2\)\(D\)Records/Friendly Fires&Folder=Patriot Shootdown of US Navy F18](https://www6.centcom.mil/foia_rr/FOIA_RR.asp?Path=/5 USC 552(a)(2)(D)Records/Friendly Fires&Folder=Patriot Shootdown of US Navy F18) [Accessed July 28, 2016].
- US Central Command, 2016. *Summary of the Airstrike on the MSF Trauma Center in Kunduz, Afghanistan on October 3, 2015; Investigation and Follow-on Actions*, MacDill Air Force Base, FL. Available at: [https://www6.centcom.mil/FOIA_RR_Files/5 USC 552\(a\)\(2\)\(D\)Records/1. Airstrike on the MSF Trauma Center in Kunduz Afghanistan - 3 Oct 2015/00. CENTCOM Summary Memo.pdf](https://www6.centcom.mil/FOIA_RR_Files/5 USC 552(a)(2)(D)Records/1. Airstrike on the MSF Trauma Center in Kunduz Afghanistan - 3 Oct 2015/00. CENTCOM Summary Memo.pdf) [Accessed July 28, 2016].
- US Department of Defense, 2005. Department of Defense Human Factors Analysis and Classification System: A mishap investigation and data analysis tool. , p.35.
- US Department of Defense, 2015. Department of Defense Human Factors Analysis and Classification System: A mishap investigation and data analysis tool. , p.29. Available at: http://www.public.navy.mil/navsafecen/Documents/aviation/aeromedical/DOD_HF_Anlys_Clas_Sys.pdf [Accessed July 26, 2016].
- US Department of Defense, 2012. *MIL-STD-882E System Safety*,
- US Department of Defense, 2013. Unmanned Systems Integrated Roadmap FY2013-2038. , p.168. Available at: www.defense.gov/Portals/1/Documents/pubs/DOD-USRM-2013.pdf.
- US Department of Defense Joint Staff, 2011. *Joint Publication 3-0. Joint Operations*, Arlington, VA.
- US Department of Defense Joint Staff, 2012. *Joint Publication 3-01: Countering Air and Missile Threats*, Arlington, VA.
- US Department of Defense Joint Staff, 2014a. *Joint Publication 3-30. Command and Control of Joint Air Operations*, Arlington, VA.
- US Department of Defense Joint Staff, 2014b. *Joint Publication 3-31. Command and Control for Joint Land Operations*, Arlington, VA.
- US Department of the Army, 2016. *ATP 3-01.7 Air Defense Artillery Brigade Techniques*, Washington DC.
- US Department of the Army, 2002. *Field Manual Number 3-01.85 (FM 44-85) Patriot Battalion and Battery Operations*, Washington, DC.
- US Department of Transportation, 2014. *FAA Faces Significant Barriers to Safely Integrate Unmanned Aircraft Systems into the National Airspace System*, Washington, DC.
- US Government Accountability Office, 2013. GAO-13-346T. Unmanned Aircraft Systems: Continued Coordination, Operational Data, and Performance Standards Needed to Guide Research and Development. Statement of Gerald L. Dillingham.
- US Nuclear Regulatory Commission, 1975. *WASH-1400 Reactor Safety Study*, Washington, DC. Available at: <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:WASH-1400#8> [Accessed November 30, 2014].
- Vicente, K. & Rasmussen, J., 1992. Ecological Interface Design: Theoretical Foundations. *IEEE Transactions on systems, man, and cybernetics*, 22(4), pp.589–606.
- Vincoli, J.W., 2006. *Basic Guide to System Safety* Second., Hoboken, NJ: John Wiley & Sons, Inc.
- Watson, E.F. & Holmes, K., 2009. Business Process Automation. In S. Y. Nof, ed. *Springer Handbook of Automation*. Dordrecht: Springer-Verlag Berlin Heidelberg, pp. 1597–1612.
- de Weck, O.L., Roos, D. & Magee, C.L., 2011. *Engineering Systems: Meeting Human Needs in a Complex Technological World*, Cambridge, MA: MIT Press.
- De Weck, O.L., Ross, A.M. & Rhodes, D.H., 2012. Investigating Relationships and Semantic

- Sets Amongst System Lifecycle Properties (Ilities). In *Third International Engineering Systems Symposium CESUN 2012*. Delft University of Technology.
- Weichbrodt, J., 2015. Safety rules as instruments for organizational control, coordination and knowledge: Implications for rules management. *Safety Science*, 80, pp.221–232. Available at: <http://dx.doi.org/10.1016/j.ssci.2015.07.031>.
- Weick, K.E., 1976. Educational Organizations as loosely Coupled Systems. *Administrative Science Quarterly*, 21(1), pp.1–19.
- Weigmann, D.A. & Shappell, S.A., 1997. Human Factors Analysis of Postaccident Data: Applying Theoretical Taxonomies of Human Error. *The International Journal of Aviation Psychology*, 7(1), pp.67–81.
- Wiener, N., 1956. *The Human Use of Human Beings: Cybernetics and Society* 2nd ed., Garden City: Doubleday & Company, Inc.
- Woods, R.H.J., 1990. *The Role of the Corps Air Defense Artillery Brigade*. US Army Command and General Staff College. Available at: <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=AD B041508>.
- Young, W. & Leveson, N.G., 2014. An Integrated Approach to Safety and Security Based on Systems Theory. *Communications of the ACM*, 57(2), pp.31–35. Available at: <http://dl.acm.org/citation.cfm?doid=2556647.2556938> [Accessed May 3, 2014].

[Page intentionally left blank]

APPENDIX A. Flawed Coordination Guidance and Examples

This appendix is the supplement to Table 16. Flawed Coordination Guidance for Unsafe Control Action Causal Analysis. The following discussion and examples step through each flawed coordination case and elements using the guide words and phrases listed in the table to provide greater context for identifying coordination scenarios that can lead to UCAs.

A1. Flawed Coordination Case 1. Coordination Missing Leads to UCAs

If there are interdependent conditions between two or more decision systems, coordination behavior should exist. However, when a coordination strategy is missing, decision systems are acting independently, which can lead to UCAs.

The primary coordination element applicable to this case is coordination strategy (element 2), which is missing. There are also no other explicit coordination safety goals (element 1) and group DM efforts (element 4) between decision systems that would indicate coordination is in progress. If group DM towards a coordination goal exists without a coordination strategy, this is flawed coordination case 4 (coordination strategy established late).

An example of where coordination is missing and needed is during emergency management scenarios. In such a case, the emergency creates interdependency for a group to emerge and address it. During early emergency response, however, coordination may be missing vertically and laterally between decision systems that leads to UCAs.

A2. Flawed Coordination Case 2. Coordination Inadequate Leads to UCAs

Flawed coordination case 2 describes the condition where a coordination strategy exists. However, one or more of the coordination elements may be missing or inadequate. It only takes one coordination element to be missing or inadequate to negatively influence an outcome and lead to a UCA. Flawed coordination case 2 is perhaps the most demanding of the flawed coordination cases in analysis because the concept of *inadequate* coordination is perhaps the broadest of the flawed coordination cases.

Coordination Components

- (1) Coordination goals can be inadequate for coordination. (see the coordination framework discussion)
- (2) In flawed coordination case 2, a coordination strategy exists. However, the coordination strategy can be inadequate.

One of the primary reasons for inadequate strategy is being ambiguous or missing aspects of an adequate strategy. Strategy may not provide bounds of acceptable or desired behaviors, or the bounds are ambiguously defined. Strategy may be missing needed actions or steps in a process. The strategy may miss or ambiguously define temporal constraints, such as: start and stop times, duration of behaviors, sequence of behaviors, or if behaviors must be simultaneous.

Strategy can also be inadequate when multiple coordination strategies exist. Decision systems in such environments may not know another strategy exists, let alone is being used by the other decision system. For example, air interdiction missions involving large airstrike packages require significant planning efforts to ensure all aircrew understand the overall coordination strategy. Perhaps the environment changes and the mission commander changes the strategy for a portion of the package before the mission, but does not ensure the rest of the package is aware believing there is no risk to the accomplishing the mission. Unaware of the updated coordination strategy, the package aircraft may act in accordance with the original coordination strategy that is now hazardous based on the amended strategy.

Multiple coordination strategies may also be incompatible and lead to hazardous scenarios. For example, in aviation the collision avoidance rules dictate aircraft to alter course to the right when engaged in a head-on collision scenario. Collision avoidance software for future horizontal maneuvering may suggest or allow left maneuvers for head-on collision scenarios. The incompatible strategies can lead to hazardous head-on collision scenarios when one aircraft maneuvers left following automation and the other approaching aircraft maneuvers right following vertical coordination standards.

(3) Decision systems can be missing or inadequate for coordination.

During coordination efforts, it is essential to have the right experts for any given problem. The required experts may be missing and continuing with coordination may lead to peril without expert knowledge. For example, to develop the coordination strategy between Patriot missile systems and coalition aircraft using the defended airspace, experts are needed. Without Patriot system experts or aircraft experts, critical knowledge of system operations and assumptions may be missing.

Decision systems must also have ability to handle expected coordination efforts, to include emergency or off nominal scenarios. Cognitive ability and physical skills may be inadequate for humans. If training is inadequate, hazardous scenarios can result. It is possible that no matter the training, the human decision system cannot meet a minimum threshold. Training may not solve unsafe system design and interactions, but is a perspective to address for coordination.

Automation is a decision system also. Automation must meet the information processing demands for coordination, including time requirements. Automation hardware specifications can be inadequate to meet coordination scenario demands, which may lead to hazardous coordination scenarios.

Coordination Processes

(4) Communications may be missing or inadequate.

The communication channels may be inadequate and lead to hazardous scenarios. The communication channels should be known and be compatible. In humans, communication can occur from visual, auditory, and tactile channels. Concerns for decision systems may include using compatible channels (i.e. verbal communication for auditory channels) and that the channel being used is known. For example, pilots know to use visual communications when verbal communications are inoperative. Pilots should look for a green light from the control tower as a signal for clearance to land in a visual-only communication environment.

Another perspective on communication channels are the use of analog or digital channels. Decision automation uses digital communications and humans are often reliant upon analog or digital channels for long distance communications. There are many concerns for use of digital and analog communication channels beyond the scope of this research. However, higher level concerns include inadequate channel capacity, bandwidth, and ability to handle internal and environmental noise. The higher level concerns may result in communication delays, dropped communications, and static affecting the intelligibility of communications.

The communication language is important, both in human and digital communications. The communication languages may be incompatible such as written symbols not known or understood. The ability to use a language may be inadequate and degrade coordination efforts even with the same language. For example, flying in non-English speaking countries there can be a local dialect that is difficult for visiting aircrew members to understand and consequently coordination can be a challenge. Digital communication languages must be compatible as well.

In addition to the language, the send and receive protocols may be inadequate and hazardous scenarios can develop. In human communications, the timing and sequencing of communications should be addressed. Spatial aspects are important as well for protocols. For example, visual communications may require protocols to address obstructions or human limitations. In flying, ground signals to aircrew may require large and high contrast symbols to be seen. In digital communications, there are many protocol concerns with message format, timing, buffering, layering and so forth.

(5) Group decision-making (DM) may be missing or inadequate.

In flawed coordination case 2, group DM may be missing if there is coordination strategy (when both are missing this is case 1). For example, rules can exist that provide a coordination strategy for two peer decision systems. However, if group DM is missing the decision system cannot engage in lateral coordination to address situations which can lead to hazardous scenarios.

Group DM needs a physical or virtual environment. The environment may be uninhabitable for humans, such as too loud, too cold or hot, too dangerous, etc. Virtual environments for group DM may have concerns such as bias of those physically present or not (e.g. a vote may not count as much if not physically there) and potentially missing out on non-verbal information (e.g. facial expressions).

Group DM protocols are needed. Some example protocol concerns include: how to determine alternatives; who can determine alternatives; how group decisions are made; who makes decisions. Group DM protocols may enable consensus voting and the majority wins, or that group DM continues until some threshold of participants agrees. Another example is that group DM protocols may assign final decision

responsibility to one or a subset of the group. Inadequate protocols can lead to ambiguity in group decision outcomes. Inadequate protocols can also delay coordination strategy development, addressed in flawed coordination case 4 (coordination strategy late).

Value functions are needed for group decisions. Inadequate value functions may lead to hazardous scenario if they inadequately address safety. For example, value functions may allow decisions to proceed too close to an unsafe envelope to improve another objective function such as maximize profit. It may be decided to continue operations at a manufacturing plant with a critical maintenance check overdue because of a strike by union maintenance workers. Perhaps the management group believed their past safety records justified skipping the maintenance interval.

Group DM also needs a framework or paradigm to solve any given problem. Inadequate frameworks can lead to hazardous strategies when critical perspectives, assumptions, or interactions are missed or are incorrect.

(6) Observation of common objects may be missing or inadequate.

Observation or knowledge of common objects enables development and execution of a coordination strategy. Inadequate observation of common objects can lead to hazardous scenarios. One concern is when observation of different objects occurs. This may occur from use of different sensors. For example, an electro-optics sensor may see objects at night when the human eye cannot. Coordination efforts between aircrew of such a night scenario can lead to misidentification of a hostile target.

Different object may be observed when decision system observations are asynchronous. Observations may be asynchronous by design or by scenario. Under asynchronous observations, decision systems may believe they are observing the same object, but are not. Another concern is that the decision systems do not observe common objects because there is not a perceived need to observe by one or more interdependent decision systems.

The physical specifications such as sensor resolution, data processing times, and delays in information transmissions can affect observation of common objects. Observation protocols individually or in coordination may be inadequate also, such as the observation update rates. One decision system may observe at 1 hertz (1 second cycle) and another decision system observes at 0.1 hertz (10 second cycle) and the 0.1 hertz observation may be outside the cycle needed to adequately address a scenario.

Coordination Enabling Conditions

(7) Authority, responsibility, accountability (ARA) may be missing or inadequate.

Coordination must ensure decision systems have the right authority and responsibility to engage in necessary coordination behaviors. Responsibility may not be assigned for coordination activities. A mismatch of authority and responsibility may mean aspects of coordination are not accomplished or there are delays in coordination. Authority and responsibility within or between decision systems may be ambiguous, leading to hazards.

Accountability is applicable to the coordination strategy and may be inadequate throughout coordination phases to include receiving the strategy, agreeing on the strategy, compliance with, and completion of the strategy. For example, a strategy may exist but the decision systems did not receive it. This may occur because the transmission signal failed in some manner or because the decision systems were attending a different problem. Without receiving a coordination strategy, no matter how safe it was, a hazardous scenario can develop.

Accountability is concerned with observation and observation rates of the decision systems themselves. Observation can assist coordination by ensuring decision systems are behaving as intended. Inadequate observation can lead to hazards when decision systems are not behaving as intended due to misunderstanding or a scenario is different than anticipated.

Accountability affects trust and confidence in coordination behavior. Lack of confidence in the other decision system may result in questioning the coordination strategy, questioning if decision systems carried out the strategy, or ignoring the decision system altogether. Having inadequate confidence in the other decision systems can lead to hazardous scenarios.

Accountability is related to time constraints. Inadequate accountability can occur from time constraints not established or not monitored. For example, an air-refueling tanker aircraft needs to meet up with receiving aircraft. Without an established contact time, the results could be hazardous. The time constraints may not be monitored even if established. Using a similar example, the tanker aircrew may not realize the time it takes to reach a contact point and begins flying there too late.

Another accountability perspective is the ability for decision systems to be influenced by others. Coordination requires decision systems to be coordinable. Missing coordinability may occur with automation that was not designed to be coordinable. An example of missing coordinability can be found in aviation today with the coordination between ATC and aircraft decision systems. Using the coordination framework, TCAS is a decision component of the aircraft decision system that makes decisions on aircraft maneuvers to avoid collisions. While ATC influences pilot decisions, ATC cannot directly influence TCAS decisions by its design.

Coordinability also applies to humans. Humans may not be coordinable by organizational design. For example, an expert might be needed for an engineering effort or for standards development of a sociotechnical system, but the funding and management organization do not have influence over the expert's time.

Inadequate coordinability may also occur from internal motivations and external incentives on the decision system. From the accountability perspective, however, resisting safe coordination efforts is perhaps more of a security than safety concern. Whereas from a coordination goals perspective, this may lead to pushing or accepting less safe behavior.

(8) Common understanding may be missing or inadequate.

Coordination must have common understanding to be successful. A fundamental concern is the understanding of local and system states for coordination in space and time. Common understanding may

be inadequate due to decision system knowledge of their state in absolute or relative terms (to the environment or other decision systems), which may lead to UCAs.

Inadequate understanding may come from different local and holistic models of the processes, relationships, and interactions for example. Similar to models are information reference frames. For example, coordination may use geo-physical artifacts or time for execution of a coordination strategy. If the wrong geo-physical reference frame is used, hazardous scenarios can result.

Process or automation modes affect common understanding. Process behaviors change and may be limited depending on the mode, such as flight in takeoff and landing gains versus cruise gains. Coordination with inadequate understanding of process or automation modes may lead to UCAs.

Another concern is common understanding of the coordination strategy. In execution of the coordination strategy, inadequate understanding may lead to hazardous scenarios.

(9) Predictability may be missing or inadequate.

Predictability is inherently about models. With missing or inadequate models, both mental models and automation algorithms, coordination may lead to UCAs. Task familiarity influences predictability. When decision systems are new or the environment is new, task familiarity and thus predictability may be inadequate. Time constraints can also affect predictability. For example, if collision scenario is seconds away, the ability for aircraft decision systems to run mental simulations or algorithms to process and display information may be inadequate.

A3. Flawed Coordination Case 3. Coordination Strategy Leads to UCAs

The coordination strategy must lead to safe outcomes. Flawed coordination case 3 seeks to identify how established coordination strategy directly leads to unsafe control and how it could be developed.

(2) Coordination strategy may lead to hazards.

The coordination strategy can lead to hazards in at least two parts of the general coordination problem referenced in Figure 17a: 1) the decision system coordination output $y_{a,b}(t)$ and 2) the system outcome, which is the coordination output paired with the environment. An example of the coordination strategy leading to an unacceptable output $y_{a,b}(t)$ independent the environment is when two aircraft using TCAS collide. An example of the coordination output and environment leading to an unacceptable outcome is when two fighter aircraft perform air-to-ground strike missions (e.g. air interdiction), but their coordination strategy does not account for updated enemy ground order of battle.

The coordination strategy when executed as intended should be feasible and not lead decision systems into unsafe states. Inadequate assignment of decision systems in space and time may occur, even if unintentional. This flawed case perspective may update a coordination strategy before an accident prompts the update.

An earlier version of TCAS (traffic collision avoidance system) that is still in operations today provides an example of strategy that leads to hazards. MIT Lincoln Laboratory researchers pointed out that with TCAS Version 7.0 logic the reversal maneuver strategy between aircraft on collision course would not occur unless the aircraft had 100 feet separation (Kuchar & Drumm 2007). A reversal maneuver is one where the initial suggested maneuver is reversed, such as a climb reversed to descend. The TCAS 7.0 logic strategy may be inadequate for at least two reasons: 1) aircraft in a potential collision scenario (i.e. spatially close) were allowed to pass within 100 feet and 2) when aircraft are at the same altitude (within 100 feet) the TCAS does not change an alert. In TCAS 7.0 logic, it was possible to remain within 100 feet of another aircraft perfectly on collision course without any adjustment from TCAS to indicate a problem to the aircrew, which is a hazardous scenario.

This scenario actually occurred in the 2002 Überlingen mid-air collision as “...both aircraft remained within 100 feet vertically of each other throughout the encounter” (Kuchar & Drumm 2007) p. 285. In part a response to the Überlingen mid-air, TCAS logic 7.1 was updated to address the 100 feet separation requirement for a reversal maneuver (Federal Aviation Administration 2011).

The TCAS example was coordination strategy relative to the interdependent decision systems. A coordination strategy must also meet face validity relative to the environment. For example, should collision avoidance systems such as the future UAS detect-and-avoid system recommend a coordination maneuver towards the ground? In the worst case environment, such as being close to the ground and the UAS is a low performance aircraft, a maneuver towards the ground may lead to hazards. Flawed case 3 seeks hazard scenarios from using the coordination strategy itself. In a system engineering effort, case 3 provides a separate and hopefully independent safety perspective on the designed coordination strategy.

A coordination strategy may become unsafe with time. That is, it may not be enough to set a coordination strategy and not evaluate it again as the system and environment are dynamic and uncertain. Rather, the coordination strategy may need continual updating to adapt to changes. For example, wartime operations may have primary and contingency coordination strategies. With changing geopolitical forces, however, even the best plans require updating. The coordination strategy may need to be evaluated in more real-time the closer the strategy dictates physical process actions. For example, when fighter aircraft arrive a training area the coordination strategy may need to change based on the weather. Regular interval evaluations or event triggers may assist in determining if a coordination strategy has been “attacked” and needs updating. A flawed coordination strategy may result from missing or inadequate evaluation and update rates or update triggers.

Development of the coordination strategy is also applicable to flawed coordination case 3. Missing or inadequate information inputs to the decision systems can result in unsafe strategy. Information inputs related to the system, the environment, and other decision systems are needed. Missing or inadequate temporal constraints—e.g. timing duration, sequence, and simultaneity—can lead to unsafe strategy. The models used should be evaluated. Strategy evaluation methods may be missing or inadequate. For example, a coordination strategy can be evaluated on paper by a team of independent experts (e.g. using STPA-Coordination), by model and simulation trials, by hardware and human in the loop experiments, and by real-world testing.

Last, the coordination strategy must be feasible. The strategy cannot rely on decision systems to accomplish actions in conflict with natural laws and that exceed some property constraint such as physical strength. For example, a coordination strategy cannot rely on an aircraft flying below stall speed or above structural limitations.

A4. Flawed Coordination Case 4. Coordination Strategy Late Leads to UCAs

A coordination strategy must be established in time to influence and correct an accident scenario. Flawed coordination case 4 identifies how inadequate coordination elements influence a coordination strategy being established late, which can lead to UCAs.

Coordination Components

- (1) Coordination goals may be late. Such a scenario may occur when organizations are formed in reaction to events and goals are not yet established. Without established goals, coordination strategy lacks overarching guidance.
- (2) Coordination strategy is established late. This is the emphasis of flawed coordination case 4.
- (3) Decision systems established late. Decision systems needed to develop a coordination strategy may not have the ability or knowledge to develop a coordination strategy. For example, decision systems in the decision-making hierarchy may develop higher level coordination strategy for sociotechnical systems. When one person leaves it may take several months before a new hire can acclimate to the new job demands and knowledge base to affect coordination strategy.

Coordination Processes

- (4) Communications may be inadequate.

When remote communication channels are used to develop a coordination strategy, data transfer and communication protocol delays may be inadequate. For example, Solar Radiation Storms produce x-rays and solar energetic protons that can degrade and even block satellite communications (National Oceanic and Atmospheric Administration 2016). Remote UAS pilots depend upon satellite communications for UAS operations and inadequate accounting for space weather disruptions and delays may lead to late coordination efforts.

- (5) Group DM may be inadequate.

The time constraints on hazardous scenarios may not be known or they may be incorrect. For example, in a mid-air collision scenario the pilots should know how much time they have to develop a coordination strategy for collision avoidance. The time constraints for collision avoidance should include factors such

as aircraft performance, time from human action to aircraft response, and time for humans to make individual decisions regarding aircraft maneuvers. If one or both pilots are unaware of the time constraints on the collision scenario, they coordination strategy may be developed too late to influence a collision free encounter.

The group DM protocols may be inadequate and require too much time. The scenario may be that group DM occurs when a hazardous event is known. However, the protocol time demands are inadequate to deal with the required hazardous scenario.

(6) Observation of common objects may be inadequate.

Observing different objects may cause delays in strategy development as the information being used may be different. Observation of common objects can be inadequate when observation is asynchronous, the update frequency too low, or the observation duration takes too much time.

Coordination Enabling Conditions

(7) Authority, responsibility, and accountability may be established late.

Authority and responsibility apply to decision systems at every level of a sociotechnical system and in vertical and lateral coordination relationships. Standards to address authority and responsibility may be inadequate. When the scenario is new or the decision systems involved in an interdependent condition are new, establishing authority and responsibility in real time may be necessary.

Coordination strategy development needs accountability if it is to be on time. Accountability includes time constraints for decision systems to develop a coordination strategy. Accountability also includes monitoring decision systems and timely alerting them when time constraints may not be met. Inadequate accountability can lead to strategy developed too late.

(8) Common understanding may be inadequate. Efforts to achieve common understanding may cause strategy to be developed too late.

(9) Predictability may be inadequate. Dynamic models for a given scenario may be inadequate and cause time constraints on the development of coordination strategy to be incorrect. Prediction models may calculate time incorrectly or perhaps are using inadequate time measures. Using the collision avoidance example, TCAS bases time measures off of what is called the closest point of approach (CPA) to another aircraft, which is range divided by closure rate (Federal Aviation Administration 2011). However, CPA does not tell me when aircraft can no longer influence the outcome, which occurs at a time before reaching CPA. Perhaps a better time measure is time to when actions can no longer influence the outcome.

[Page intentionally left blank]

APPENDIX B. RTCA SC-228 Draft STPA on UAS Integration Report

This appendix provides an edited excerpt of the draft STPA report supporting RTCA SC-228 Safety Working Group efforts, which was accomplished in July 2015. The initial SC-228 Safety Working Group was disbanded late 2015 and this report was not published. The analysis results contained in the report, however, are still applicable to safe UAS integration efforts.

The draft report was accomplished before the ideas in this thesis materialized into a coordination framework and STPA-Coordination. The thesis case study emphasis is on coordination behavior, while this draft report focuses on control loop interactions with emphasis on the detect-and-avoid, which is commensurate with the SC-228 efforts; results of both analyses are recommended for implementation. Results may overlap where coordination and control loop interactions represent the same relationships, such as ATC interactions with aircrew.

Note, figures and tables in this appendix are self-contained and not included in the thesis list of figures and tables.

B. Title Page

SAFETY REPORT FOR RTCA SC-228 DETECT AND AVOID SAFETY SUB-GROUP

UAS Integration. A Systems-Theoretic Safety Analysis for Design of the Detect and Avoid System

JULY 2015

©2015 Massachusetts Institute of Technology. All rights reserved.

Kip Johnson, Lt Col, USAF

MIT Department of Aeronautics and Astronautics

B. Abstract

UAS integration into the NAS must be safe and is a fundamental charter of the FAA. What does it mean to be safe? Safety, according to MIL-STD-882E, is the freedom from conditions that cause accidents (US Department of Defense 2012). Given this unambiguous definition, it follows that safety analysis and design efforts at minimum should find the conditions that cause accidents and eliminate them. Preventing accidents through safety design was the motivation for this report in support of RTCA SC-288 MOPS.

Conditions that cause accidents are many. Traditional safety analysis methods focus on failure conditions and predicting failure and accident rates, treating safety as a reliability problem. In addition to failure conditions, however, accidents can result from inadequate design requirements, software errors, human errors, missing functions (e.g. feedback), and flawed interactions to name a few.

In order to identify accident causation scenarios beyond failure conditions, STPA (Systems-Theoretic Process Analysis) was used. STPA is a new hazard analysis technique based on a systems-theoretic accident model called STAMP (Systems-Theoretic Accident Model and Processes) (Leveson 2004). In STAMP, safety is a control problem, not a reliability problem.

Using a systems engineering framework, STPA was successfully adapted and applied to the UAS integration system and the DAA. From the scenarios, design requirements were developed to eliminate the hazardous scenarios. STPA resulted in a set of qualitative functional design constraints and requirements necessary for safe integrated flight operations. There are three recommendations.

Recommendation 1. Use STPA results herein as certification requirements for DAA functional design. Industry should meet the safety design constraints and requirements to eliminate hazardous scenarios. If not able to eliminate the hazardous scenarios, then mitigate their effects.

Recommendation 2. ATC shall have timely feedback on the tactical decision systems it controls, which includes information on the DAA system maneuver suggestions and the remote pilot's decision.

Recommendation 3. Local airspace control (i.e. ATC) shall receive timely feedback on communications and control channels that affect their ability to control the unmanned aircraft.

Traditional safety efforts are concerned with predicting failure and accident rates. STPA is concerned with finding unsafe behaviors and interactions that lead to accidents. When used in design, STPA can prevent accidents due to software and human errors, requirement flaws, missing functions, and unsafe interactions a priori. The two approaches should prove beneficial for safe UAS integration.

B1. Systems Engineering Baseline

System safety engineering should be and often is integrated within the larger systems engineering effort. This chapter provides the systems engineering baseline needed for DAA and UAS integration safety analysis and design.

B1.1. System Requirements

STPA is part of a system engineering framework, a technical and management framework useful to develop, implement, operate and dispose of systems. At the beginning, a requirements analysis is conducted. The system requirements are grounded in safety, which is preventing accidents. We first identify the system-level hazards that can lead to accidents. The system requirements are then the functional constraints needed to avoid the hazards. From these system level requirements, STPA generates more detailed requirements. The detailed requirements must have traceability back to the accidents. The safety chain needs to link safety constraints/requirements → hazards → accidents for the design requirements to be related to safety.

Following is the systems engineering framework for UAS integration.

- System. National Airspace System (NAS)
- System Purpose. The National Airspace System enables safe and efficient use of the airspace by airborne stakeholders.
- Goal. Safe flight operations, freedom from accidents
 - A1. Mid-air collisions
 - A2. Ground collisions
- Hazards.
 - H1. Violation of aircraft minimum separation boundaries. (←A1)
 - H2. Controlled flight into terrain maneuver. (←A2)
 - H3. Loss of aircraft controlled flight. (←A1, A2)
- System Safety Constraints (SC). These are derived from the hazards and represent the highest constraints on system operations. Further refinement in abstraction and eventually to actual technology and processes shall always follow these constraints.
 - SC1. Flight operations shall not lead to loss of minimum separation requirements. (←H1)
 - SC2. Flight operations shall not induce or contribute to a controlled flight into terrain maneuver. (←H2)
 - SC3. Flight operations shall not induce or contribute to loss of aircraft controlled flight. (←H3)
- Safety Analysis Objectives.

- Objective 1. Identify hazardous functions and interactions to the NAS from UAS integration.
- Objective 2. Engineer design requirements necessary to avoid the identified hazardous behaviors and system interactions.

B1.2. Safety Control Structure

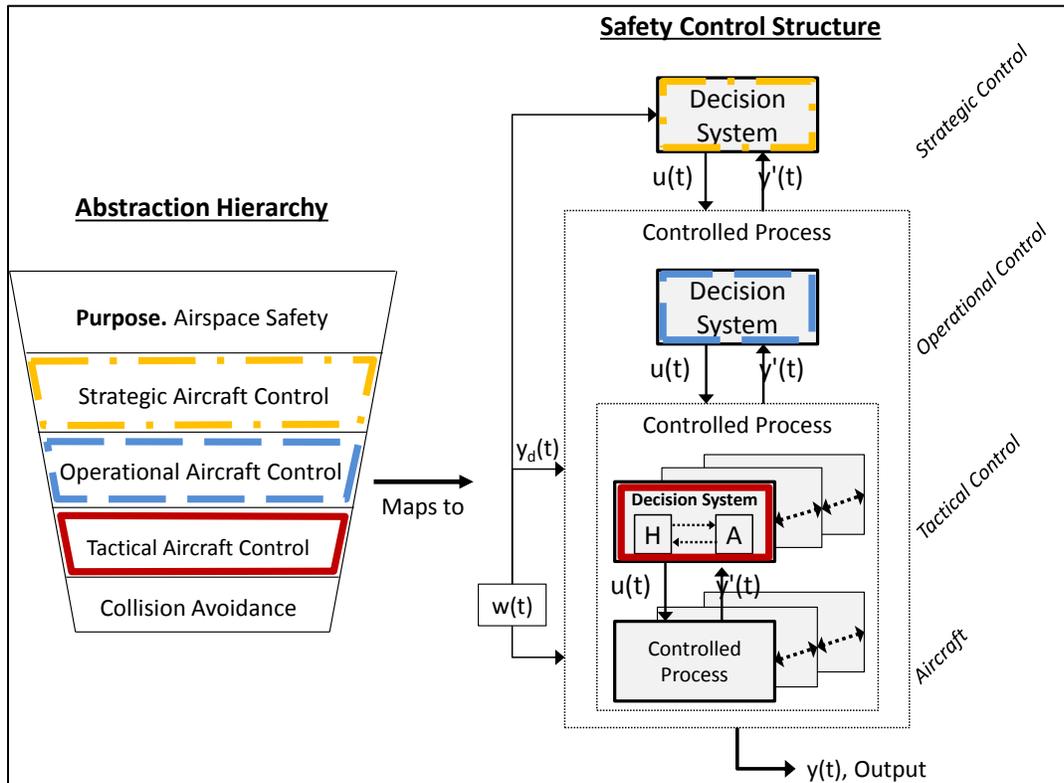


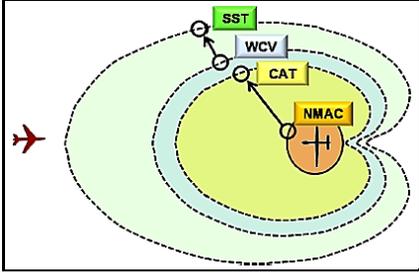
Figure 4. UAS-NAS Integration Safety Control Structure

B1.3. Concept of Operations and Environment

The STPA analysis followed the concept of operations (ConOps) and scenarios of interest within the current literature and RTCA efforts. Table 2 highlights the relevant ConOps and their application to operations.

Table 2. Concept of Operations

Category	Concept and assumptions	Application to Operations
Flight Rules	All UAS shall file and fly an IFR flight plan (Federal Aviation Administration 2012).	In the US, UAS operations will only fly under positive control, and Class G IFR rules (no ATC). The worst case

		safety environment is Class G, and the ConOps does not restrict UAS from Class G.
	Regulations will allow UAS to follow well-clear and collision avoidance guidance while under positive control (RTCA SC-228 2014).	This concept allows the UAS controller to self-separate as determined by the DAA system. A well-clear safety bubble is enforced through this concept should ATC not provide timely assistance.
Flight Operations	ATC does not have a direct link to the UA for flight control purposes (Federal Aviation Administration 2012).	Direct UAV control remains with the UAS operator, and future DAA systems. This concept significantly affects the safety control structure and analysis-need to monitor this assumption.
	Fully autonomous UAS operations are not permitted (this does not apply to lost link autonomy). The PIC has full control, or override authority to assume control at all times during normal UAS operations (Federal Aviation Administration 2012).	Safety analysis will include human-in-the-loop UAS operations.
	<p>UAS flight has the potential for two separation boundaries, one boundary more conservative in time and space than the other, Figure 6.</p>  <p>Figure 6. UAS Separation Boundaries. (Reprinted from (Federal Aviation Administration 2013b), p. 3-20. Figure in public domain)</p> <p>The self-separation threshold (SST) is the more conservative layer. At the SST, the UAS maneuvers to avoid a well-clear violation (WCV) (Federal Aviation Administration 2013b). The well-clear concept was derived in part from the 14 CFR §91.181 maneuver requirement to remain “well-clear” of aircraft while</p>	While there may be two separation boundaries within UAS operations, STPA will use the worst case CAT separation boundary for analysis of H1: Violation of aircraft minimum separation boundaries (←A1).

	under positive ATC control. The collision avoidance threshold (CAT) is where a maneuver should avoid a near mid-air collision (NMAC).	
DAA Technology	The assumption is the DAA will have both cooperative and non-cooperative sensors (RTCA SC-228 2014). The UAS will have self-detection capabilities. The DAA functional solution is not yet determined. It is envisioned to provide information and some form of maneuver suggestions in the vertical and horizontal. ⁵	Safety analysis will address loss of self-detect function as intruders may not have electronic identification means. The DAA maneuver suggestions will be treated as providing a set of safe maneuver alternatives.
Electromagnetic Spectrum	The spectrum necessary to support UAS operations is available (Federal Aviation Administration 2012).	The assumption should be watched carefully as the integrated system unfolds.

The environment includes factors outside the system boundary that system designers cannot or will not influence. The safety analysis shall address how the system will account for the environmental disturbances listed below. The environmental disturbances and assumptions for UAS integration are listed in Table 3.

Table3. Environmental Disturbances

Disturbance Factors	Description	Concerns
Airborne threats	Airborne threats are airborne obstacles outside the span of control and a potential collision conflict. Threats are different for each decision system level.	It may not be feasible or desired to protect against all airborne threats, such as asteroids.
Ground threats	Ground threats are the terrain itself or ground-based obstacles such as towers.	n/a
Weather	Meteorological conditions that may impact visibility or aerodynamic flight.	n/a
Cybersecurity	Malevolent actors purposefully trying to disrupt NAS operations through cyber-attacks. Or, accidental cyber disruptions to remote operations.	Over-the-air link communications and control makes this environmental factor a significant concern, both intentional and accidental cyber interferences.

⁵ From RTCA SC-228 communications and involvement

NAS flight operations can be categorized into many scenarios. The most germane categories are described in Table 4.

Table 4. Flight Scenario Descriptions

Scenario	Description	Assumptions	Concerns
Airspace	US airspace has several categories—Classes A, B, C, D, E and G—that each have different aircraft equipage and pilot training entry requirements. Class G is uncontrolled airspace	UAS operations will not create new airspace designations (Federal Aviation Administration 2012).	See-and-avoid behavior is paramount in these airspaces. Class C, D, and E airspace are mixed control, which has potential for hazardous interactions. Class G operations are heavily reliant on visual separation. Reliability analysis may vary encounter rates based on airspace category in efforts to predict accidents rates. In contrast, STPA analyzes worst case scenario and efforts prevent accidents.
Flight Phase	Flight phases include takeoff, departure, enroute, arrival, and landing.	DAA may be used in all flight phases.	Reliability analysis may vary encounter rates based on flight phase in efforts to predict accident rates. In contrast, STPA analyzes worst case scenario and efforts prevent accidents.
Intruder equipage	Important intruder equipage includes: electronic ID capabilities and collision avoidance technology.	none	Collision avoidance technology may not be compatible or may not be installed on aircraft. The safety analysis will account for non-coordinated avoidance maneuvers. A concern for integrated flight operations is a safety barrier design philosophy that views the equipage as independent components that fail stochastically.

Airspace and phase of flight are common categories in traditional safety analyses as they dictate encounter density and other probabilities. Unfortunately, accidents do not care about airspace or flight phase. The same accident can occur in class A or class B airspace, and during enroute or departure flight phases.

In summary, the safety analysis setup includes:

- System of interest. Flight operations only.
- Scope of analysis. The DAA system and its immediate interactions within the safety control structure.

- Analysis scenario. STPA is a worst case analysis, not based on probabilities. STPA is concerned with unsafe controls and why they occurred. Decomposition by airspaces, flight phase, and intruder equipage are only done if related to control.
- Environmental disturbances. Airborne obstacles, ground obstacles, and meteorological conditions will be factored into the safety analysis. Cyber security vulnerabilities will not be addressed.

B2. STPA Results and Discussion

The levels of control modeled in the safety control structure Figure 4 are analyzed with STPA. Only the Tactical Control decision system level is analyzed in sufficient detail to provide meaningful design guidance. This is an arbitrary decision to be most useful for the present RTCA SC-228 safety and design efforts. The derived safety requirements herein are necessary but *not* sufficient for NAS safety. The system should be analyzed holistically using STPA to find hazardous scenarios and to recommend design solutions.

The higher levels of control are analyzed superficially to show the reader how to start STPA, and to provide context and a safety constraint envelope for STPA on the tactical control decision system.

B2.1. Strategic Control

Strategic control (ST) is predominantly the rules, regulations, and policy for aggregate flight operations. Strategic control is the broadest form of control for the NAS. Strategic control has the same safety constraints as detailed in the previous section B1.1 above. Table 5 shows one example of STPA and resulting design requirements. Further hazard analysis (i.e. step 2) is not accomplished at the strategic control level. It should be noted, however, the design requirements highlight safety concerns in the current NAS.

Table 5. Unsafe Strategic Control Actions

Unsafe Control Actions (UCA)	UCA Descriptions	Safety Design Requirements
UCA-ST1 Not providing control action leads to hazard	Strategic Control fails to regulate separation when required safe	ST1.1 All aircraft shall be separated by lateral, vertical, or timing. ⁶ ST1.2. Strategic control shall coordinate separation for aircraft on collision course by lateral, vertical, or timing. ⁷

⁶ US airspace Class C, D, and E mixes controlled and uncontrolled aircraft, which is a safety concern.

⁷ Potential collision courses are addressed in 14 CFR §91.113 Right of way rules: distress, converging, head-on, overtaking, and landing.

	separation violation possible. (←H1)	ST1.3. Strategic control shall require minimum safe performance and equipment for flight in same airspace. ST1.4. Strategic control shall have deconfliction strategy for when control is lost (e.g. communication and remote control failures). ⁸
--	--------------------------------------	--

B2.2. Operational Control

The control actions at the operational level include aircraft separation maneuvers in geometry and timing, and are guided by the same system safety constraints in section B1.1 above. Air Traffic Control and local agencies making rules and regulations are decision systems responsible for operational control. Table 46 summarizes the unsafe control actions for operational control.

Table 46. Operational Unsafe Control Actions (STPA Step 1)

Unsafe Control Actions	UCA Descriptions	Safety Design Requirements
UCA-OP1. Not providing control action leads to hazard	Operational control fails to command separation maneuver when required safe separation violation imminent. (←H1)	OP1. Operational control shall command conflict-free separation maneuver when separation violation imminent. ⁹
UCA-OP2. Providing control action causes hazard	UCA-OP2.1. Separation maneuver commanded into another aircraft safe separation zone. (←H1)	OP2.1. Operational control separation maneuver commands shall avoid aircraft separation boundaries.
	UCA-OP2.2. Operational control commands separation maneuver terrain when separation violation imminent. (←H2)	OP2.2. Operational control separation maneuver shall avoid terrain.
	UCA-OP2.3. Operational control commands separation maneuver during critical flight phases (low energy, high drag, and high workload). (←H2, H3)	OP2.3. Operational control shall use separation commands that increase energy and are directive (simple) during critical flight phases.
UCA-OP3. Provided	Operational control commands separation	OP3. Operational control will account

⁸ Safety is controlled top-down. From a system-theoretic approach, lost link procedures for UAS integration need to be mandated by strategic control versus by individual aircraft as is currently done with UAS Certificate of Authorizations.

⁹ “Workload permitting” and “when the work situation permits” are accepted reasons for Air Traffic Control to not do something related to safety (Federal Aviation Administration 2014a). From a systems-theoretic safety design perspective, workload permitting is not safe control. If workload does not permit safe control actions then design a solution—improve feedback, improve decision aids, decrease traffic, or improve procedures are potential solutions.

at incorrect time (too early/late) or wrong sequence	maneuver too late for system response capabilities when separation violation imminent. (←H1, H3)	for system response capabilities: communications, operator reactions, and aircraft maneuver capability.
UCA-OP4. Provided for incorrect duration (too soon/long)	UCA-OP4.1. Operational control separation maneuver is stopped too soon when required for safe separation. (←H1)	OP4.1. Operational control separation commands shall have magnitude and duration to safely separate.
	UCA-OP4.2. Operational control separation maneuver is held too long when required for safe separation, maneuvering into another aircraft's safe separation zone or terrain. (←H1, H2)	OP4.2. Operational control separation commands shall have magnitude and duration to avoid initial and follow-on aircraft and terrain obstacles.

Now, STPA step 2 causal analysis is conducted, which asks *why* did the unsafe control action occur? Only a few selected unsafe control actions are addressed to highlight how STPA: 1) finds unsafe controls and scenarios already acknowledged in documents, and 2) can derive safety design insights not previously acknowledged or considered.

Why would UCA-OP2.1 occur, commanding a separation maneuver into another safe separation zone? I will use TCAS for the next two examples as it is analogous to the DAA functions. The as-is NAS architecture does not require TCAS RA feedback for ATC to use. Here is one of many potential unsafe scenarios:

Scenario A. ATC is controlling two aircraft that are on a collision course. The controller is not aware of the situation or falsely believes that the conflict is not a problem. Aircraft A is equipped with TCAS II and Aircraft B is not equipped. Aircraft A is given an RA to climb. At the same time, ATC becomes aware and issues a climb command to Aircraft B. The two aircraft have a near mid-air collision best case and a mid-air collision worst case.

One industry answer to Scenario A is to implement TCAS reversal logic. Here is the same scenario except current reversal TCAS II logic is included:

Scenario B. ATC is controlling two aircraft that are on a collision course. The controller is not aware of the situation or falsely believes that the conflict is not a problem. Aircraft A is equipped with TCAS II and Aircraft B is not equipped. Aircraft A is given an RA to climb. At the same time, ATC becomes aware and issues a climb command to Aircraft B. 10 seconds goes by while the results of actions settle out, and collision is still imminent. Aircraft A reverses based on TCAS II logic. At the same time, ATC reverses command telling Aircraft B to descend immediately. The two aircraft have a near mid-air collision best case and a mid-air collision worst case.

The safe separation of two or more aircraft in the NAS results from the actions of multiple decision systems. Fixing the DAA algorithm alone to address Scenario A or Scenario B is a *local* attempt to solve a system safety problem. A DAA algorithm fix would not help the unsafe interactions that led ATC to provide the unsafe control actions in Scenarios A and B. The NAS decision systems shall be designed to interact safely, which requires integration. A safety design paradigm shift is needed from design of an *independent* DAA safety barrier to one where DAA is an integrated *additional* safety function.

Going back to the safety control structure Figure 4, we have the functional relationships between decision systems that should exist for safe control. Feedback between decision systems is required. Current guidance for pilots reacting to a TCAS RA is to provide feedback “as soon as practicable after responding to the RA” (Federal Aviation Administration 2011) p. 39, which would be required if deviating from a clearance or instruction. This may not be timely feedback on either the decision to maneuver or the executing the maneuver itself. In addition to lack of timely pilot feedback, the TCAS RAs are not displayed in most ATC work stations around the world (Beadle 2010). In the few countries where TCAS RAs are displayed, it is apparently not in real-time. ATC needs feedback from the DAA to safely control air traffic. Even better feedback to ATC is the pilot’s decision regarding the avoidance maneuver because the pilot is responsible for sending the control signal (flight controls).

Current regulation alleviates ATC of responsibility during TCAS RAs, “...the controller is not responsible for providing standard separation between the aircraft that is responding to an RA and any other aircraft, airspace, terrain or obstructions” (Federal Aviation Administration 2014a) p. 2-1-12. Without adequate feedback, there are safety concerns involved with relinquishing control during the time when safe control could be most beneficial. Let us look at the same scenarios above, but now with timely information feedback from TCAS. A plausible outcome is ATC provides Aircraft B (non-TCAS) with an initial command other than climb (TCAS issued maneuver for Aircraft A) that not only negates the collision potential but also minimizes traffic flow disturbances. With TCAS feedback, ATC knows who has a TCAS RA and can continue to safely control the non-TCAS aircraft or leave alone those pairs responding to TCAS RAs.

Recommendation 2. ATC shall have timely feedback on the tactical decision systems it controls, which includes information on the DAA system maneuver suggestions and the remote pilot’s decision.

How about UCA-OP1, not providing a safe control when one was required for safe separation? One pertinent scenario relating to lost link and loss of communications and control:

Scenario C. There is an IFR UAS and a VFR general aviation aircraft in the same airspace. ATC has been in continuous and recent contact with the UAS. ATC issues a vector to remain clear of the VFR GA traffic. The GA traffic subsequently turns into the UAS and is on a potential collision trajectory. At the same time, the remote pilot temporarily loses control of the UAS (lost link) and communications with ATC. ATC realizes the impending situation, only now the scenario is more time pressured than earlier. ATC vectors the UAS to avoid the GA aircraft, but there is no answer and ATC waits to see if the UAS maneuvers. ATC tries again since there is no positive feedback of the UAS responding. 10 seconds or more has gone by and the potential collision is now only a few seconds away. ATC makes a timely decision to alert the GA aircraft on guard of collision traffic off their nose 2 miles. The GA aircraft is not on the controlling frequency and hears a feint garble over the radio. ATC makes another call over guard, but it is now too late.

The design recommendation is that UAS have capabilities to automatically feedback lost link status to the remote operator and ATC as well. This could be accomplished by an automatic UAS alert (e.g. automatic transponder squawk). One study found the “most” controllers determined lost link within a minute (Kamienski et al. 2010), which may be too late. The FAA recognized the safety implications with UAS

integration and lost link as evidenced by this mandate in the UAS in NAS policy: “In the event of lost link, the UA shall squawk code 7600, if transponder equipped” p. 5 (Federal Aviation Administration 2014b). However, *if* transponder equipped does not solve the control problem when not transponder equipped.

Recommendation 3. Local airspace control (i.e. ATC) shall receive timely feedback on communications and control channels that affect their ability to control the unmanned aircraft.

STPA at the operational control level provided insight into necessary DAA feedback to ATC and reinforced the necessity for lost link feedback for ATC. Feedback to ATC on DAA guidance information is not a matter of *could provide*, but is rather a matter of *should provide* to ATC to prevent unsafe control actions.

B2.3. Tactical Control. UAS Decision System

The UAS decision system responsible for safe maneuvers is comprised of the UAS operator and the DAA. STPA on the UAS decision system analyzes its behavior, and its functional relationships within the decision system and between decision systems. The current function of the DAA is to provide both traffic information and maneuver guidance in the form of suggestions or set of acceptable trajectories. When the DAA system provides trajectory suggestions, it is making a decision related to aircraft control and is part of the decision system function. Automatic UAS control is a potential future function (RTCA SC-228 2014). Figure 7 is the generic control diagram used for STPA. Within decision system (two-way) interactions may exist with the operator and DAA. The generic decision system as a unit interacts with the levels $n+1$ and $n-1$ and coordinates with other level n decision systems.

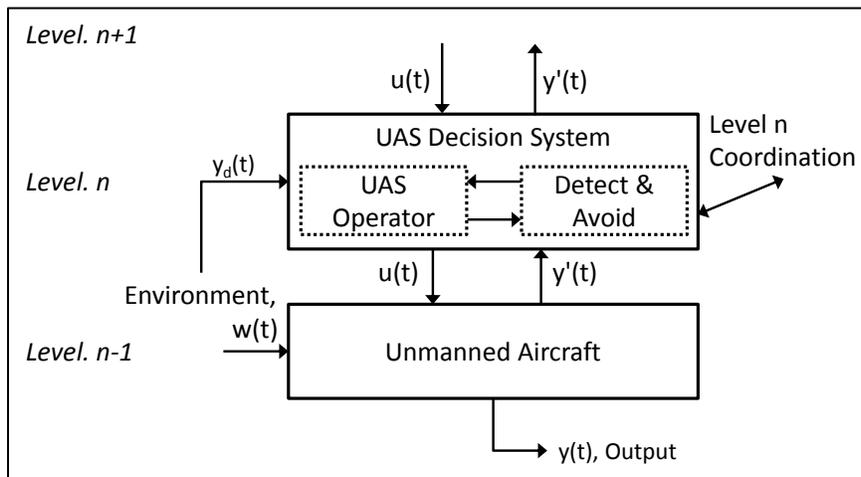


Figure 7. UAS Decision System (Tactical) Control Loop Diagram, General Case

Table 7 shows the UAS decision system constraints needed for safe UAS integration, which are refined from the system level hazards and safety constraints.

Table 7. UAS Decision System Hazards and Safety Constraints

Tactical Control (TAC) Hazards	UAS Decision System Safety Constraints
--------------------------------	--

H-TAC1.1. Loss of separation, collision avoidance threshold (←H1)	SC-UAS1. UAS decision systems shall not allow UA to violate self-separation requirements.
H-TAC1.2. Interference with ATC separation services (←H1)	SC-UAS2. The UAS decision system shall minimize interference with ATC separation service without priority.
H-TAC2.1. TAC induces or contributes to controlled flight into terrain maneuver (←H2)	SC-UAS3. The UAS decision system shall not maneuver the UA into terrain or ground-based obstacles.
H-TAC3.1. TAC induces or contributes to a loss of controlled flight (←H3)	SC-UAS4. The UAS decision system shall not maneuver the UA beyond aero-structural capabilities. SC-UAS5. The UAS decision system shall not maneuver the UA to lose remote control inadvertently.

The control action used in the analysis is a separation maneuver, without further discretization into climb, descent, left, right, speed up, and slow down, or any combination. Discretizing an infinite problem space for this analysis does not have a good stopping point, and the analysis would quickly become intractable. Rather the decision for an acceptable or desired separation maneuver is an operational and tactical consideration already constrained top-down by system requirements to avoid system hazards. For this STPA, the separation control implies any one or combination of the geometry and timing options. This level of abstraction allows for a useful and tractable analysis.

Human factors engineering principles for display design are critical for safe UAS decision system control. However, display design is not a focus of this safety report. In general, DAA system displays shall be intuitive, simple, and follow basic human factors principles (e.g. control-display compatibility principle (Rothrock et al. 2006)) to assist the UAS decision system with:

- Timely separation maneuver responses
- Separation maneuvers in high workload scenarios
- Separation maneuvers near aerodynamic, structural, and control limits where safety margins are small

Table 8 summarizes safety design requirements from analysis of UAS decision system unsafe control actions. The safety design requirements apply to the remote pilot and DAA system, unless specified otherwise.

Table 8. UAS Decision System Unsafe Control Actions (STPA Step 1)

Unsafe Control Action	UCA Description	Safety Design Constraints
UCA-TAC1. Control required for safety is not provided	UAS decision system fails to command separation maneuver when safe separation violation imminent. (←H-TAC1.1)	UAS1. UAS decision system shall command safe separation maneuver when required.

UCA-TAC2. Providing control action causes hazard	UCA-TAC2.1. UAS decision system commands separation maneuver into the intruder when separation violation imminent. (←H-TAC1.1)	UAS2.1. UAS decision system shall not command separation maneuver into intruder.
	UCA-TAC2.2. UAS decision system commands separation maneuver into additional aircraft when separation violation imminent. (←H-TAC1.1)	UAS2.2. UAS decision system shall not induce additional separation violations with initial separation maneuver.
	UCA-TAC2.3. UAS decision system commands separation maneuver into terrain when separation violation imminent. (←H-TAC2.1)	UAS2.3. UAS decision system shall avoid terrain when executing a separation maneuver.
	UCA-TAC2.4. UAS decision system commands separation maneuver that is in conflict with other controls, when separation violation imminent. (←H-TAC1.2)	UAS2.4.1. UAS decision system shall maneuver IAW strategic and operational control constraints. UAS2.4.2. UAS decision system separation maneuvers shall minimize disruption to ATC services.
	UCA-TAC2.5. UAS decision system commands separation maneuver beyond aircraft capability when separation violation imminent. (←H-TAC3.1)	UAS2.5.1. UAS decision system shall have knowledge of aircraft aero-structural capabilities, limitations, and safety margins at the low and high energy flight envelopes. UAS2.5.2. UAS decision system shall be warned when approaching aero-structural limitations. UAS2.5.3. UAS decision system commanded maneuvers shall remain within the aircraft aero-structural flight envelope. Design consideration: Flight control automation may restrict portions of the flight envelope to prevent inadvertent aero-structural limitation excursions.
	UCA-TAC2.6. UAS decision system commands separation maneuver during critical flight phases (high workload, low safety margins, near terrain), when separation violation imminent. (←H-TAC2.1, H-TAC3.1)	UAS2.6.1. UAS decision system shall not decrease energy during critical flight phases, keeping separation maneuvers within environmental (i.e. terrain) and aerodynamic constraints.
	UCA-TAC2.7. UAS decision system	UAS2.7.1. UAS decision system shall

	commands separation maneuver that disrupts continuous remote aircraft control, when separation violation imminent. (←H-TAC1.1, H-TAC1.2, H-TAC2.1, H-TAC3.1)	command maneuvers within the aircraft's C2 link acceptable envelope to prevent inadvertent lost link. UAS2.7.2. UAS decision system shall not command UAV into environments prohibitive to C2 function.
UCA-TAC3. Provided at incorrect time (too early/late) or wrong sequence	TAC3.1. UAS decision system commands separation maneuver too late for system response capabilities when separation violation imminent. (←H-TAC1.1) • Too early: not desired	UAS3.1.1. UAS decision system shall not delay separation maneuver command. UAS3.1.2. UAS decision system shall compensate separation maneuvers for communication and aircraft response delays. UAS3.1.3. DAA alerts shall provide the decision system enough time for its decision and action functions.
UCA-TAC4. Provided for incorrect duration (too soon/long)	UCA-TAC4.1. UAS decision system stops maneuver too soon when required for safe separation. (←H-TAC1.1)	UAS4.1. UAS decision system shall hold separation maneuver for the necessary duration to avoid or exit a separation violation.
	UCA-TAC4.2. UAS decision system holds maneuver too long when required for safe separation, maneuvering into another aircraft's safe separation zone or terrain obstacle. (←H-TAC1.1, H-TAC1.2, H-TAC2.1)	UAS4.2. UAS decision system shall not hold the separation maneuver longer than necessary to avoid the initial intruder.

The STPA causal analysis (step 2) results are next. The analysis focused on identification of hazardous scenarios that were unique to remote flight operations and different from the as-is NAS architecture: human remote operations, the use of sensors for self-separation, and over-the-air communications and control.

B2.3.1. STPA Causal Analysis. UAS Operator

The functional relationships envisioned for the near term were used for the STPA causal analysis, shown in Figure 8. The UAS operator will have final responsibility for the decision system control signal, $u(t)$. The DAA will provide some form of maneuver guidance to the UAS operator, shown as the one-way arrow.

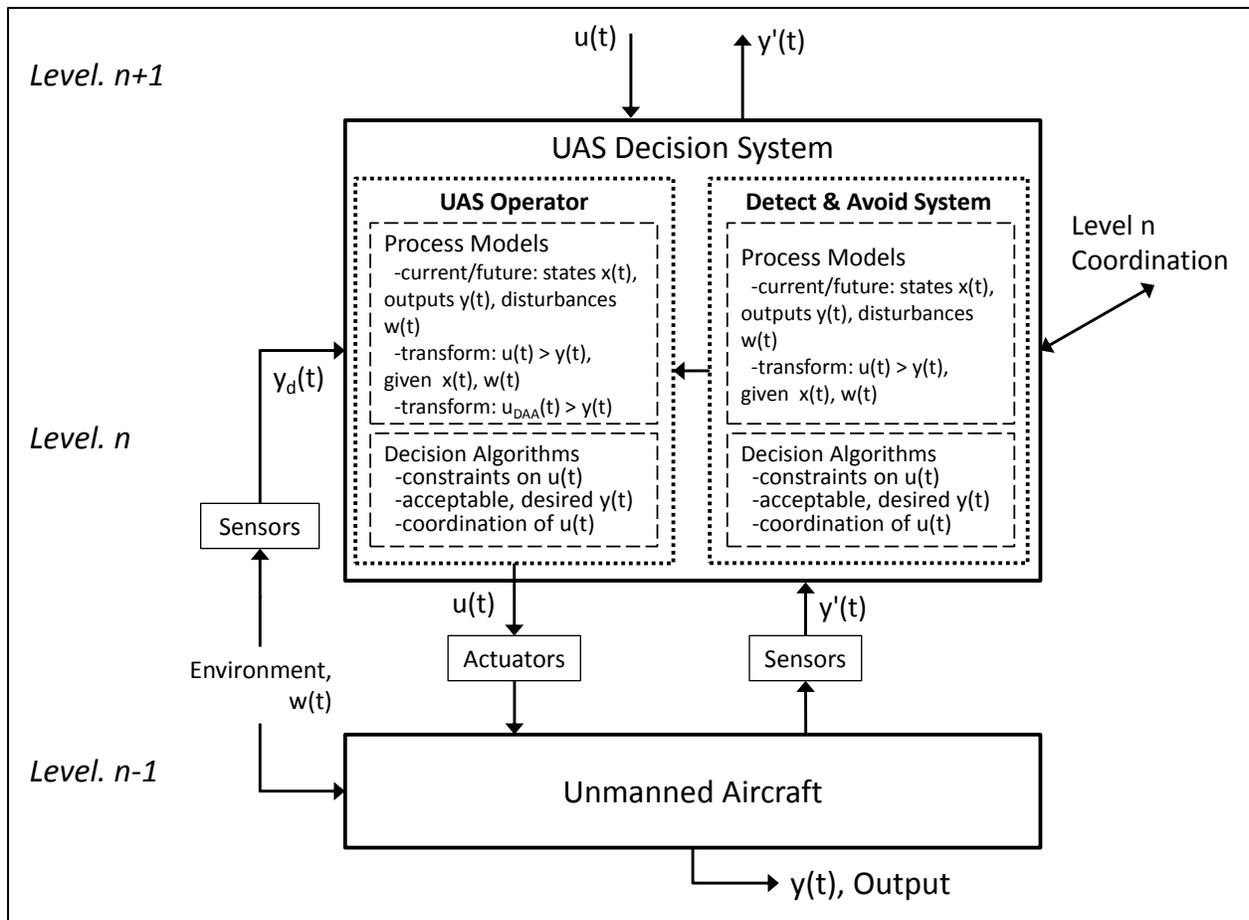


Figure 8. UAS Decision System Current Control Architecture

Mode awareness and trust are significant concerns for safe outcomes in potential collision scenarios, especially when multiple decision systems are involved in a life or death situation. Table 9 presents results from the STPA causal analysis and the recommended design requirements related to mode awareness and trust.

Table 9. STPA on UAS Operator

UCA Description	Scenario	Safety Design Requirements
UCA-TAC1. UAS decision system fails to command separation maneuver when safe separation violation imminent.	The UAS operator does not remember to power on the DAA system, or leaves it in standby mode during flight operations.	1) The DAA shall have an independent alert or caution enunciator for DAA not in operating mode while conducting flight operations. 2) The DAA system should have automatic and independent power on capability for DAA system.
	If DAA mode is manually selected: The UAS operator does not select the	3) The UAS operator shall be trained on mode selection and the

	<p>appropriate DAA mode for the given flight conditions, and a separation maneuver suggestion is not given when required.</p>	<p>corresponding DAA behaviors.</p> <p>4) The DAA system shall prominently display its current mode.</p> <p>5) The DAA shall alert the UAS operator of a potential mismatch between:</p> <ul style="list-style-type: none"> a) DAA mode and flight condition, and b) DAA mode and aircraft configuration
<p>UCA-TAC2.1. UAS decision system commands separation maneuver into the intruder when separation violation imminent. (←H-TAC1.1)</p>	<p>There may be three or more decision systems involved in an ambiguous collision situation. Worse, the maneuver suggestions or commands to the UAS operator may be in conflict. Who is following DAA, who is not? Does ATC already know about my DAA RA or not? Does ATC have better SA than me or not? Is the intruder DAA-equipped or not? Is my DAA coordinating the maneuver or not? These are just a few of the doubting questions when receiving conflicting commands. When one’s life is at stake, blindly following an algorithm that is potentially independent of other decision systems may not be reasonable. The UAS operator may maneuver into the intruder without coordination.</p> <p>Scenario that improves trust in DAA suggested maneuvers: DAA informs UAS operator that intruder accepted the separation maneuver coordination.</p>	<p>6) The UAS operator shall have feedback on coordination between decision systems that maneuver is 1) coordinated and 2) that coordination occurred.</p> <p>7) UAS operator shall have a means to acknowledge acceptance of suggested coordination. The within decision system relationship should have a way for the UAS operator to acknowledge DAA suggestions, shown as the dotted (orange) arrow in this Figure 9:</p> <div data-bbox="1031 1186 1430 1333" style="border: 1px solid black; padding: 5px; text-align: center;"> <p>UAS Decision System</p> </div> <p>Figure 9. UAS Decision System, Within Interactions</p>
<p>UCA-TAC2.4. UAS decision system commands separation maneuver that is in conflict with other controls, when separation violation imminent. (←H-TAC1.2)</p>	<p>ATC instructs climb and DAA suggests a separation maneuver other than climb. The scenarios were discussed in Scenarios A and B, section B2.2 above. The scenario outcome depends upon <i>coordinated</i> maneuvers between two (or more) aircraft to be safe. Coordination does not occur with one DAA making maneuver suggestions in isolation, independent of ATC and other decision systems. The potential for separation violations exists without coordination. Scenarios that improve trust in decision systems</p>	<p>8) The DAA shall receive and incorporate higher level operational controls (ATC) into its separation maneuver algorithm.</p> <p>9) The DAA shall feedback collision avoidance maneuver suggestions to ATC.</p> <p>10) The DAA shall incorporate strategic control rules and regulations into its separation</p>

	<p>that a coordinated maneuver is occurring:</p> <ul style="list-style-type: none"> • If ATC commands descent, followed by DAA descend RA. • If DAA gives descend RA and ATC issues climb to intruder aircraft. 	maneuvers.
--	---	------------

B2.3.2. STPA Causal Analysis. Detect and Avoid System

The DAA system is a component of the UAS decision system. The DAA system is the key technology enabler for integrated UAS operations as currently envisioned through Title 14, Part 91 Code of Federal Regulations §91.111 Operating near other aircraft, §91.113 Right of way rules, and §91.181 Course to be flown (Federal Aviation Administration 2013b). The DAA’s near-term functional relationships are shown in Figure 8 as a one-way interaction with the UAS operator.

The following Table 10 expands on the UAS decision system hazards in Table 7 that are specific to the DAA and describes the corresponding safety constraints.

Table 10. Detect and Avoid Safety Constraints

Detect and Avoid Interaction Hazard	Detect and Avoid Safety Constraints
H-TAC1.2. Interference with ATM separation or information services	SC-DAA1. The DAA system shall keep false alarm rates operationally acceptable. SC-DAA2. The DAA system shall be electro-magnetically compatible with ATC information services.
H-TAC3.1. DAA induces or contributes to flight beyond aero-structural limitations or lost communications	SC-DAA3. The DAA system shall not disrupt UAS operators during critical flight phases. SC-DAA4. The DAA system shall be electro-magnetically compatible with aircraft control.

The following Table 11 summarizes unsafe control actions and design requirements specific to the DAA system, expanded from the decision system unsafe control actions in Table 8.

Table 11. Detect and Avoid System Unsafe Control Actions

Unsafe Control Action	UCA Description	Safety Design Constraints
UCA-DAA1. Not providing control action leads to hazard	same	
UCA-DAA2. Providing control action causes hazard	UCA-DAA2.1. DAA system commands separation maneuver that is in conflict with other controls	DAA2.1. DAA system shall coordinate actions with other collision avoidance systems.

	when separation violation imminent, inducing a separation violation. (←H-TAC1.1)	
	UCA-DAA2.2. DAA system commands energy depleting separation maneuver during critical flight phases, when separation violation imminent. (←H- TAC2.1, H- TAC3.1)	DAA2.2.1. DAA system shall minimize false alarm rates during critical flight phases. DAA2.2.2. DAA system shall produce intuitive and simple to execute guidance to assist the UAS operator in making a low safety margin separation maneuvers during high workload flight phases.
UCA-DAA3. Provided at incorrect time (too early/late) or wrong sequence	UCA-DAA3. DAA system commands separation maneuver too late for system response capabilities when separation violation imminent. (←H- TAC 1.1) • Too early: Not desired	DAA3.1. DAA system commands shall integrate system time response capabilities: communications, human decisions and actions, aircraft maneuver capability, and other time-delayed events.
UCA-DAA4. Provided for incorrect duration (too soon/long)	same	

The DAA system causal analysis results are presented in Table 12, 13, 14, and 15. The STPA results provide a framework to guide design, development, and certification of the DAA system for safe integrated NAS flight operations. Failure scenarios are not addressed in this technical report as that is the focus of the RTCA SC-228 Safety Subgroup. However, the safety control structure models and control loop diagrams can be used for failure assessments to provide a measure of consistency and adequacy in reliability and failure chain hazard analyses.

Table 12. Detect and Avoid System Causal Analysis, Not Providing Control Action Leads to Hazard.

UCA Description	Scenario	Safety Design Requirements
UCA-TAC1. DAA fails to command separation maneuver when required for safe separation.	A non-cooperative intruder is outside self detection field of regard and on a collision course. This scenario may occur in any flight phase and most airspace categories.	11) Self-detection shall have both vertical and horizontal field of regard capability that can account for worst case collision trajectories.
	The DAA algorithm makes inadequate	12) The DAA algorithm shall incorporate

	assumptions about aircraft maneuverability for predicting intruder future state. For intruders with high maneuver performance capabilities, straight line and no acceleration assumptions may be inadequate for safe separation. These assumptions are used for TCAS II (M.J. Kochenderfer et al. 2010).	dynamic horizontal and vertical maneuvers for predicting future intruder states.
	The intruder is inside field of regard but is not detected due to its size or due to its energy reflection/absorption capabilities. The intruder may not be detected inside FOR due to weather occluding EO/IR sensors.	13) Design consideration: A mix of self-detect sensor technologies may be desirable to counter weather and intruder low-detection configurations. Radar and EO/IR sensors are one combination example. 14) The UAS decision system shall not operate the UAS in weather conditions that do not allow self-detection.
	In a multiple intruder environment, the UAS may track them using both cooperative and non-cooperative technology. If a cooperative intruder subsequently loses electronic ID capability, the UAS self-detection ability may be tracking other aircraft and not be capable of tracking more. The dropped intruder may maneuver into a separation hazard condition without the UAS being alerted.	15) The DAA algorithm shall prioritize self-detect energy and sensors on the highest threat intruders. 16) The DAA shall have the ability to change tracked targets. 17) The DAA should minimize time tracking non-cooperative intruders when not a primary threat. a) Rationale. The DAA self-detection capability should maximize time in surveillance mode to ensure non-cooperative intruders found.
	The DAA system has incorrect intruder data due to degraded non-cooperative sensor performance from environmental, energy jamming, or energy spoofing disturbances.	18) DAA shall monitor, detect and feedback degradations to the UAS decision system to make informed maneuver decisions. 19) The DAA shall incorporate intruder uncertainty from its own degradations into separation maneuver guidance. 20) Design consideration. Degradation thresholds should be determined for when DAA function is inadequate for operations.
	The algorithm assumptions may inadequately handle low altitude flight	21) The DAA algorithm shall have a feedback to discriminate between low-

	<p>operations in other than terminal area environments.</p> <p>If low altitude flight is accounted for, the DAA system feedback may be inadequate for the algorithm to distinguish between terminal area operations and low-altitude flight operations.</p> <p>As an example, TCAS II 7.1 provides TAs only below 1000 feet AGL, and aural annunciations are inhibited below 400-600 feet AGL (Federal Aviation Administration 2011). If an RA scenario exists during low altitude operations less than 1000 feet AGL, the pilot would only receive a TA.</p>	<p>altitude flight operations and terminal area operations.</p> <p>22) The DAA shall have feedback to discriminate between the same.</p> <p>23) Design considerations: Potential feedback cues for algorithm logic may include landing and drag devices, or communication signals such as ILS.</p>
	<p>If DAA mode selection is automatic: The mode may believe the aircraft is in one flight phase (or aircraft configuration) but is actually in another. Once example is that the DAA believes it is in landing gear configuration, but is actually in cruise configuration. Maybe a gear or flap malfunction would cause this mismatch. The DAA is now suggesting maneuvers based on the wrong algorithms and models, which may inhibit a correct DAA response.</p>	<p>24) If DAA mode is automatic, based on flight phase: The actual configuration must be observed and the information fed back to the DAA. The flap lever position is not the same as the actual flap position; this is the same with the gear lever and actual gear positions.</p> <p>25) The DAA mode shall be known by the UAS operator.</p>
<p>DAA system commands proper separation maneuver, but it is not executed.</p>	<p>UAS decision system is in high workload conditions, such as conducting a mission or in critical flight phases, and does not recognize that a loss of separation condition exists.</p>	<p>26) The DAA alerts shall make decision system aware of potential collision situation.</p>
	<p>The UAS operator receives a DAA alert to impending separation concerns; however the operator does not comprehend the severity of the condition and wrongly prioritizes other duties seemingly more pressing.</p>	<p>27) The DAA information and alerts shall assist human in understanding the severity of the situation and in making separation maneuver decisions.</p> <p>28) Design consideration. Predicted time to (near) collision or time to maneuver would be useful severity information (e.g. countdown to when maneuver command must begin)</p>
	<p>The DAA may have varying alert levels and guidance based on different separation conditions (see Figure 6). The decision</p>	<p>29) The DAA alerts shall be unique from one another and have an intuitive sense of severity.</p>

	system may not comprehend or receive information that the collision scenario deteriorated and is more likely now.	30) An impending collision alert shall be distinct from any other potential safe separation (i.e. well-clear violation) scenario.
	Up/downlink signal lost during separation maneuver due to aircraft geometry or configuration masking and the aircraft goes into lost link mode.	31) The algorithm shall account for aircraft geometry and configurations when commanding a separation maneuver. 32) The DAA system shall be updated when new configurations are released. 33) Design considerations: a) Flight control automation may keep the aircraft within link limits. b) Design DAA for automatic collision avoidance maneuver if link lost for any reason during manual controlled maneuver.

Table 13. Detect and Avoid System Causal Analysis, Providing Control Action Causes Hazard.

UCA Description	Scenario	Safety Design Requirements
UCA-TAC2.1. DAA system commands separation maneuver into the intruder when separation violation imminent.	Update rates may not capture dynamic maneuver inflections (e.g. climb to descend or left to right) during a separation maneuver decision. For an uncoordinated separation maneuver, the trajectory assumptions may not be valid for high performance and dynamic intruders.	34) <i>See design requirements 8) and 12)</i> respectively and associated hazardous scenarios.
UCA-TAC2.2 DAA system commands separation maneuver into additional aircraft when safe separation violation imminent.	The DAA system does not have the necessary energy to track more than one intruder and commands a separation maneuver to avoid the initial intruder that puts the UAV in a non-safe area.	35) The DAA system shall clear the intended maneuver airspace when intruder conditions permit, such as when the intruder is not yet a threat or when the intruder is not maneuvering.
	There are additional aircraft just beyond the DAA non-cooperative FOR, and the commanded maneuver to avoid the initial intruder induces a safe separation violation of the additional aircraft.	36) Non-cooperative sensor energy shall be coordinated with commanded maneuver to ensure the latest disturbance information during maneuver.

DAA system commands safe maneuver, but maneuver violates separation standards of another aircraft.	Under time duress, a UAS decision system misunderstands the commanded maneuver and does not execute correctly.	37) Displays shall be intuitive and simple, follow standard stimulus-response compatibility principles so that under high time pressures the UAS operator will understand the display.
UCA-TAC2.3. DAA system commands separation maneuver into terrain or ground obstacle, when separation violation imminent.	The DAA system commands a vertical maneuver descend because it does not have terrain or obstacle data or it is incorrect data. The remote operations take away the human senses and awareness of being close to the ground during maneuver duress and the UAS operator follows the descend command.	38) The DAA process models shall have feedback on the UAS current height above terrain. 39) Design considerations: solutions may include accurate digital terrain data or the use of real-time height data from onboard sensors (e.g. RALT).
	The DAA algorithm does not have a coordinated vertical maneuver strategy for flight conditions in close proximity to the ground. Or, the DAA algorithm does not consider or prioritize the ground as a constraint.	40) DAA algorithm shall coordinate maneuvers with the ground as a constraint. 41) Design consideration: For low altitude flight environments, the DAA should coordinate dual climbs, one climb/one level, or horizontal maneuvers IAW airspace collision avoidance guidelines.
DAA system commands a climb maneuver when the terrain is a factor, but the UAV maneuvers towards the ground.	The UAS operator mental model may not be aware of or forgets about the close proximity to terrain and maneuvers against the DAA climb because the decision system believes he/she knows more about the intruder and the environment than the DAA.	42) The DAA system shall have ground proximity information to alert or make the UAS decision system continuously aware of close terrain until the conflict is resolved.
UCA-TAC2.4 (UCA-DAA2.1). DAA system commands separation maneuver that is in conflict with other controls (intruder, ATC, UAS decision system, regulations, etc.) inducing a separation violation.	The DAA system has inadequate requirements for uninterrupted operations in current airspace regulations, such as normal VFR/IFR flight operations in mixed airspaces that allow 500 feet vertical separation. Thus under normal environments, the DAA may command separation when not required and in direct conflict to other airspace controls.	43) DAA separation and collision avoidance guidance shall be compatible with strategic and operational controls.
	The DAA provides maneuver guidance	44) DAA is part of the UAS decision

	<p>is in opposition to ATC guidance. Aware of a potential collision, ATC issues a climb command to one aircraft. Knowing a climb was issued to one aircraft, ATC gives a descend command to the other to ensure a 1000 foot separation. At the same time the DAA provides maneuver guidance to one aircraft opposite to the ATC command. The UAS operator follows the DAA separation maneuver into a collision scenario.</p>	<p>systems and shall receive higher level control inputs to make a coordinated separation maneuver suggestion. DAA shall receive ATC control inputs.</p> <p>45) Timely feedback on decision system/pilot actions is required for ATC and intruder to have confirmation that coordination occurred, updating each decision system’s mental model.</p>
<p>UCA-TAC2.5. DAA system commands separation maneuver that is beyond current aircraft capability.</p>	<p>With such a diversity of actual and expected UAV performance capabilities and limitations, it is possible the DAA algorithm separation command assumptions are not compatible with or do not accommodate current aircraft, current aircraft configuration, or current aircraft flight conditions.</p> <p>This scenario is realistic as the primary collision avoidance technology today TCAS was designed for a <i>typical</i> passenger airliner, and “It would be very challenging to adapt TCAS to accommodate the diversity of unmanned aircraft that are expected to be flying in the NAS” p. 52 (Kochenderfer et al. 2008).</p>	<p>46) The separation algorithm shall be interoperable and compatible with all aircraft.</p> <p>47) The separation algorithm shall account for aircraft’s aero-structural limitations in all flight regimes and aircraft configurations.</p> <p>48) There shall be feedback to the DAA on actual aircraft configuration that affects aero-structural performance, such as landing gear and lift/drag devices to ensure compatible commanded maneuver.</p> <p>49) The algorithm shall have feedback on actual aircraft and configuration to check correct software load and performance parameters.</p> <p>50) Design consideration. The algorithms should be designed to accommodate future performance improvements.</p>
	<p>Near stall, the aircraft does not have sufficient safety margin to execute any maneuver without increasing energy first. If the DAA system commands a climb, for example, and the decision system executes without first increasing velocity a stall may occur.</p>	<p>51) The DAA system shall have specific aircraft aero-structural model limits to incorporate into commanded separation maneuver.</p> <p>52) The DAA system shall command separation maneuvers that also include velocity command for maneuvering on or near aero-structural limits.</p> <p>53) Design consideration. The DAA should be directive to increase or</p>

		decrease velocity, then climb or descend when operations near limits.
	Another limit scenario is flight on or near the UAV structural limits and the DAA system commanding a descent separation maneuver that subsequently causes the UAV to exceed structural limits. Worst case may cause structural damage and loss of controlled flight.	54) On or near the structural aircraft limits, the DAA system shall command a separation maneuver that first improves structural safety margins, such as decreasing velocity.
DAA system commands safe maneuver, but maneuver exceeds aircraft capability.	With remote operations, the communication and control delays may cause PIOs during high stress collision avoidance maneuvers that eventually exceed aero-structural limitations.	55) The DAA shall receive real-time feedback on control loop up/downlink delays to command a safe maneuver. 56) Design consideration: In time pressured scenarios, the DAA should guide (i.e. flight directors) a safe separation maneuver to help prevent PIOs. a) Continuous manual control is difficult to impossible under heavy time delays. 57) Design consideration: The UAS flight control system should monitor for and dampen/filter high frequency control inputs.
	During critical flight phases such as near stall or structural limits, commanded maneuvers may not take into account the little to no safety margins. With lack of in-situ visual and psychomotor cues to remind the UAS operator of near-limit flight, the operator responds too aggressively and maneuvers the aircraft beyond controlled flight.	58) The DAA system shall provide near limit information (e.g. alerts) along with the separation maneuver suggestion in efforts to affect a deliberate and smooth maneuver within limitations. 59) The DAA maneuver guidance near limits should sequence velocity and directional changes as appropriate. a) Low energy example. First increase velocity, and then climb. b) High energy example. First decrease velocity, then descend (or climb). 60) Design consideration. A flight director along with directive aural command may be beneficial for these scenarios.
UCA-TAC2.6 (UCA-	DAA algorithm may be prohibitive for	61) Terminal area challenges the DAA

<p>DAA2.2). DAA system commands separation maneuver during critical phase of flight.</p>	<p>safe flight if designed separation or collision margins and algorithms are not capable of handling normal VFR and approach characteristics of terminal areas and airport pattern operations. An unnecessary separation maneuver increases workload and decreases safe flight margins during an already high workload, low energy, and high drag scenario. Safe operations are degraded with inadequate DAA algorithms to handle normal terminal area flight operations.</p>	<p>system shall account for:</p> <ul style="list-style-type: none"> a) When on final approach (glide slope feedback, gear down feedback, etc.), restrict the surveillance area. b) Slow collision convergence vectors. Incorporate scenarios into alert thresholds to avoid false alarms in closely spaced parallel approaches for example. c) Incorporate VFR electronic identification into TA/RA alert matrix when in terminal environmental conditions. d) VFR pattern operations. Algorithm shall account for potential VFR dynamic maneuvers, both horizontal and vertical while in the terminal area. e) Algorithm shall be able to discriminate between low flying aircraft and aircraft surface movement.
	<p>Future operations were not accounted for in separation algorithm design, such as terminal operations in Class B airspace. Another possibility is an emergency may necessitate operations and landing within Class B.</p>	<p>62) Algorithm shall account for Class B characteristics in case of emergency operations and to ensure future integrated operations in current design.</p>
	<p>The DAA system commands a separation maneuver during terminal area flight operations for an aircraft on the ground due to inadequate algorithm coordination.</p>	<p>63) Cooperative aircraft on the ground shall not interfere with flight operations. 64) The DAA shall be able to filter out surface aircraft information.</p>
	<p>Aircraft transitioning from ground to flight (takeoff) or flight to ground (landing) are not adequately handled by the DAA system and the sudden jump in intruder altitude and velocity may trigger a false alarm.</p>	<p>65) The DAA system shall smoothly handle intruder state transitions between surface and flight in terminal area operations.</p>
<p>UCA-TAC2.7. DAA system commands</p>	<p>The DAA algorithm assumptions may not account for aircraft geometry or</p>	<p>66) <i>See design requirements 31), 32), and 33).</i></p>

separation maneuver that disrupts continuous remote aircraft control, when separation violation imminent.	possible configurations and mask signal during separation maneuver.	
	During LOS operations, the DAA algorithm does not account for terrain between the signal generator and the UAV. When a separation violation is imminent, the DAA commands a separation maneuver that masks the C2 LOS link.	67) The DAA algorithm shall account for LOS C2 terrain masking.

Table 14. Detect and Avoid System Causal Analysis, Control Action Provided at Incorrect Time or in Wrong Sequence.

UCA Description	Scenario	Safety Design Requirements
UCA-TAC3 (UCA-DAA3). DAA system commands separation maneuver too late for system response capabilities when separation violation imminent.	If the DAA system uses a fixed C2 delay value, any conditions which exceed these delays will have a late separation command.	68) UAS link delays are dynamic, and DAA system shall have real-time feedback of both up and downlink time delays. 69) Rationale. Adequate measure of link delays is necessary to for not only safe separation maneuver commands, but also minimizing adverse impact to other NAS participants from unnecessary link delay safety margins.
	If the DAA algorithm assumes a common aircraft performance model with expected values or range of values, then power-limited UAVs may not maneuver in time. For example, 1500 fpm is the current assumed pilot maneuver for TCAS II 7.1 (Federal Aviation Administration 2011). This assumes the aircraft can handle 1500 fpm climb. Maximum climb rates are drastically different between the Global Hawk (HALE) and Predator (medium UAV), 3400	70) The DAA shall have specific aircraft performance models and constraints. 71) Rationale. With such a wide variety of current and future UAV performance characteristics, assumptions may be too restrictive for separation maneuver algorithms. 72) Design consideration: The DAA algorithm should be adaptable to different aerodynamic and performance models and constraints.

	fpm vs. 550 fpm respectively. ¹⁰ The TCAS climb rate assumption and corresponding resolution advisories would not work for the Predator.	
	Intruder is a high performance aircraft and is dynamically maneuvering (turning for example) in a way that decreases separation. Current TCAS update rates on both Mode A/C and Mode S transponders when within RA criteria are 1 hertz (Federal Aviation Administration 2011). In scenarios where the separation is already seconds away from near-collision, and the C2 link delays are several seconds, the DAA surveillance update rate may be inadequate.	73) Intruder update rates shall be adequate for potential dynamic aircraft encounters, especially in airspaces where both VFR and IFR aircraft fly together. 74) The DAA shall account for dynamic intruders in determining non-cooperative sensor energy priorities in multiple intruder scenarios. 75) Design consideration: Aircraft performance and maneuverability may be determined by recent trajectory data (changes in velocity, positions, etc.), or by electronic identification of aircraft type for examples.
DAA system commands on time safe maneuver, but maneuver executed too late.	Downlink communication is not reaching or is delayed in reaching the UAS operator due to electromagnetic interference or other communication errors.	76) The DAA shall be electromagnetic compatible with the NAS, SC-DAA2 . 77) The UAS decision system shall have real-time feedback on C2 delays. 78) The UAS decision system shall be alerted to C2 link delays outside of normal tolerances. 79) Rationale. With this information, the decision system can decide the value of the DAA guidance and take actions to ensure safe flight.
	Downlink or uplink relevant communication is being actively denied or degraded	80) The DAA shall be analyzed for cybersecurity concerns related to unsafe control actions. The command link (control action) and the downlink (feedback) should be assessed in an integrated manner. a) Cybersecurity of the C2 link is a safety concern, but outside the scope of this technical report.
	The UAS operator was task saturated on a mission task and did not hear or	81) DAA system alerts shall make UAS operator aware of severity of threat, whether a

¹⁰ Defense Airborne Reconnaissance Office, 1996. *The Defense Airborne Reconnaissance Office Unmanned Aerial Vehicle (UAV) Annual Report FY1996* (p. 31), Washington, DC.

	<p>recognize a DAA alert for separation. Unaware of how long the alert has been going on, the UAS operator takes a normal amount of time to assess the situation and increase situational awareness to make a maneuver decision. Unknown to the UAS operator however, there is no time remaining for a decision and action; only time to act immediately.</p>	<p>well-clear violation (less severe) or near mid-air collision threshold (more severe) to provide a sense of severity.</p> <p>82) The UAS decision system shall know time remaining to provide a control action that will successfully avoid a separation violation.</p> <p>a) Rationale. Time remaining to collision is not as useful as there is some finite time before the collision that collision is irreversible.</p> <p>83) The DAA should provide a maneuver <i>now</i> suggestion when time to maneuver has expired.</p>
--	---	---

Table 15. Detect and Avoid System Causal Analysis, Control Action Provided for Incorrect Duration.

UCA Description	Scenario	Safety Design Requirements
UCA-TAC4.1. DAA system separation maneuver is stopped too soon when required for safe separation.	The intruder is a non-cooperative dynamic maneuvering aircraft and the commanded maneuver did not adequately update throughout a separation maneuver, stopping while still within an unsafe zone.	<p>84) The DAA system shall continue to update throughout the commanded maneuver.</p> <p>85) The DAA system shall check that UAS is clear of safety thresholds prior to stopping separation maneuver guidance.</p>
	<p>The DAA commands a maneuver that does not allow sensors to track a non-cooperative intruder, and the DAA stops providing intruder and separation information. Loss of track scenarios include:</p> <ol style="list-style-type: none"> 1. The UAS self-detect sensors are masked by the aircraft or configuration stores during the separation maneuver. 2. The UAS maneuvers too aggressively for non-cooperative technology to 	<p>86) The DAA shall continue to command a maneuver until the UAV is in a (predicted) safe zone.</p> <p>87) If maintaining track is necessary for separation:</p> <ol style="list-style-type: none"> a) Command shall guide maneuver in both magnitude and rate to ensure track. b) The DAA shall warn decision system of impending mask or lost track. c) Recommend. Directive alert on corrective maneuver response such as “decrease bank.” d) The DAA system shall incorporate geometric and configuration silhouettes into separation algorithm. e) The DAA shall coordinate multiple sensors to seamlessly track intruder through maneuver. Non-cooperative vs non-cooperative, non-cooperative vs. cooperative. f) The DAA shall have slew rates compatible

	maintain track during separation maneuver.	with UAV maneuverability. 88) If maintaining track is not necessary for separation: a) The DAA shall handle lost intruder tracks during separation maneuvers and continue alert or guidance until (predicted) maneuver complete. b) The DAA shall have ability to maintain sensor energy in direction of intruder with lost track to minimize time without high fidelity track information.
DAA system commands correct maneuver, but the maneuver was stopped too soon.	Up/downlink signal lost during separation maneuver due to aircraft geometry or configuration masking and the aircraft goes into lost link mode.	89) <i>See Design Requirements 31), 32), and 33).</i>
	The UAS operator does not understand the temporal relationship between the separation guidance display and actual separation scenario due to inherent C2 link time delays, and incorrectly stops the separation maneuver before safely separated.	90) To minimize potential confusion in time constrained scenarios, the DAA should provide separation maneuver guidance that is more directive; at least part of the guidance should be directive. 91) Design considerations. a) A flight director could accomplish directive separation maneuver guidance. b) Under less time duress, e.g. a well clear violation, the DAA may provide maneuver guidance suggestions or traffic information only. 92) The DAA shall receive feedback on UAS decision system control outputs to alert when separation controls released too soon.
UCA-TAC4.2. DAA system commands separation maneuver too long, maneuvering into another aircraft's safe separation zone or terrain obstacle.	The DAA system process model has inadequate feedback on C2 link delays and commands separation too long in a direction that places the UAV into another unsafe zone. High density terminal area flight operations may be especially prone to these disruptions.	93) The DAA system shall have real-time feedback of C2 link delays and incorporate this information into the separation guidance stopping set point. 94) The DAA separation maneuver shall be adequate to clear current threat, but not held longer than necessary. 95) Rationale. A separation maneuver held longer than necessary may create additional conflicts or further disrupt the NAS, increase workload for all controllers, and degrade safety.

	The DAA may lose track of an intruder during a maneuver and overcompensate separation guidance to improve likelihood that UAV will be clear of unsafe scenario.	96) See <i>UCA.TAC4.1</i> this table for constraints on maintaining intruder track. 97) Design consideration. a) Ensuring safe separation from the current known threat is a high priority, and intruder location uncertainty shall be taken into account. b) It may be acceptable to infringe on another safe zone to ensure clear from initial intruder.
DAA system commanded a correct separation maneuver, but the maneuver was executed too long.	The UAS operator executes maneuver too long because there is no clear information or guidance on when the maneuver should stop or when the unsafe environment has passed.	98) The DAA system shall unambiguously transition from safe separation maneuver suggestions to a safe state. 99) The DAA system should provide the UAS operator with an unambiguous <i>stop</i> separation maneuver suggestion.
	The human natural tendency may be to overcorrect to ensure safe separation.	100) The DAA shall receive feedback on the UAS decision system control outputs to alert when controls are held too long.

B3. Conclusions

How do we design safe UAS integration into the NAS? STAMP provides an alternative system-theoretic model of accident causality used in this report to address this challenging question. STAMP treats safety as a control problem, and it captures accident scenarios more typical of complex sociotechnical systems—human error, software error, inadequate design requirements, flawed interactions and missing functions. Based on STAMP, the safety analysis used STPA to identify unsafe controls and unsafe scenarios. From these unsafe controls, unsafe scenarios, and the use of hierarchical functional control models, safety design was to figure out how to eliminate the hazardous scenarios.

The report presented STPA results and the derived safety design constraints and requirements. I want to highlight a fundamental difference between STAMP and failure event chain accident models. STPA derived design requirements *integrate* the DAA function into the NAS as an *additional* safety function; whereas DAA design in a failure chain is treated as an *independent* safety barrier. In summary, it is recommended to use the STPA derived safety design requirements herein for DAA certification of black box behaviors and interactions.

This report is primarily the efforts of the author alone, which is a limitation. While having aviation and safety experiences, I did not have the benefits of additional expertise for the analysis and developing design requirements. You may disagree with the STPA analysis and design recommendations, or feel I missed hazardous scenarios; this is the nature of qualitative inquiry regardless of how many people participated. However, the report has benefits beyond the technical safety content. It is my hope that the

report provides industry with an adequate systems-theoretic framework to conduct STPA independently and to level of detail desired as the DAA system design matures.

Safety is the freedom from conditions that cause accidents, and this report leads UAS integration closer to reaching this goal.

APPENDIX C. STPA-Coordination Frequency Analysis

This appendix provides the STPA-Coordination coding data used for frequency and comparison analysis. Coding consisted of counting unique STPA-Coordination hazardous scenarios and recommendations, while using similar abstraction levels consistent with the DO-344 FHA results and functional requirements analysis. Table and Table 48 show the STPA-Coordination frequency analysis data, with hazardous scenario count in the left two columns and recommendation count in the right two columns. These tables are excerpts of the tables used in Chapter 5 to present STPA-Coordination results.

Table 47. STPA-Coordination Lateral Coordination, Count Data

Scenarios		STPA-Coordination: UAS DS Lateral Coordination	Recommendations and Considerations	Rec's	
128	71	Case 1. Coordination Missing.		139	84
UAS	DAA			UAS	DAA
0		1. Coordination Goals. n/a	n/a	0	
0		2. Coordination Strategy. n/a.	n/a	0	
0		5. Group DM. n/a. UAS and aircraft decision systems can engage in pre-planned or real-time group DM.	n/a	0	
		Case 2. Coordination Inadequate.			
0		1. Coordination Goals. n/a	n/a	0	
0		2. Coordination Strategy.	<ul style="list-style-type: none"> Comprehensive lateral coordination shall be established between UAS and aircraft decision systems Vertical ATC coordination shall be established as determined by STPA-Coordination analysis UAS decision systems shall provide emergency status to others for integration into coordination maneuvers. Consider. Aircraft decision systems involved in a collision scenario shall make positive corrections to mitigate collision potential. Standardization and the DAA To reduce ambiguity, UAS decision systems shall follow one coordination strategy at a time 	1	0
1	0	<ul style="list-style-type: none"> Decision systems have alternative lateral maneuver strategies for collision avoidance while operating in shared airspace. 		1	0
1	1	<ul style="list-style-type: none"> (within DS) The DAA may provide guidance that is not compatible with an emergency scenario. 		2	1
3	3	<ul style="list-style-type: none"> (Within DS) The DAA provides a maneuver envelope to aircrew. 		3	1
4	1	<ul style="list-style-type: none"> Use of lateral coordination strategy for collision avoidance can be ambiguous. 		6	6
2	2	<ul style="list-style-type: none"> (within DS) The DAA does not calculate and integrate into coordination maneuver strategy the time when maneuvers can no longer influence an NMAC—a no-influence threshold. 		1	0

1	1	<ul style="list-style-type: none"> (within DS) Strategy is safe, but UAS aircrew do not follow them due to ambiguity with DAA displays and information. 	<ul style="list-style-type: none"> Assuming comprehensive coordination, strategy shall use a layered approach to collision avoidance. The DAA shall provide cooperation status with other aircraft decision systems to the UAS aircrew. Consider. All aircraft in shared airspace should have compatible collision avoidance equipment. Consider. All flight operations in shared airspace shall use a single frequency, verbal and digital. The DAA/CAS shall account for time when maneuvers can no longer influence an unsafe outcome (i.e. NMAC) The DAA shall account for individual UAS performance and energy characteristics for calculating the dynamic no-influence threshold. The DAA shall unambiguously display maneuver guidance, 	2	0
				1	1
				1	0
				1	0
				1	1
				1	1
				1	1
0		3. Decision Systems. n/a		0	
0		4. Communications.	<ul style="list-style-type: none"> DAA communication shall be compatible with existing collision avoidance systems, or 	1	1
1	0	<ul style="list-style-type: none"> The bandwidth required for lateral coordination is inadequate. For UAS and DAA operations, 	<ul style="list-style-type: none"> Collision avoidance systems shall be upgraded for compatibility. 	1	0
1	1	<ul style="list-style-type: none"> (within DS) The DAA send/receive protocols and language may not be compatible with other collision avoidance or electronic identification systems. 	<ul style="list-style-type: none"> Communication bandwidth shall permit (near) real-time DAA coordination with other decision systems when needed for collision avoidance. 	1	0
1	0	<ul style="list-style-type: none"> The channel capacity required for UAS and DAA lateral coordination efforts is inadequate. 	<ul style="list-style-type: none"> Communication channel capacity shall meet (near) real-time information requirements needed for lateral coordination. 	1	0
5	1	<ul style="list-style-type: none"> Communication transmissions occluded or degraded potentially due to: 	<ul style="list-style-type: none"> The location of communications equipment shall not interfere with coordination-related communication transmissions. 	1	0
			<ul style="list-style-type: none"> The placement of communications equipment shall not unduly limit UAS maneuvers 	1	0

			<ul style="list-style-type: none"> The DAA shall be electromagnetically compatible with onboard and external equipment. 	1	1
			<ul style="list-style-type: none"> If maneuver limits are needed to prevent degraded or interrupted communications, the UAS decision system shall know limitations: 	4	1
0		5. Group DM.	<ul style="list-style-type: none"> Regulations shall establish group DM protocols. 	4	1
3	0	<ul style="list-style-type: none"> Aircrew do not use available communication channels, verbal or digital, for group DM. 	<ul style="list-style-type: none"> The DAA shall inform aircrew if maneuver guidance is in cooperation with other aircraft. 	1	1
1	0	<ul style="list-style-type: none"> Aircrew do not observe the correct communication channels and cannot engage in group DM. 			
1	1	<ul style="list-style-type: none"> (within DS) The DAA may or may not be in cooperation with the other aircraft. 			
0		6. Observation of Common Objects.	<ul style="list-style-type: none"> Decision systems shall share observed information with each other. 	1	1
5	4	<ul style="list-style-type: none"> One or more aircraft decision systems do not observe each other because of the following: 	<ul style="list-style-type: none"> UAS decision systems shall have station keeping and navigational capability 	1	0
1	0	<ul style="list-style-type: none"> Aircraft decision systems do not observe each other in shared airspace because they do not expect each other. 	<ul style="list-style-type: none"> UAS decision systems shall be alerted to special use airspace boundaries. 	1	0
1	0	<ul style="list-style-type: none"> One or more aircraft decision systems do not observe the same surrounding aircraft (same reasons as for not observing each other). 	<ul style="list-style-type: none"> Consider. DAA shall have a mode that alerts when intruder is within a safety envelope 	1	1
2	1	<ul style="list-style-type: none"> Aircraft decision systems cannot resolve maneuver guidance that is deemed unsafe by one and not the other decision system. 	<ul style="list-style-type: none"> UAS decision systems shall fly in a manner that accounts for observation equipment limitations. 	1	0
3	3	<ul style="list-style-type: none"> (within DS) The DAA does not observe the same objects as the aircrew and subsequently provides maneuver guidance that aircrew will not follow. 	<ul style="list-style-type: none"> Decision systems shall observe or otherwise have knowledge of terrain and ground obstacles. 	1	1
1	1	<ul style="list-style-type: none"> (within DS) UAS aircrew observe different aircraft than the DAA. 	<ul style="list-style-type: none"> The DAA shall have a means to check observation of common objects with other collision avoidance systems. 	4	4
			<ul style="list-style-type: none"> The DAA shall (re-) negotiate a compatible and safe maneuver set where UAS maneuvers are constrained by other ground or airborne objects. 	1	1
			<ul style="list-style-type: none"> Consider. Design and regulation requirements to ensure electronic 	1	0

			identification capability on aircraft and other airborne objects flying in the NAS.		
			<ul style="list-style-type: none"> Consider. The DAA shall have self-observation capability beyond sector coverage, such as forward hemisphere coverage. 	2	2
			<ul style="list-style-type: none"> Visual correlation to factor traffic shall be used to assist UAS decision systems. Visual correlation may be achieved through: 	2	2
0		7. ARA.	<ul style="list-style-type: none"> Coordination strategy shall establish accountability or protocol to achieve accountability 	1	0
1	0	<ul style="list-style-type: none"> Decision systems are not on same frequency and accountability does not exist. 	<ul style="list-style-type: none"> Consider. Regulations should allow decision systems to achieve accountability on same frequency as ATC. 	1	0
1	0	<ul style="list-style-type: none"> Decision systems are on the same frequency, whether controlled or uncontrolled airspace. Decision systems may not acknowledge strategy or provide updates on the execution of the strategy for other decision systems. 	<ul style="list-style-type: none"> The DAA/CAS shall provide means to establish lateral coordination accountability. Accountability requirements at a minimum shall include: 	6	3
3	3	<ul style="list-style-type: none"> (within DS) DAA provides maneuver guidance without other decision system cooperation. Lack of cooperation may occur from: 	<ul style="list-style-type: none"> ATC and aircrew shall be trained in collision avoidance accountability requirements. 	1	0
5	1	<ul style="list-style-type: none"> (within DS) The DAA does not have means to establish accountability for lateral coordination. 			
0		8. Common Understanding.	<ul style="list-style-type: none"> With comprehensive coordination, regulations shall prescribe a layered set of coordination strategies 	1	0
1	0	<ul style="list-style-type: none"> There are alternative coordination strategies for collision avoidance and UAS decision systems are not aware of which strategy is being used. 	<ul style="list-style-type: none"> To assist UAS aircrew common understanding of factor airborne and ground obstacles and collision time constraints, the DAA displayed information: 	3	3
9	4	<ul style="list-style-type: none"> UAS decision systems may have different understanding or awareness of the severity of the separation violation scenario. 	<ul style="list-style-type: none"> Display of ownship state and relative state information to factor obstacles shall be unambiguous to UAS aircrew. 	1	1
3	0	<ul style="list-style-type: none"> Common understanding may be hindered by too much uncertainty in decision system states. Uncertainty may derive from: 	<ul style="list-style-type: none"> The DAA system shall have distinctive alert levels to signify severity. 	1	1

2	2	<ul style="list-style-type: none"> (within DS) DAA state information or state information received from other aircraft decision systems may be missing or wrong due to: 	<ul style="list-style-type: none"> Severity alerts shall be consistent across collision avoidance systems. 	1	1
1	1	<ul style="list-style-type: none"> (within DS) DAA provides ambiguous information to UAS aircrew relating to ownship state or state relative to separation/collision potential. 	<ul style="list-style-type: none"> Disabling DAA cautions and warnings shall be a deliberate action to avoid inadvertent disabling. 	1	1
4	4	<ul style="list-style-type: none"> (within DS) DAA maneuver guidance does not integrate the same information or constraints as other decision components 	<ul style="list-style-type: none"> Cautions and warning shall be "on" as default. 	1	1
1	1	<ul style="list-style-type: none"> (within DS) The performance models and assumption used to determine maneuvers may be different for each decision system, which may lead to UCAs. 	<ul style="list-style-type: none"> The DAA system shall meet minimum uncertainty requirements for flight certification. 	1	1
3	3	<ul style="list-style-type: none"> (within DS) The set of possible maneuvers to solve a potential collision scenario is different for each decision component, which may lead to UCAs. 	<ul style="list-style-type: none"> The DAA system shall meet minimum reliability requirements for flight certification. 	1	1
2	2	<ul style="list-style-type: none"> (within DS) DAA and collision avoidance automation used by each aircrew may be in automation modes that are incompatible and provide different decision information to each aircrew. 	<ul style="list-style-type: none"> Decision systems shall be alerted when state information may be missing, incorrect, or beyond acceptable uncertainty. 	3	3
3	3	<ul style="list-style-type: none"> (within DS) The DAA provides guidance that unidirectional (i.e. climb only, left turn only, etc.) because of observed obstacles. 	<ul style="list-style-type: none"> Decision systems shall integrate the same information for collision avoidance maneuver decisions, including: 	2	2
4	0	<ul style="list-style-type: none"> Verbal radio communications help aircrew build common understanding. Aircrew may be on different radio frequencies: 	<ul style="list-style-type: none"> Decision systems shall use the same or similar performance models for a given aircraft and configuration. 	1	1
1	1	<ul style="list-style-type: none"> (within DS) The DAA knows if the alerts and maneuver guidance are in cooperation with other aircraft decision systems. 	<ul style="list-style-type: none"> Consider. Aircraft decision systems shall use the same set of maneuver combinations to ensure common understanding 	1	1
1	1	<ul style="list-style-type: none"> (within DS) The DAA believes it is in cooperation with another CAS, but in fact the other aircraft is not controllable due to some failure or degradation of systems related to flight control. 	<ul style="list-style-type: none"> The DAA/CAS shall communicate separation and collision avoidance maneuver limitations 	1	1
1	1	<ul style="list-style-type: none"> (within DS) The DAA has different alerting thresholds than other CAS for developing and providing collision avoidance maneuver guidance. 	<ul style="list-style-type: none"> The DAA shall not be constrained in maneuver guidance by a limited maneuver set of other collision avoidance systems. 	1	1
			<ul style="list-style-type: none"> Consider. The set of collision avoidance maneuvers to include 	1	1

			vertical, horizontal		
			<ul style="list-style-type: none"> The DAA shall have a means to alert other decision system of incompatible or incorrect mode for cooperation, 	1	1
			<ul style="list-style-type: none"> The DAA shall receive alerts from other collision avoidance systems if in standby or other incompatible mode for cooperation. 	1	1
			<ul style="list-style-type: none"> The DAA shall highlight (e.g. by display) airborne and ground obstacles that are accounted for in the maneuver guidance to help assist common understanding with the UAS aircrew. 	1	1
			<ul style="list-style-type: none"> The DAA shall give cooperation status when providing collision alerts 	1	1
			<ul style="list-style-type: none"> Aircraft decision systems shall alert each other (and ATC) when aircraft is not fully controllable so coordination can account for inability to maneuver. 	1	1
			<ul style="list-style-type: none"> The DAA shall alert other DAA/CAS when the UAS is no longer controllable by aircrew. 	1	1
			<ul style="list-style-type: none"> Consider, the DAA shall automatically cooperate and maneuver for collision avoidance should UAS aircrew flight controls fail or degrade. 	1	1
			<ul style="list-style-type: none"> Consider. The DAA alerting thresholds shall match other CAS thresholds for collision avoidance in efforts to promote timely 	1	1
0		9. Predictability.	<ul style="list-style-type: none"> Temporal constraints for maneuvering shall be known by decision systems. 	3	3
2	1	<ul style="list-style-type: none"> The decision systems may be missing temporal constraints to predict when maneuvers are required (□UCA1.0) 	<ul style="list-style-type: none"> Consider use of worst-case temporal models. If other than worst-case models are used 	1	1
1	0	<ul style="list-style-type: none"> The decision systems may have incorrect temporal models or not account for worst case environment impact on time 	<ul style="list-style-type: none"> Decision systems shall share maneuver intentions. 	1	0
3	3	<ul style="list-style-type: none"> (within DS) Without accountability, DAA ability to predict is limited against an observed decision system maneuvering independently. Problems may arise when: 	<ul style="list-style-type: none"> The DAA system shall meet minimum uncertainty requirements for flight certification. 	1	1

1	1	<ul style="list-style-type: none"> Predictability may be hindered by uncertainty in decision system states. 	<ul style="list-style-type: none"> Decision systems shall be alerted when state information may be incorrect from system degradation or failures. 	3	1
2	2	<ul style="list-style-type: none"> DAA information from one or more aircraft decision systems may be wrong due to: 	<ul style="list-style-type: none"> The DAA shall integrate accountability information (i.e. confirmation of maneuver strategy received and agreed) to maneuver guidance. 	1	1
3	0	<ul style="list-style-type: none"> Predictability is inadequate when not sharing decision system maneuver intentions. 	<ul style="list-style-type: none"> Consider. When accountability is established between decision systems, the DAA should reduce maneuver guidance uncertainty to reflect improved predictability. 	1	1
1	1	<ul style="list-style-type: none"> (within DS) The DAA may not update and improve maneuver guidance when accountability established between decision systems. 	<ul style="list-style-type: none"> The DAA shall use performance models that account for various aircraft and configurations. 	1	1
2	2	<ul style="list-style-type: none"> (within DS) The performance models used for determining maneuvers are inadequate, which may be caused by: 	<ul style="list-style-type: none"> The DAA and CAS shall share aircraft type and configuration for use in coordination. 	1	1
		Case 3. Coordination Leads to Hazard.			
0		2. Coordination Strategy.	<ul style="list-style-type: none"> Coordination strategy shall account for aerodynamic and performance limitations. 	1	0
4	0	<ul style="list-style-type: none"> Not feasible. 	<ul style="list-style-type: none"> The DAA shall account for aircrew (human) performance limitations. 	1	1
0		<ul style="list-style-type: none"> Not acceptable. 	<ul style="list-style-type: none"> The coordination maneuver strategy shall include adequate start and stop times, which are explicit in maneuver guidance. 	1	0
1	0	<ul style="list-style-type: none"> The coordination strategy does not provide a stop time or provides an inadequate stop time. 	<ul style="list-style-type: none"> The coordination strategy shall not maneuver aircraft to cross altitudes 	1	0
0		<ul style="list-style-type: none"> (within DS) DAA and CAS recommend maneuvers that lead to UCAs. 	<ul style="list-style-type: none"> Consider. If cross altitude maneuvers are deemed acceptable 	1	0
2	2	<ul style="list-style-type: none"> Coordinated maneuvers have aircraft cross flight paths (i.e. the maneuvers are into each other. 	<ul style="list-style-type: none"> The coordination strategy shall not maneuver aircraft into additional airborne obstacles that may lead to another mid-air collision. 	1	0
3	3	<ul style="list-style-type: none"> Maneuver one or more of the aircraft into other airborne obstacles. In such cases, the coordination strategy could lead to other separation violations. 	<ul style="list-style-type: none"> The coordination strategy shall not maneuver aircraft towards terrain 	6	0
4	4	<ul style="list-style-type: none"> Maneuver one or more aircraft towards terrain or other ground obstacles. 	<ul style="list-style-type: none"> The DAA shall alert UAS aircrew when missing terrain data, 	1	1

			corrupted, or expired terrain data		
			<ul style="list-style-type: none"> □ The DAA shall account for follow on traffic post-maneuver. 	1	1
Case 4. Coordination is Late.					
0		1. Coordination Goals. n/a			
3	0	2. Coordination Strategy.	<ul style="list-style-type: none"> The coordination elements shall integrate to establish an acceptable strategy within dynamic time constraints. 	0	
0		3. Decision Systems. n/a			
0		4. Communication.	<ul style="list-style-type: none"> The DAA shall have a means to measure communication delays between aircraft decision systems and ATC. 	1	1
1	1	<ul style="list-style-type: none"> (within DS) The DAA does not account for communication delays in determining separation alerts and maneuver guidance. 	<ul style="list-style-type: none"> The DAA shall integrate communication delays into alerts and maneuver guidance. 	1	1
0		5. Group DM. Group DM processes may lead to UCAs.	<ul style="list-style-type: none"> If digital means are used to assist in group DM, the DAA shall have standard messages available for negotiation 	1	1
1	0	<ul style="list-style-type: none"> If group DM uses digital means, the process may take too long. 	<ul style="list-style-type: none"> Decision time constraints shall be calculated for UAS decision systems and displayed for aircrew using one or a combination of visual, audio, and tactile feedback displays. 	1	0
1	0	<ul style="list-style-type: none"> Group DM protocols do not track time constraints on the current separation or collision scenario. In such cases, 	<ul style="list-style-type: none"> The DAA shall provide maneuver guidance with enough time for individual UAS aircrew to make decisions and take actions. 	1	1
1	1	<ul style="list-style-type: none"> (within DS) The DAA maneuver guidance does not account for human performance limitations, such as the time needed to make decisions and take actions. 			
1	0	6. Observation of Common Objects.	<ul style="list-style-type: none"> Update rates shall be adequate for (near) real-time coordination of separation maneuvers. 	1	0
0		7. ARA. Authority and Responsibility.	<ul style="list-style-type: none"> Decision systems shall have coordination authority; regulation shall allow them to engage in lateral coordination as needed for collision avoidance. 	1	0
1	0	<ul style="list-style-type: none"> Establishing coordination authority and responsibility takes time that may not exist when there is a collision scenario 	<ul style="list-style-type: none"> Decision systems shall establish <i>decision</i> authority and responsibility for lateral coordination decisions in 	3	0

		potential.	collision avoidance scenarios. Consider:		
			<ul style="list-style-type: none"> When not the decision authority, decision systems shall be responsible to engage in coordination and evaluate coordination for feasibility and acceptability (i.e. does not lead to hazards). 	1	0
0		7. ARA. Accountability.	<ul style="list-style-type: none"> Time constraints on developing a coordination strategy will be established, displayed, and monitored by decision systems. 	1	0
1	1	<ul style="list-style-type: none"> Time constraints are not established by decision systems for developing the maneuver strategy. 	<ul style="list-style-type: none"> The DAA shall alert UAS decision systems when time remaining to accomplish collision avoidance maneuvers is low. 	1	1
1	0	<ul style="list-style-type: none"> Time constraints may be established, but are not monitored or forgotten by decision systems when developing strategy. 	<ul style="list-style-type: none"> The DAA low time alert shall remain active until a maneuver is accomplished or manually acknowledged. 	1	1
2	0	8. Common Understanding.	<ul style="list-style-type: none"> Consider. Collision avoidance scenarios should use the same thresholds and severity alerts in training and in developing the DAA and CAS. 	1	0
2	2	9. Predictability.	<ul style="list-style-type: none"> The DAA shall include temporal factors such as: 	5	5

Table 48. Coding STPA-Coordination Vertical Coordination, Count Data

Scenarios		STPA-Coord: ATC Vertical Coordination	Recommendations and Considerations	Rec's	
66	15	Case 1. Coordination Missing.		77	35
UAS	DAA			UAS	DAA
0		1. Coordination Goals. n/a	n/a	0	
0		2. Coordination Strategy. Missing	<ul style="list-style-type: none"> When ATC coordination by control is missing, there shall be a replacement comprehensive coordination strategy. 	4	2
2	0	<ul style="list-style-type: none"> ATC near real-time vertical coordination is one of several coordination strategies in the NAS. 	<ul style="list-style-type: none"> If UAS is allowed to fly without ATC control, the UAS shall have self-observation capability at least commensurate with established visual requirement for in-situ pilots. 	1	0
			<ul style="list-style-type: none"> Consider. Automatic collision avoidance maneuvers should be required for aircraft that may fly without ATC coordination, such as military flight operations or flight operations in 	1	1

			Class G airspace.		
2	0	5. Group DM. Missing	<ul style="list-style-type: none"> Consider. Aircraft that fly where ATC services exist shall be under ATC control to assist in safe coordination efforts. 	1	0
Case 2. Coordination Inadequate.					
0		1. Coordination Goals.	<ul style="list-style-type: none"> FAA management and leadership shall ensure collision avoidance is a top priority goal. Training shall ensure human decision systems can meet the expected workload demand in off-nominal conditions, both ATC and aircrew. 	1	0
1	0	<ul style="list-style-type: none"> ATC familiarity with task and environment may foster a belief that they can push the traffic scenarios tighter 		1	0
1	0	<ul style="list-style-type: none"> External pressures on ATC to increase traffic flow beyond individual comfort levels. 			
1	0	<ul style="list-style-type: none"> UAS aircrew mission accomplishment goals may cause safety goal divergence. 			
0		2. Coordination Strategy.	<ul style="list-style-type: none"> ATC coordination by control shall be unambiguous when alternative coordination strategies exist. (within DS) To minimize control coordination ambiguity during a collision scenario, the UAS/DAA decision system shall provide ATC with the following as a minimum: 	2	0
2	0	<ul style="list-style-type: none"> In current regulations, coordination by control strategy can be ambiguous. 		1	1
2	0	3. Decision Systems. Inadequate ATC ability and potentially within DS ATC coordination may lead to UCAs.	<ul style="list-style-type: none"> ATC shall establish training certification programs for collision avoidance scenarios to include additional UAS/DAA concerns. Some concerns include: 	1	0
0		4. Communications	<ul style="list-style-type: none"> The UAS maneuver algorithms shall account for communication limitations and constraints between remote aircrew, UAS, and ATC to ensure uninterrupted communications. Power, non-interference, and reliability shall be confirmed adequate for communications. UAS decision systems shall be alerted in (near) real-time when vertical ATC coordination is interrupted. Consider. An alternative digital communication channel shall exist for ATC-UAS communications Vertical coordination shall account for communication time delays in collision avoidance maneuvers. 	1	1
4	0	<ul style="list-style-type: none"> Verbal communication channels may be interrupted and not allow information to pass between ATC and UAS decision systems 		1	1
1	0	<ul style="list-style-type: none"> Single voice communication channels may be in use during time needed to communicate with aircrew in an impending separation violation. 		1	0
1	0	<ul style="list-style-type: none"> Communication time delays between ATC and remote UAS aircrew may be inadequate for time-critical scenarios. 		1	0
				4	4

1	0	5. Group DM.	<ul style="list-style-type: none"> Consider. The use of digital means for vertical coordination during collision avoidance scenarios. 	3	2
		6. Observation of common objects. Observation of common objects may be inadequate, which may lead to UCAs.	<ul style="list-style-type: none"> ATC shall provide safety alerts that inform UAS aircrew on the bearing, range, and altitude of collision factor airborne objects. 	1	0
1	0	<ul style="list-style-type: none"> ATC may observe more objects than individual aircrew having primary and secondary radars. 	<ul style="list-style-type: none"> ATC shall continue to update aircrew on factor traffic until aircrew acknowledges visual. 	1	0
2	2	<ul style="list-style-type: none"> (within DS) DAA observe different objects than the aircrew and ATC. 	<ul style="list-style-type: none"> UAS aircrew shall acknowledge visual of airborne objects, or request another point out if there is a discrepancy. 	1	0
1	0	<ul style="list-style-type: none"> ATC observation update rates may be inadequate (not necessarily the physical equipment). 	<ul style="list-style-type: none"> UAS aircrew shall know DAA observation limitations against air and ground obstacles encountered during flight operations. 	1	0
			<ul style="list-style-type: none"> The DAA shall observe or have information on the same objects observed by other decision systems. 	3	3
			<ul style="list-style-type: none"> ATC shall have adequate observation update rates commensurate with proximity of UAS to other aircraft and active special use airspaces. 	1	0
0		7. ARA.	<ul style="list-style-type: none"> Given lateral coordination recommendations above in Table 26, accountability between ATC and aircrew shall be established: <ul style="list-style-type: none"> ATC-UAS accountability shall include strategy in use (i.e. vertical or lateral coordination) and planned maneuver to benefit predictability and common understanding of the scenario. Aircrew shall have methods to confirm the use of lateral coordination strategy with ATC. The DAA shall send accountability information to ATC. The DAA shall provide UAS aircrew with simple and error resistant means to confirm with ATC that lateral coordination strategy in use The DAA shall eliminate or mitigate spurious signals that may be interpreted as an alert by ATC Consider. Filter spurious DAA alert signals at the ATC receiving end if spurious DAA signals cannot be eliminated. ATC shall confirm receipt of accountability information from aircraft 	0	
3	1	<ul style="list-style-type: none"> When the DAA self-separation or collision avoidance maneuver response is complete, the UAS decision system may: 		1	0
1	1	<ul style="list-style-type: none"> (within DS) The DAA alerts and maneuver guidance may be displayed to ATC. 		1	0
1	1	<ul style="list-style-type: none"> (within DS) DAA guidance or alerts may be spurious. For example, ATC may receive DAA alerts that are not displayed to the correlated UAS aircrew. 		5	5
1	0	<ul style="list-style-type: none"> Aircrew do not relay to ATC alternative maneuver intentions in response to DAA guidance. 		1	1
1	0	<ul style="list-style-type: none"> Aircrew clearly and accurately state intentions to ATC that they are following DAA guidance 		1	1
2	2	<ul style="list-style-type: none"> (within DS) Accountability. Missing coordinability. The DAA is not coordinable by ATC vertical coordination strategy. 		1	0
				3	1

			decision systems.		
			<ul style="list-style-type: none"> The DAA shall be vertically coordinable by ATC control instruction. 	1	1
			<ul style="list-style-type: none"> Consider. CAS in general shall be vertically coordinable by ATC and vertical standardization. 	1	0
0		8. Common Understanding.	<ul style="list-style-type: none"> ATC shall emphasize separation or collision scenario in communications with UAS decision systems to assist common understanding of the situation severity. 	1	0
1	0	<ul style="list-style-type: none"> An otherwise safe ATC coordination instruction may not be followed by individual UAS decision systems. 	<ul style="list-style-type: none"> Consider. Communications shall be on one frequency for high density traffic operations to assist in communications 	1	0
1	0	<ul style="list-style-type: none"> Aircrew may delay or question ATC intentions when an impending separation violation or collision is not known or severity of situation is not obvious. 	<ul style="list-style-type: none"> Consider. Compatible information sharing technology shall be mandatory for aircraft in certain shared airspaces, 	1	1
1	0	<ul style="list-style-type: none"> Aircrew may unintentionally ignore instructions as they are not expecting them. 	<ul style="list-style-type: none"> The DAA shall alert UAS aircrew of degradation where information is uncertain. 	1	1
1	0	<ul style="list-style-type: none"> Aircrew can communicate with ATC on UHF and VHF frequencies, which is a common difference between civilian and military flight operations. 	<ul style="list-style-type: none"> The UAS decision system shall relay loss of DAA capability to ATC, like for other IFR equipment failures. 	1	0
1	0	<ul style="list-style-type: none"> ATC receives additional information than aircraft decision systems from its primary and secondary radars and other systems (e.g. ADS-B). 	<ul style="list-style-type: none"> Consider. DAA shall automatically relay failure or degradation to ATC 	1	1
1	1	<ul style="list-style-type: none"> (within DS) The DAA does not have the same information as ATC and does not perceive an impending separation violation at all. 			
1	1	<ul style="list-style-type: none"> (within DS) The DAA fails or degrades. 			
0		9. Predictability.	<ul style="list-style-type: none"> UAS decision systems shall provide ATC with maneuver intentions before and after a collision avoidance maneuver. Intentions may be provided by: 	3	1
4	1	<ul style="list-style-type: none"> ATC does not know if aircrew are responding to ATC control strategy or not, which hinders predictability when UAS aircrew are not following ATC. ATC may not be aware of the DAA alert because: 	<ul style="list-style-type: none"> Under lateral coordination, the DAA/CAS shall provide aircraft system state information to ATC for additional means to correlate aircraft in a collision scenario. 	1	1
1	1	<ul style="list-style-type: none"> ATC is aware of a DAA alert and correlated maneuvering aircraft, but maneuver guidance and cooperation information is not received by design or other factor. 	<ul style="list-style-type: none"> ATC shall receive DAA alerts for informational purposes and to improve coordination predictability. 	1	1

3	3	<ul style="list-style-type: none"> ATC is not aware of aircrew maneuver strategy. Even if ATC received UAS DAA alerts, the intention is not received. 	<ul style="list-style-type: none"> ATC shall be trained in expected UAS performance characteristics that affect maneuver response. 	1	0
1	0	<ul style="list-style-type: none"> ATC does not have appropriate UAS performance models to predict response to maneuver instructions. 	<ul style="list-style-type: none"> Consider. Maneuver category (e.g. high, medium, low) information shall be available for ATC to assimilate in developing coordination maneuver strategy. 	3	1
		Case 3. Coordination Leads to Hazard.			
0		1. Coordination Goals.	n/a		
0		2. Coordination Strategy.	<ul style="list-style-type: none"> Consider. A priority matrix for collision avoidance maneuver strategy shall be used. 	1	0
2	0	<ul style="list-style-type: none"> Infeasible: ATC gives instructions that is not feasible given constraints. 	<ul style="list-style-type: none"> Consider. ATC shall have collision avoidance automation similar to DAA/CAS to assist in time-critical situations. 	1	0
6	1	<ul style="list-style-type: none"> Unacceptable: ATC gives instruction that is followed leading to an unsafe outcome. 	<ul style="list-style-type: none"> The UAS and aircraft decision systems shall revert to comprehensive lateral coordination should vertical coordination not work 	1	0
			<ul style="list-style-type: none"> ATC shall have terrain information as an input to developing a coordination maneuver strategy. 	1	0
			<ul style="list-style-type: none"> The DAA/CAS shall alert UAS aircrew for potential terrain concerns. 	1	1
			<ul style="list-style-type: none"> If the DAA is coordinable by ATC, the DAA shall evaluate airborne objects and terrain in the maneuver strategy 	1	1
		Case 4. Coordination Late.			
		1. Coordination Goals. n/a.			
5	0	2. Coordination Strategy.	<ul style="list-style-type: none"> The UAS decision system shall know when ATC coordination can no longer influence 	2	2
1	0	3. Decision Systems.	<ul style="list-style-type: none"> ATC workload shall have adequate safety margin to account for off-nominal conditions 	1	0
1	0	4. Communications.	<ul style="list-style-type: none"> In vertical coordination, communication delays shall be accounted for in determining when ATC must begin coordination 	1	0
1	0	5. Group DM.	<ul style="list-style-type: none"> In a collision avoidance scenario, ATC shall be directive in coordination. 	1	0
0		6. Observations of common objects. n/a	n/a		
1	0	7. ARA.	<ul style="list-style-type: none"> ATC shall be alerted with increasing severity based on time remaining to having no influence. 	1	0
1	0	8. Common Understanding.	<ul style="list-style-type: none"> ATC and aircraft decision systems shall have common understanding of time remaining for engaging in and following ATC coordination 	1	0

			instructions.		
1	0	9. Predictability.	<ul style="list-style-type: none"> • A decision threshold metric shall be established for ATC to develop a separation/collision • ATC shall be given information on the time remaining for coordination strategy development. 	1	0
				1	0

APPENDIX D. Coding of and Comparison with DO-344 FHA and Requirements Analysis

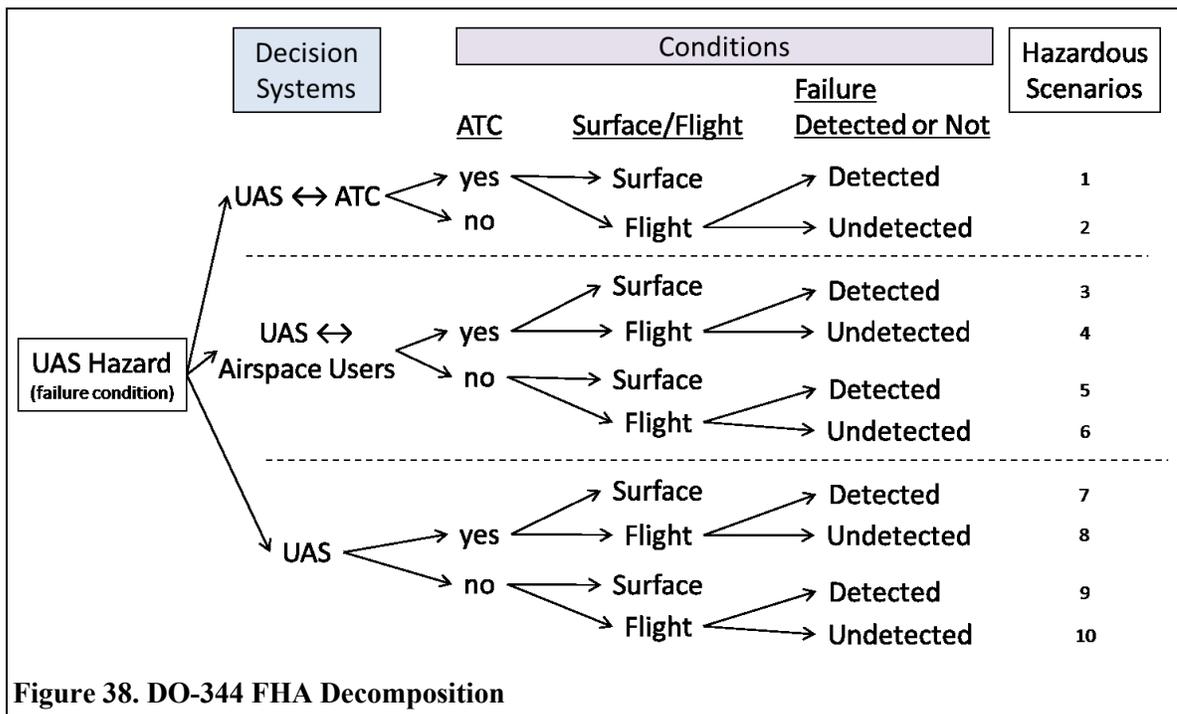
According to the Terms of Reference, Special Committee (SC)-203 was charged with developing the MASPS (Minimum Aviation System Performance Standards) for UAS in NAS operations in classes A, G and E (RTCA SC-203 2010). Safety analysis was part of the SC-203 effort and primarily consisted of developing and documenting a Functional Hazard Analysis. The FHA scope and UAS problem formulation are an ideal match for comparison against STPA-Coordination results.

A comparison of STPA-Coordination results to the SC-203 FHA documented in DO-344 Volumes 1 and 2 (RTCA SC-203 2013a; RTCA SC-203 2013b) was accomplished. Appendix I of DO-344 Volume 2 included the full FHA with tables spanning over 250 pages. The FHA considered four basic “functions”: 1) avoid hazard function, 2) communication function, 3) navigation function, and 4) control function. The FHA considered 42 UAS failures (including errors) as hazards; each hazard consisted of 30 potential hazardous scenarios from combining the following factors:

- Decision system interactions: hazard with UAS and ATC relationship, UAS and other airspace user relationship, or UAS only.
- Environment: hazard with ATC or not.
- Environment: hazard in surface operations, terminal air operations, or enroute navigation.
- Environment: hazard detected or not.

Related to flight environmental conditions, there were approximately 840 potentially hazardous scenarios (42 hazards, each with 20 conditions) considered by the FHA. The following steps were used to code the FHA data for comparison against the STPA-Coordination results:

- Create hazardous scenario categories for each UAS hazard per the following Figure 38:



- The *Flight* condition category combines the FHA “terminal” and “enroute” flight categories. Many of the hazard scenario descriptions were cut and paste. Where it was not a direct cut-and-paste, the descriptions were deemed not sufficiently different to warrant a separate category for comparison to STPA-Coordination.
- The UAS↔ATC relationship, non-ATC environment was not considered in the comparison and was mostly deemed not applicable in the FHA. Note that quantitative descriptions of the FHA in this thesis do not include the UAS↔ATC / non-ATC scenarios.
- As shown in Figure 38, the coding resulted in up to 10 potential unique scenarios for each FHA UAS hazard; although, most UAS hazards had less than 10 unique scenarios.
- For each FHA hazard, determine if it relates to one of the nine coordination elements introduced in the coordination framework.
 - Coded the hazard to the applicable coordination element and qualitatively compare to STPA-Coordination.
 - UAS hazards that are individual UAS concerns were not compared, including UAS control and feedback hazards (4.1.2, 4.2.1, 4.2.2, 4.4.1, 4.4.2). These are hazards that could be addressed by STPA causal analysis of the control loop relationships.
 - UAS hazards related to hazardous weather environments and cloud clearances were not compared because these are more individual concerns than hazardous coordination (1.2.2, 1.3.1, 1.3.2, 1.4.1, 1.4.2, 1.6.2).
 - Hazards related to ancillary flight plan services and other UAS support personnel (2.5.1, 2.6.1) are out of scope and were not compared.
 - Hazards related to UAS ability to keep time (e.g. time of day) were not compared as the concern was more directed at the individual UAS (3.4.1, 3.4.2).

The results from coding the FHA for coordination are presented in Table 49. Each hazard was assigned a coordination element most applicable and a description of the comparison given. In the table, the FHA ID and hazard description were taken from DO-344 Volume 2, Appendix I (RTCA SC-203 2013b) unless otherwise cited as Volume 1 (RTCA SC-203 2013a). The comparison column shows comparison analysis to the FHA in Volume 2, unless otherwise cited as Volume 1.

Table 49. FHA Coding and Comparison Results

FHA ID (DO-344 Vol 2)	Hazard Description Note. Labels from DO-344 Vol 2 (2013), Appendix I	Coord Elem	Coordination Description	Comparison
--------------------------	---	------------	--------------------------	------------

1	Avoid Hazards Function		"The Avoid Hazards function refers to any action taken to keep safely away from direct hazards posed by moving and stationary objects (e.g., aircraft, terrain, structure, severe weather, etc.) and inherent hazards of entry in unauthorized surface areas or	
----------	-------------------------------	--	---	--

			airspace" (p. 40 vol 1)	
1.1.1	Loss of ability to sense and avoid traffic	6	UAS decision system cannot observe common objects	<p>FHA:</p> <ul style="list-style-type: none"> -NSE (ATC, ATC env) "If undetected, ATC would take no action, having no affect on their operation" (p. I-2). -NSE (Airspace user, non-ATC env) "If detected, the UA pilot would work to maneuver the aircraft away from last known position of proximate traffic...having no effect on airspace users as they would have no awareness of the UA" (p. I-5). <p>STPA-Coordination:</p> <ul style="list-style-type: none"> -Vertical Coordination. Without knowing the UAS DAA inoperative, they may miss an opportunity to correct a collision scenario believing the UAS has the DAA. -Lateral Coordination. In a collision scenario, aircraft decision systems cannot observe each other, which is a significant safety concern for coordination and collision avoidance contrary to the FHA.
1.1.2	Erroneous sensory or self-separation/collision avoidance information or execution	8	Within DS concern for common understanding	<p>FHA.</p> <ul style="list-style-type: none"> -"Worst Credible Error: Misleading information directs UA into conflict with other aircraft" (p. I-8). -Misleading is vague in this hazard. -It is also a higher abstraction hazard than provided in the Navigation function hazards (ID 3x)--3.1.2, 3.2.2, 3.3.2. <p>STPA-Coordination: Similar concerns in both FHA and STPA-Coordination</p>
1.2.1	Loss of ability to provide clearance from structures, obstacles and terrain	6	UAS decision system cannot observe terrain and ground objects	<p>FHA:</p> <ul style="list-style-type: none"> -NSE (ATC, ATC env, undetected) "If undetected, no action would be taken by ATC" (p. I-14). -NSE (Airspace user, ATC env, undetected) "If undetected, would have no consequence to proximate aircraft"

				(p. I-16). STPA-Coordination: -Vertical Coordination (Case 3). May impact ability to evaluate ATC coordination instruction and renegotiate. -Lateral Coordination. May impact DAA/CAS cooperation in developing acceptable maneuvers.
1.2.2	Erroneous execution of clearance from structures, obstacles, and terrain	n/a	n/a. This is an individual UAS concern	n/a
1.3.1	Loss of ability to maintain cloud clearance minimums	n/a	n/a. This may influence individual see-and-avoid reaction times when coordination does not exist.	STPA-Coordination. Clouds may limit the DAA ability to observe, not a clearance from a cloud.
1.3.2	Erroneous cloud clearance information	n/a	n/a. With DAA, UAS would avoid clouds if necessary.	
1.4.1	Loss of ability to remain safely clear of atmospheric or meteorological hazards	n/a	n/a. This is an individual UAS concern.	
1.4.2	Erroneous information on hazardous atmospheric or meteorological conditions	n/a	n/a. This is an individual UAS concern.	
1.5.1	Loss of ability to remain clear of unauthorized airspace	6	The coordination concern is observation of interdependent aircraft decision systems when not expected, whether a special use airspace or unauthorized entry into Class A, B, C airspace for examples.	FHA: -NSE (ATC, ATC env, undetected) "If undetected, ATC would take no action" (p. I-50). -"If undetected by the UAS, military pilots or the restricted airspace controlling agency, the UA could inadvertently enter into restricted airspace and, once the UA pilot is alerted by the sense and avoid system, begin avoidance maneuvers. However, due to high closure speeds ... and

				<p>unawareness of the military pilots, a near midair collision may result” (p. I-53). Good coordination discussion, but the unauthorized airspace and closure speed concerns are perhaps misplaced.</p> <p>STPA-Coordination -VERTICAL Coordination. If ATC does not detect flight path deviations, this may lead to unsafe coordination contrary to FHA NSE rating. -Lateral Coordination. Aircraft in authorized airspace not expecting UAS and may not observe them. The FHA attributing inadvertent entry or closure speeds are themselves not the safety concern. Protected airspace may be the safest place to fly if not in use! Closure speeds are inherent property of a collision.</p>
1.5.2	Erroneous information concerning the ability to remain clear of unauthorized airspace	8	With uncertainty or errors in observed state or in DAA calculations, common understanding between decision systems is affected	<p>FHA: -"Worst credible error: Misleading position or altitude data places UA in unauthorized airspace" (p. I-56).</p>
1.6.1	Loss of ability to maintain minimum visibility conditions	6	The visibility conditions needed to observe airborne obstacles are important for coordination	<p>FHA: NSE (Airspace user, non-ATC env, detected) "If detected, the pilot would return to known VMC conditions and land as soon as practicable, having no effect on other airspace users" (p. I-65).</p> <p>STPA-Coordination -Lateral Coordination. If detected does not solve the loss of visibility needed to observe another airborne obstacle, which is a hazardous coordination scenario.</p>
1.6.2	Erroneous Reporting of minimum visibility conditions	n/a	n/a	Not addressed in FHA

2	Communicate Functions		"The communicate function refers to voice and data exchanges among the UAS pilot, ATC and proximate traffic to communicate intent, instructions, and responses. ...Also...among UAS personnel" (p. 44 vol 1)
2.1.1	Loss of external communication with ATC	4	<p>Vertical coordination communications</p> <p>FHA: -NSE (ATC, ATC env, undetected) "If undetected, the controller would take no action, having no effect on normal procedures or workload" (p. I-74). -NSE (Airspace user, ATC, undetected) "If undetected, pilots in the terminal areas would maintain routine operations" (p. I-76)</p> <p>STPA-Coordination. This hazard may occur from many reasons and in worst case conditions could lead to a loss of separation, regardless of likelihood. ATC may not know there is a loss until when the communications are needed.</p>
2.1.2	Misleading external communications between UA pilot(s) and ATC	n/a	Not addressed in FHA
2.2.1	Loss of external communications between UAS pilot and proximate traffic	4	<p>Lateral coordination communications</p> <p>FHA. -assessed as NSE or MIN in all cases, with "... negligible effect on safety" (p. I-90) and "... a slight loss of situational awareness" (p. I-89) -In this section, the FHA acknowledged the "RTCA Issue Paper 'UAS control and communications architectures' recommends that partyline comms are not needed except at non-towered airfields" (p. I-86)</p> <p>STPA-Coordination. -In nearly complete contrast with the FHA severity assessment, lateral coordination is dependent upon UAS-Proximate Aircraft communications, both verbal and digital means. Without communication, real-time coordination is difficult to impossible.</p>

				-partyline comms are applicable to coordination element Group DM, but is deemed not needed
2.2.2	Misleading external verbal communications between UAS pilot and proximate traffic	n/a		Not addressed in FHA
2.3.1	Loss of external data communications from UA to ATC	8	Loss of state information (position, altitude)	similar
2.3.2	Misleading external data from UA to ATC	8	Degradation of state information (position, altitude)	similar
2.4.1	Loss of external data from UA to proximate traffic	8	Loss of state information (position, altitude)	FHA: NSE (Airspace user, non-ATC env, undetected) "...pilots not made aware that their aircraft no longer has TCAS protection from UA would have no effect on pilots as they would maintain routine operations" (p. I-113).
2.4.2	Misleading data from UA to proximate traffic	8	Degradation of state information (position, altitude)	FHA: "Worst credible error: Erroneous advisory information sent to conflicting aircraft" (p. I-116).
2.5.1	Loss of external communications with ancillary services	n/a		Out of scope for case study
2.5.2	Erroneous external communications with ancillary services	n/a		Not addressed in FHA
2.6.1	Loss of internal communications among UAS crew and personnel	n/a		Out of scope for case study

2.6.2	Erroneous provision of internal communications among UAS crew and personnel	n/a		Not addressed in FHA
3	Navigation Functions		"The Navigate Function addresses the ability to obtain and maintain knowledge of the ownship current positional and geographic orientation information and of its destinations(s) using reference cues (electronic or visual)" (p. 44 vol 1)	
3.1.1	Loss of UA altitude information	8	Detailed state information	<p>FHA:</p> <ul style="list-style-type: none"> -More detailed abstraction of 2.3.1, 2.4.1. -NSE (ATC, ATC env, undetected) "...ATC would be unaware of altitude error and therefore no action would be taken by ATC" (p. I-146). -NSE (Airspace user, non-ATC env, detected) "If detected, the UA pilot would remain clear of traffic based on last know[n] information and land as soon as practical at a suitable location, having no effect on airspace users" (p. I-149) [<i>sic</i> know]. <p>STPA-Coordination: Both FHA NSEs are coordination safety concerns.</p>
3.1.2	Erroneous UA altitude information	8	Detailed state information	<p>FHA:</p> <ul style="list-style-type: none"> -More detailed abstraction of 2.3.2, 2.4.2. -NSE x2. NSE (ATC, ATC env, undetected), NSE (Airspace user, non-ATC env, detected). <p>STPA-Coordination: Both FHA NSEs are coordination safety concerns.</p>
3.2.1	Loss of UA heading and course information	8	Detailed state information	FHA: More detailed abstraction of 2.3.1, 2.4.1.
3.2.2	Erroneous UA heading/course information	8	Detailed state information	FHA: More detailed abstraction of 2.3.2, 2.4.2.

3.3.1	Loss of UA ground position information	8	Detailed state information	<p>FHA:</p> <ul style="list-style-type: none"> -More detailed abstraction of 2.3.1, 2.4.1. -NSE (Airspace user, non-ATC env, detected) "...pilots in the area would maintain routine see and avoid operations,, but may be more vigilant" [sic ,,] (p. I-173). -NSE (Airspace user, non-ATC env, undetected) "...pilots in the area would maintain routine see and avoid operations" (p. I-173). <p>STPA-Coordination.</p>
3.3.2	Erroneous UA ground position information	8	Detailed state information	<p>FHA: More detailed abstraction of 2.3.2, 2.4.2</p>
3.4.1	Loss of temporal data to UAS	n/a	n/a	<p>"Pilots use time for planning purposes but are not reliant on time for safe operation in non-ATC environments" (p. I-183).</p> <p>The FHA hazard was concerned with the individual UAS ability to have a time signal or to keep time, specifically time of day.</p> <p>STPA-Coordination: Time is a primary concern for separation and collision avoidance coordination. But the relevant time is time relative to the another object.</p>
3.4.2	Erroneous temporal data to UAS	n/a	n/a	<p>This hazard again was about ability to keep time or have a correct time signal (i.e. time of day). The FHA hazard was not about time to any given hazard such as collision. Ability to report a fix on time was the example used.</p>
3.5.1	Loss of UA trajectory definition	9	Predictability of UAS system state may be unknown	<p>FHA: This hazard is loss of control of UAS.</p>
3.5.2	Erroneous UA trajectory definition	9	Predictability of UAS system state may be unknown	

4	Control Functions		"The flight control function refers to the power or means of directing, regulating or restraining aircraft movement. Non-flight control functions refer items such as setting transponder codes, radio frequencies, deploying landing gear and making queries or initiating tests on UAS systems" (p. 46 vol 1)
4.1.1	Loss of command of UA flight control	8	Coordination requires common understanding of decision system maneuver limitations
4.1.2	Erroneous command or execution of flight path	n/a	n/a
4.2.1	Loss of feedback from UA flight controls	n/a	n/a
4.2.2	Erroneous UA flight control feedback	n/a	n/a
4.3.1	Loss of UA Non-Flight Control Command	8	If not known, this could cause common understanding problems for coordination
4.3.2	Erroneous Command of Non-Flight Controls	8	Comm and DAA modes errors

STPA-Coordination. Vertical, Lateral. This condition needs to be known by decision systems.

STPA-Coordination: The hazard is out of scope. Erroneous UAS control is part of STPA step 2 and answers the question why was safe coordination not followed?

FHA: redundant with "undetected" in hazard 4.1.1., 4.1.2.

STPA-Coordination. The hazard deals with UAS control actions and is out of scope. Loss of UAS control feedback is part of STPA step 2.

STPA-Coordination. The hazard deals with UAS control actions and is out of scope. Loss of UAS control feedback is part of STPA step 2.

FHA:
 -NSE (UAS, (non)ATC env, (un)Detect) "There is no known non-control telecommand that would adversely affect safety of the UAS flight system" (p. I-235).
 -NSE (Airspace user, non-ATC env, undetected) "No effect on airspace users" (p. I-233).

STPA-Coordination: Aircraft decision systems must account for configuration.

FHA:
 -Worst credible errors: landing gear position, altimeter setting.

STPA-Coordination: Aircraft decision systems may error in mode selection or configuration selection.

4.4.1	Loss of feedback from UA non-flight controls and data	n/a	n/a	FHA: redundant with "undetected" in hazard 4.3.1., 4.3.2.
4.4.2	Erroneous feedback of non-flight control data	n/a	n/a	FHA: redundant with "undetected" in hazard 4.3.1., 4.3.2.

Table 50 summarizes the FHA frequency analysis of unique hazardous scenarios related to coordination and with similar scope to the STPA-Coordination analysis. The first column labels the hazard identification numbers used in the FHA and link to the descriptions given in Table 49. The following coding scheme was used:

- NSE: FHA classified hazardous scenarios as No Safety Effect (not included in hazard count).
- MIN: FHA classified hazardous scenarios as Minimal severity risk (not included in hazard count).
- 1: Unique hazard count with assessed risk greater than MIN.
- 0: A non-ATC hazard that was not unique from the ATC hazard, rather a (near) duplicate of the ATC environment hazardous scenario.
- Shaded red and bright red identified where the FHA assessed NSE, but were in part related to hazardous coordination scenarios.
- (RTCA SC-203 2013a) determined: “Hazards having a MINIMAL safety effect are deemed to have a low enough risk so as not to require a safety objective” (p. 76). Thus, in addition to Minimal risk scenarios, scenarios assessed as No Safety Effect (NSE) were not counted in the comparison. For each UAS hazard scenario deemed higher risk than MIN (i.e. in increasing order, Minor, Major, Hazardous, and Catastrophic):
 - Counted each unique UAS-ATC hazardous scenario.
 - Counted each unique UAS-Airspace user hazardous scenario.
 - The UAS only branch of the FHA hazardous scenarios (i.e. the bottom branch of Figure 38) was not counted because: 1) if coordination was part of the scenarios, it was deemed redundant with the UAS-Airspace user scenarios (previous bullet), or 2) the UAS only scenarios were not concerned with coordination-related scenarios such as equipment failure leading to controlled flight into terrain (this would be handled by current STPA).

Referencing Table 50, the frequency analysis included FHA scenarios in columns labeled “UAS↔ATC” and “UAS↔Airspace user” that were coded “1” without any other identifier.

Table 50. FHA Frequency Analysis of Coordination Hazards

FH A ID	UAS↔ATC (flight)		UAS↔Airspace user (flight)				UAS only (flight)				SUM: Unique Scenarios	SUM: Coord Scenarios
	ATC		ATC		Non ATC		ATC		Non ATC			
	Detect	Undetected	Detect	Undetected	Detect	Undetected	Detect	Undetected	Detect	Undetected		

	Sum	17	Sum	31			Sum	43			91	48
1												
1.1.1	MIN	NSE	1	1	1	0	1	1	0	0	5	3
1.1.2	MIN	1	1	1	1	0	1	1	0	0	6	4
1.2.1	MIN	NSE	NSE	NSE	NSE,0	NSE,0	1	1	0	0	2	0
1.2.2											0	0
1.3.1											0	0
1.3.2											0	0
1.4.1											0	0
1.4.2											0	0
1.5.1	MIN	NSE	MIN	1	MIN,1	0	1	1	1	1	5	1
1.5.2	MIN	NSE	MIN	1	MIN,0	0	1	1	1	0	4	1
1.6.1	MIN	NSE	1	1	NSE	1	1	1	0	0	5	3
1.6.2											0	0
2												0
2.1.1	1	NSE	MIN	NSE	NSE(n/a)	NSE,1(n/a)	MIN	NSE	NSE(n/a)	NSE,1(n/a)	1	1
2.1.2											0	0
2.2.1	NSE	NSE	MIN	MIN	MIN,1	MIN,1	MIN	MIN	MIN,0	MIN,0	0	0
2.2.2											0	0
2.3.1	MIN	1	MIN	1	NSE	NSE	MIN	1	NSE	NSE	3	2
2.3.2	MIN	1	MIN	1	MIN,1	1	1	1	1	0	6	3
2.4.1	NSE	NSE	MIN	NSE	MIN,1	NSE,1	MIN	1	MIN,0	0	1	0
2.4.2	NSE	NSE	MIN	NSE	MIN,1	NSE,0	MIN	1	MIN,0	0	1	0

2.5.											0	0
1												
2.5.											0	0
2												
2.6.											0	0
1												
2.6.											0	0
2												
3											0	0
3.1.	1	NSE	MIN	1	1	0	1	1	1	1	7	3
1												
3.1.	1	NSE	MIN	1	1	0	1	1	0	0	5	3
2												
3.2.	MIN	1	MIN	1	MIN, 1	1	1	1	0	0	5	3
1												
3.2.	MIN	1	MIN	1	MIN, 1	1	MIN	1	MIN, 0	0	4	3
2												
3.3.	MIN	NSE	MIN	NSE	NSE	NSE,0	1	1	1	0	3	0
1												
3.3.	MIN	1	MIN	1	MIN, 1	0	1	1	1	1	6	2
2												
3.4.											0	0
1												
3.4.											0	0
2												
3.5.	1	1	1	1	1	0	1	1	0	0	7	5
1												
3.5.	1	1	1	1	1	0	1	1	0	0	7	5
2												
4											0	0
4.1.	1	1	MIN	NSE	1	1	1	1	0	0	6	4
1												
4.1.											0	0
2												
4.2.											0	0
1												
4.2.											0	0
2												
4.3.	MIN	1	MIN	MIN	MIN, 1	MIN, 0	NSE	NSE	NSE, 0	NSE,0	1	1
1												
4.3.	MIN	1	MIN	MIN	MIN, 1	MIN, 0	NSE	NSE	NSE, 0	NSE,0	1	1
2												
4.4.											0	0

				0011 redundant scan	redundant
3.3.3	Provide Clearance from Clouds	1	0	n/a	n/a
3.3.4	Provide Clearance from Atmospheric or Meteorological Hazards	6	0	n/a	n/a
3.3.5	Provide Clearance from Unauthorized Airspace	1	1	FR-UNA-0001 have ability	6
3.3.6	Provide Clearance from Below-Minimum Visibility	1	0	n/a	n/a
3.4.1	Provide External Verbal Communications Between UAS Crew and ATC	2	1	send/receive	4
3.4.2	Provide External Verbal Communications Between UAS Pilot(s) and Pilots of Proximate Traffic	2	1	send/receive	4
3.4.3	Provide External Non-Verbal Communications from UAseg to ATC	1	1	send only	8
3.4.4	Provide External Non-Verbal Communications between UAseg and Proximate Traffic	2	1	send/receive	8
3.4.5	Provide External Communications with Ancillary Services	5	0	send/receive	n/a
3.4.6	Provide Internal Communications Among UAS Crew and Personnel	8	0	n/a	n/a
3.5	(not verbatim) support ground maneuver	1	0	n/a	n/a
3.5.1	Estimate Position and Orientation Information	4	3	FR-NAV-0002 receive state information 0003 support ATC surveillance 0004 calculate speed	8 8 2
3.5.2	Define Path(s)	5	3	FR-NAV-0006: compute the path 0009 provide intent information 0010 handle path	9 9 2

				deviations	
3.5.3	Steer along Path	4	0	individual UAS requirements	n/a
3.5.4	Navigation function inputs Note. Avoid airspace is 3.3.5, ability to navigate may not be directly related to collision coordination maneuvers.	10	1	FR-NAV-0019 support other UAS functions	8
3.6.1	Provide Command of UA Flight Controls	7	1	FR-CTR-0002 & 0003 send/receive information	8
3.6.2	Provide Feedback from UA Flight Controls	8	2	FR-CTR-0009 & 0010 feedback 0011 mode feedback / displays 0015 SA on mode changes (redundant with 0011)	8 8 redundant
3.6.3	Provide Command of UA non-Flight Controls	4	0		n/a
3.6.4	Provide Feedback from UA non-Flight Controls	4	1	FR-CTR-0021 & 0022 send/receive info	8
3.6.5	Monitor Health	2	1	FR-HLT-0001 report status to UA pilot	8
3.7	Flight planning (see ID 8, Appendix C, Volume 1)				n/a
8	(not verbatim) Flight plan--prep, build, process, file	14	4	FR-NAV-0034 UAS performance data	8
				0035 datalink performance data	2
				0036 terrain & ground obstacle data	2
				0038 lost link IAW regs	9

Vol 1,
Appx
C

APPENDIX E. CAST-Coordination Case Study Background

Appendix D discusses the development of the safety control structure for the Patriot friendly fire case study. The safety control structure was a representation of the systems involved in the incident. The information background represented in the control structure served to frame the incident problem and guide the abstraction levels used for CAST-Coordination.

E1. Literature Review, Joint Military Operations and Defensive Counterair

The Patriot friendly fire incident case study largely involved defensive counterair and airspace control joint operations systems. These systems directed the literature review to develop the safety control structure and inform CAST-Coordination. References consisted of archival records, Service doctrine, and Joint Doctrine in addition to the official accident investigation reports to include:

- Accident Investigations. There were two official government accident investigation reports on the US Patriot friendly fire shoot down of the British GR-4 Tornado aircraft.
 - United Kingdom Ministry of Defence Accident Report (United Kingdom Ministry of Defence 2004).
 - US Central Command Accident Report (US Central Command 2004). This report addressed the three Patriot incidents during the two-week period, to include the GR-4 shoot down.
- Joint Publications. The US Department of Defense Joint Publication (JP) series gives a detailed description of command and control relationships.
 - *Joint Publication 3-0. Joint Operations* (US Department of Defense Joint Staff 2011).
 - *Joint Publication 3-01. Countering Air and Missile Threats* (US Department of Defense Joint Staff 2012).
 - *Joint Publication 3-30. Command and Control of Joint Air Operations* (US Department of Defense Joint Staff 2014a).
 - *Joint Publication 3-31. Command and Control for Joint Land Operations* (US Department of Defense Joint Staff 2014b).
- Service Publications
 - ANNEX 3-01 COUNTERAIR OPERATIONS (US Air Force 2015)
 - *FM 3-01.85 (FM 44-85) Patriot Battalion and Battery Operations* (US Department of the Army 2002).
 - *ATP 3-01.7 Air Defense Artillery Brigade Techniques* (US Department of the Army 2016).
- General Information
 - Air and Missile Operation Defense: Iraqi Freedom (Anderson 2004).
 - *A System Theoretic Safety Analysis of Friendly Fire Prevention in Ground Based Missile Systems* (McCarthy 2013).
 - Report of the Defense Science Board Task Force on Patriot System Performance (Defense Science Board 2005).

E2. Joint Operations, Command and Control

Command relationships for Joint operations start with Combatant Command (COCOM) authority. This command authority is derived from Title 10 of the United State Code. Command authority cannot be delegated and is the authority over all aspects of operations, training, and logistics to accomplish the geographic or functional unified mission assigned to the command.

Operational control (OPCON) is the next lower level authority, usually delegated through COCOM. OPCON is authority to organize and employ forces, assign tasks, designate objectives and provide direction. Tactical control (TACON) is the next level authority and is inherent in OPCON and may be provided to other commanders. TACON is authority over assigned and attached forces for tactical maneuvering to accomplish a task. The support relationships are interactions among components and forces without a transfer of authority to the supported commander; forces may be directed to support while under the control of their functional command. Figure 39 summarizes and relates joint command relationships.

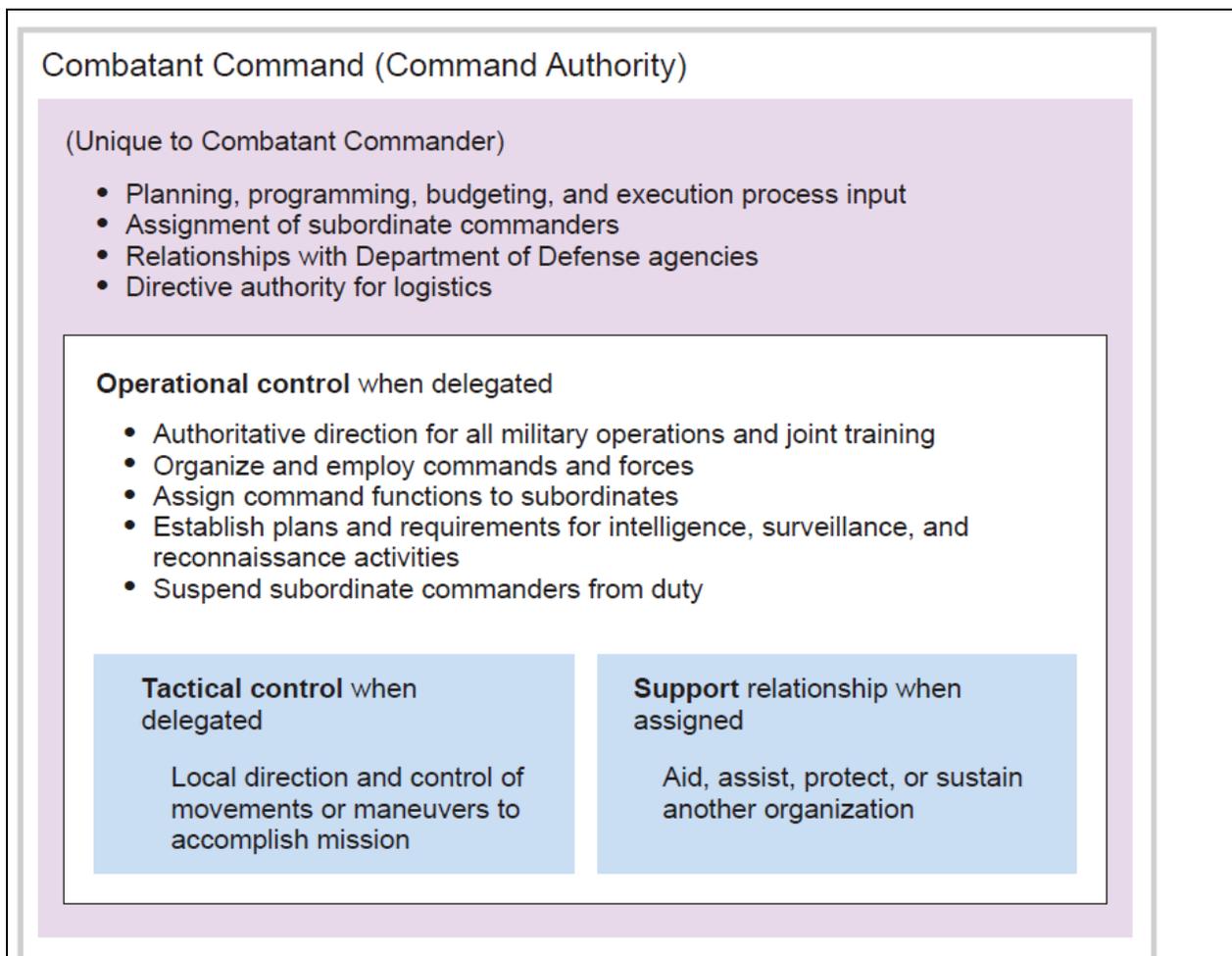


Figure 39. Joint Command Relationships

Reprinted from (US Department of Defense Joint Staff 2011), p. III-3. Figure in public domain.

E3. Defensive Counterair Systems

The sociotechnical system responsible for defensive counterair was one of the two important systems for this case study. According to the Joint Publications, the defensive counterair mission is to "...degrade, neutralize, or defeat enemy air and missile attacks attempting to penetrate friendly airspaces", which is part of the larger counterair mission "...to attain and maintain a desired degree of air superiority and protection by neutralizing or destroying enemy aircraft and missiles, both before and after launch" (US Department of Defense Joint Staff 2012) p. I-1.

Figure 40 shows the high level Joint Command structure through the air defense artillery battalions that assist in theater defensive counterair. At the top commanding the joint military operations was the Joint Force Commander (JFC). Under the JFC were component commanders: Joint Force Land Component Commander (JFLCC) and Joint Force Air Component Commander (JFACC). It should be noted that joint doctrine enables the JFC to establish command, coordination, and engagement control relationships as deemed necessary to successfully accomplish the mission. As such, the relationships are identified as general or typical to denote the joint publication standard.

The JFACC is generally made the AADC (Area Air Defense Commander) and ACA (Airspace Control Authority). In part, the AADC produces the AADP (Area Air Defense Plan) and the ACA produces the ACP (Airspace Control Plan). The joint plans (AADP and ACP) produce the coordination strategy required to safely integrate defensive counterair operations (e.g. Patriot) with the offensive air operations (e.g. aircrew). The defensive counterair engagement authority rested with the JFACC and typically through the AOC/CRC (air operations center/control and reporting center) where an Air Defense Commander would be located.

The Army Air and Missile Defense Command (AAMDC) plays an important role in the coordination of all Air and Missile Defense (AMD) assets for theater defensive counterair (DCA) efforts. Joint Doctrine states, "For DCA, the AAMDC is the senior Army air defender for both the theater Army commander/JFLCC (as the TAAMDCOORD) and the AADC (as the D[eputy] AADC)" (US Department of Defense Joint Staff 2012) p. II-22.

The AAMDC dual role under the Land and Air component commanders is highlighted by the dashed (orange) box in Figure 40. The Commander AAMDC is generally OPCON to the JFLCC, shown hierarchically below the JFLCC. The Commander AAMDC is usually in direct support to the JFACC defensive counterair effort providing AMD forces and integration expertise. The defensive counterair engagement line of command is shown with solid line from the JFACC/AADC, through the CRC, and down to the Patriot Battalions ("P" symbol). The actual defensive counter air engagement authority is delegated as required from the JFACC.

In addition to supporting the Component Commands, the AAMDC "commands all Army theater-level AMD forces" (US Department of Defense Joint Staff 2012) p. II-7. The AAMDC command is denoted in Figure 40 by the command symbol "++" and direct lines to the theater ADA forces. The Corps ADA Brigade coordinates to support the Army level Corps "XXX" forces (Woods 1990).

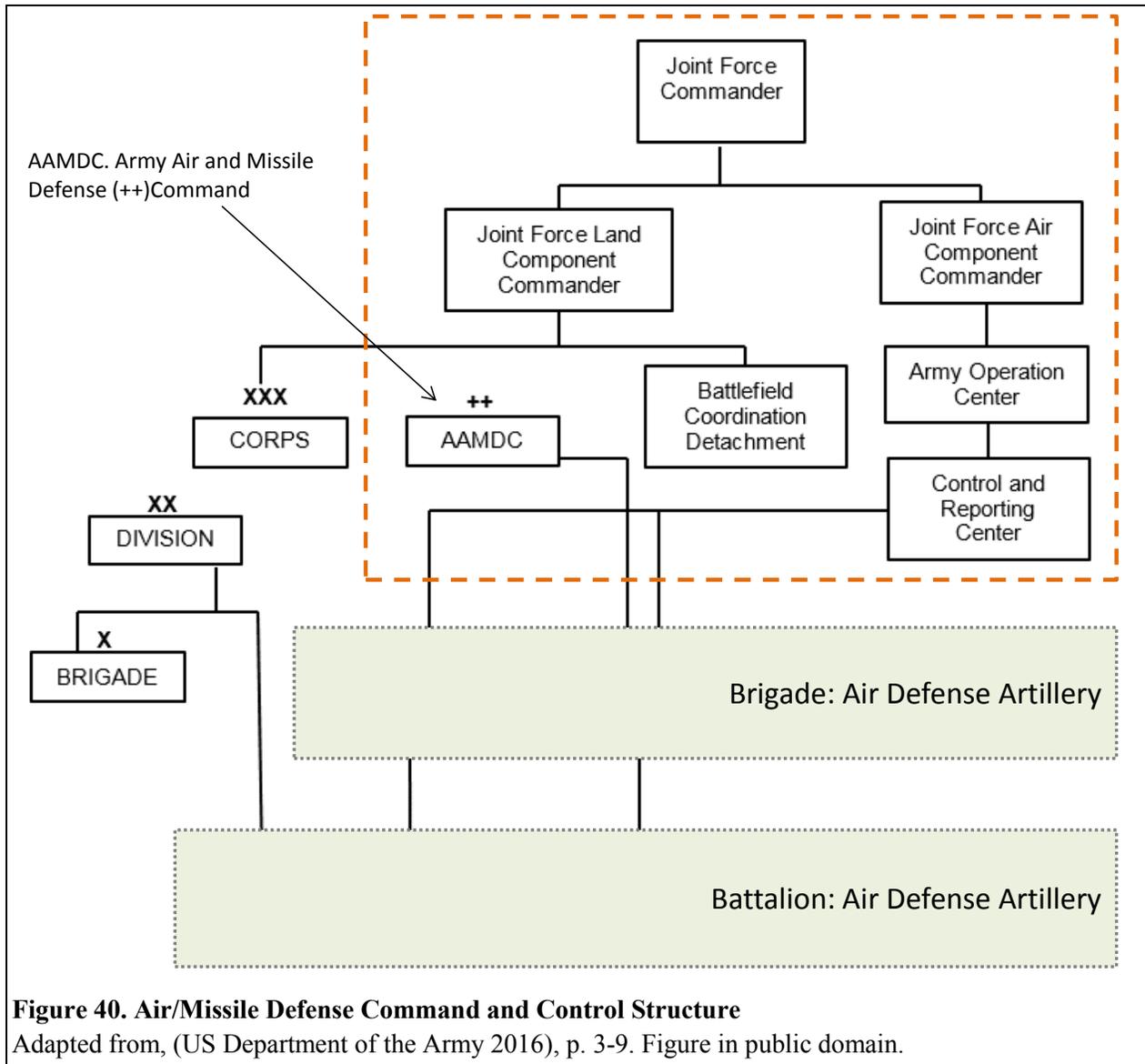


Figure 40. Air/Missile Defense Command and Control Structure

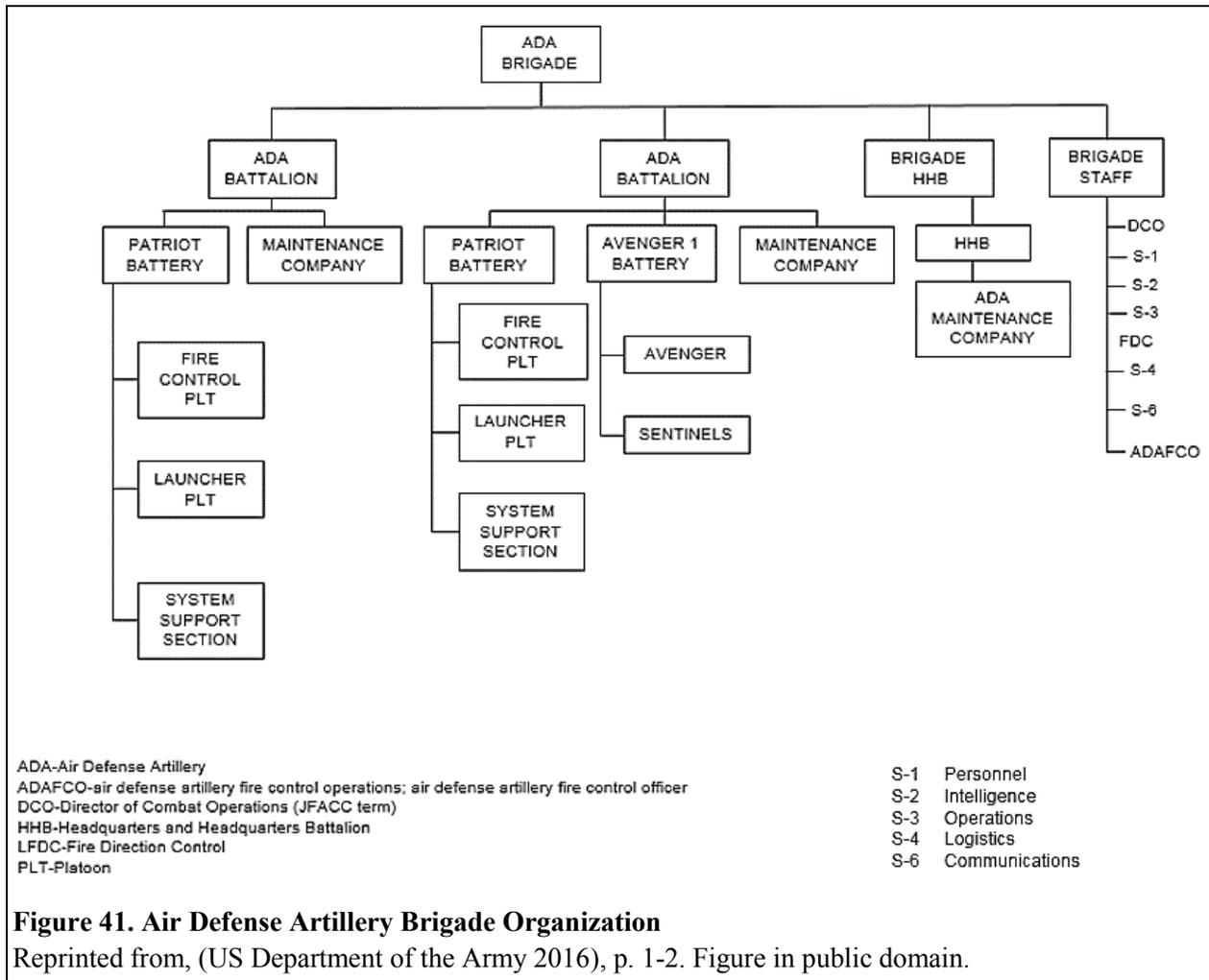
Adapted from, (US Department of the Army 2016), p. 3-9. Figure in public domain.

E4. ADA Brigade Organization

The ADA brigade "...is the focal point for solving technical and procedural integration and interoperability problems" and "...will coordinate with the AAMDC or the supported corps AMD planning cell" (US Department of the Army 2016) p. 1-1. Figure 41 shows a typical ADA Brigade control structure.

The ADA Brigade exercises control over ADA forces through the Fire Direction Center (FDC). Management by exception is generally used by the ADA Brigade FDC (US Department of the Army 2016). At the Patriot Battalion, another FDC controls the operations of the Patriot Batteries, also called fire units (FUs). Each FDC consists of a Tactical Director (TD) and Tactical Director Assistant (TDA) that monitor and make engagement decisions when they have engagement authority.

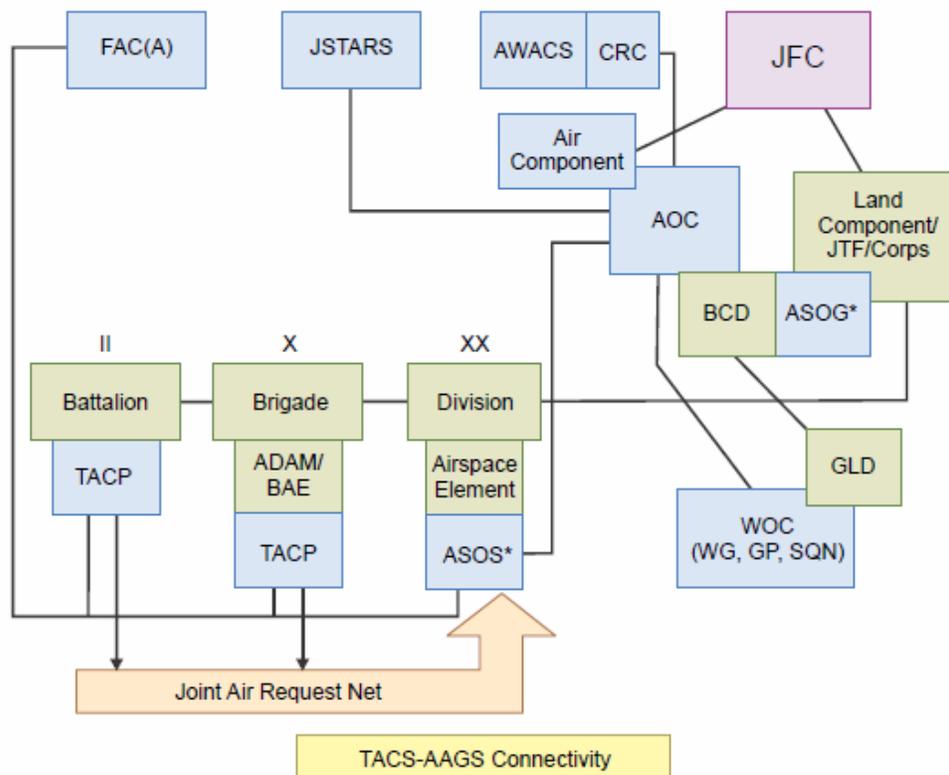
The Patriot Battery (or fire unit) is the next lower echelon from Brigade and is the “lowest tactical organizational unit” (US Department of the Army 2002) p. 6-6. There typically five to six Patriot Batteries assigned to a Battalion (US Department of the Army 2002). The Fire Control Platoon is the operational arm of the Patriot battery during sustained operations. The fire control platoon consists of a tactical control officer (TCO), tactical control assistant (TCA), and a network switch operator that work in an engagement control station (ECS). The Patriot Battery, Fire Control Platoon was the lowest decision system analyzed by CAST-Coordination in this case study.



E5. Airspace Control System

Airspace control system is the other system of significance for the case study. Figure 42 shows the command and control relationships decomposed by the JFACC and JFLCC control channels, color coded blue and green respectively. Aircrew and defensive counterair forces fall under control of the Joint Forces Air Component for airspace control.

Key Air Force and Army Components of the Theater Air Control System: Army Air-Ground System



*Exact make up and capabilities of the ASOG/ASOS tailored to match the mission assigned to the corps/division. The ASOC is normally collocated with the senior Army tactical echelon.

NOTE:
Coordination is effected between all organizations for effective/efficient operations.

Legend

AAGS	Army air-ground system	GLD	ground liaison detachment
ADAM	air defense airspace management	GP	group
AOC	air operations center	JFC	joint force commander
ASOC	air support operations center	JSTARS	Joint Surveillance Target Attack Radar System
ASOG	air support operations group	SQN	squadron
ASOS	air support operations squadron	TACP	tactical air control party
AWACS	airborne warning and control system	TACS	theater air control system
BAE	brigade aviation element	WG	wing
BCD	battlefield coordination detachment	WOC	wing operations center
CRC	control and reporting center		
FAC(A)	forward air controller (airborne)		
		—	command and control

Figure 42. Joint Air Force and Army Theater Air Control Systems

Reprinted from (US Department of Defense Joint Staff 2014a), p. II-10. Figure in public domain.

The Joint Air Operations Plan (JAOP) is the JFACC's high level integration and coordination document. When aircrew conduct theater operations to support the JAOP, they fall under the control of the Air Component/AOC and established regulations. Airspace control is guided by regulations found in the

Airspace Control Plan (ACP), Airspace Control Order (ACO), Area Air Defense Plan (AADP), Special Instructions (SPINS), and daily Air Tasking Orders (ATO), etc. For battle management and navigation, aircrew are controlled in (near) real-time by procedural or positive control often from AWACS/CRC and ATC. Aircrew will also fall under local control of their assigned Wing directing flight operations to and from an airfield.

The graphic also shows the fires and engagement control aircrew must follow when supporting the Joint Force Land Component Commander—ASOG, ASOS, TACP, FAC(A)—but this was out of scope for the case study.

E6. Case Study Foundations

CAST-Coordination is anchored in analysis of the coordination between the Patriot System and the friendly aircrew. To appreciate the benefits of a coordination perspective to accident investigation, it is important to highlight the Patriot Battery acted completely within authorized bounds, yet fratricide occurred. Among other influences, coordination was inadequate.

CAST-Coordination used the relationships represented in the safety control structure for evaluation and recommendations. The relationships were not detailed in the accident investigation reports, but rather had to be pieced together. Following are the relevant facts, logic chains, and supporting statements found in the literature that supported the chosen abstractions and relationships used for the safety control structure and CAST-Coordination.

E6.1 Control and Coordination Relationships

The Patriot Battery had engagement authority as claimed by the UK MOD report: the Patriot Battery "...had complied with extant self-defence Rules of Engagement for dealing with Anti-Radiation Missiles" (United Kingdom Ministry of Defence 2004) p. 2. Further, the Patriot Battery was also authorized to operate independently or "autonomously" with limited radio relay communications to Battalion Headquarters. USCENTCOM (2004) assessed that: "...employment of Charlie Battery, 5-52 ADA in an autonomous mode was operationally justified" (p. 10) and gave justification when "...the number and dispersal of key assets ... exceeds the capacity of the PATRIOT Battalions deployed" (p. 33).

Theater air defense engagement authority is generally not delegated below regional or sector air defense commander (RADC/SADC). However, it is not clear whether the Patriot Battery was under theater level air defense engagement control and authority. The Defense Science Board made a one line comment that the Patriots during OIF "...had no assigned air defense role, but it did have a self-defense role against anti-radiation missiles" (Defense Science Board 2005) p. 1. The word "assigned" is ambiguous. Current doctrine uses "support" for formal relationships not under a control relationships. Discussion of the actual Patriot *theater* air defense relationships could not be corroborated in the accident investigations reports. The implications are that if in formal support of theater level air defense efforts, the Patriots would fall under the theater air defense engagement authority which originated from the JFACC/AADC.

In addition to ambiguous engagement authority for Patriot operations, details of command and control relationships for air defense and airspace control were ambiguous in the accident investigation report. An organizational or C2 diagram was not to be found and a heavily redacted USCENTCOM report did not help, which was the more detailed of the two accident investigations. Understanding the USCENTCOM Freedom of Information Act released report (2004) required extensive working knowledge of joint military operations and acronyms which often implied command and coordination relationships.

The ambiguity in details of the actual engagement authority lines or C2 lines did not limit CAST-Coordination, however. It was not a limitation because CAST-Coordination evaluated theater level coordination that needed to exist between the Patriot systems and aircrew, regardless of the actual C2 relationships that allowed the Patriot to engage. Air defense coordination strategy and those involved in developing the strategy were acknowledged in the accident reports and literature, which was consistent with current Joint Publications (US Department of Defense Joint Staff 2012):

Regardless of the command relationship, all counterair forces are subject to the rules of engagement (ROE), airspace control, weapons control measures, and fire control orders established by the JFACC, AADC, and/or ACA as approved by the JFC (p. II-1).

E6.2 Safety Control Structure Development and Implications for CAST-Coordination

The developed safety control structure reflected knowledge of the air defense and airspace control systems derived from the literature and doctrine pre-dating the incident and current. The following excerpts supported the development of the safety control structure and analysis using CAST-Coordination:

- The MOD report claimed “The command and control arrangements were based on standard Allied and UK Joint Doctrine” (p. 1). Only a high level overview was provided to include: Joint Operations Commander, Air and Land Component Commanders, and liaison elements.
- The USCENTCOM accident report (2004) used the same terminology found in current Joint Doctrine that is pertinent to the accident and control structure.
 - AAMDC (Army Air and Missile Defense Command) and SADC (Sector Air Defense Commander) acronyms were used, which match Joint Publication 3-01 *Countering Air and Missile Threats* (2012) descriptions of air defense command and engagement authority.
 - AADP (Area Air Defense Plan) and ACM (Airspace Control Measures) for airspace control and coordination efforts, which are also standard coordination strategy documents in current Joint Publications.
- Colonel Anderson claimed “On the brink of war, the 32nd AAMDC brought experts from all the services to the deserts of Southwest Asia to draft the first joint Area Air Defense Plan (AADP), a plan that would integrate theater AMD in eight countries” (Anderson 2004) p. 44. This supports coordination efforts described in current Joint Doctrine in development of the AADP for theater level coordination strategy applicable to AMD forces.

- The USCENTCOM accident report (2003) stated “IAW [in accordance with] the AADP, U.S. Corps-level Patriot forces deployed forward to protect the maneuver forces and they were required to maintain connectivity with their Area Air Defense Engagement Authority (EA)” (p. 27). This supported the use of air defense engagement authority lines consistent with current Joint Doctrine, which authority delegated from the JFACC/AADC to the RADC (regional air defense commander).
- Army Field Manuals support the ADA control structure relationships from Brigade to Battery, published prior to and after the case study incident (US Department of the Army 2002; US Department of the Army 2016).

E6.3 CAST-Coordination Approach, Summary

In summary, the safety control structure was representative of typical command, coordination, and engagement authority relationships for Joint Operations relating to AMD and airspace control. The safety control structure was consistent with the doctrine before and after the incident. The model was deemed adequate for CAST-Coordination and the purposes of the case study to apply and evaluate the coordination framework and flawed coordination guidance.

CAST-Coordination evaluated the Patriot-Aircrew lateral coordination and the decision-making hierarchy coordination up to the Joint Component Commanders. Coordination relationships were analyzed at an abstraction commensurate with the accident investigation reports. Thus analysis results lead to recommendations on what coordination *should* be for the chosen abstractions, which is not limited by the details of what it actually was. The results are applicable to known coordination influences at the highest levels—the JFACC/AADC Area Defense Plan (AADP) and Air Control Plan (ACP)—for supporting coordination between the highest and lowest level, and to Patriot and aircrew coordination. The results are perhaps also applicable to today’s joint military coordination efforts to avoid air defense fratricide.

[Page intentionally left blank]

APPENDIX F. Coding Results, CAST-Coordination Case Study

This appendix provides the primary data for CAST-Coordination frequency and comparison analysis, and the coding analysis of USCENCTOM (2004) and UK MOD (2004) accident reports for comparison.

F1. Frequency Analysis of CAST-Coordination Results

Table 52 shows the CAST-Coordination data used for comparison analysis. Only unique accident influence (first column) and recommendation (last column) are counted and listed. Abstraction levels consistent with the accident investigations were used to identify and count unique influences and recommendations. The data in the tables combines CAST-Coordination results in Chapter 6.

Table 52. CAST-Coordination Frequency Analysis

Freq	Coordination Influence on the Incident	Coordination Recommendations	Freq
35	Patriot/Aircrew Flawed Coordination Influences	Patriot/Aircrew Lateral Coordination Recommendations	59
1	1. Coordination Goals	Patriot systems shall prioritize fratricide avoidance.	1
	2. Coordination Strategy (Case 2 inadequate)	· Coordination by standards alone shall be the exception and last resort when life is at stake and conditions are uncertain.	1
1	· When the stakes are life and death, standardization (safe passage routes) and component reliability (IFF working) coordination strategies were inadequate.	· Coordination methods that favor mutual adjustment are recommended given 1) a relatively low-intensity conflict	1
2	· The Patriot correctly identifying the aircraft by IFF means alone was inadequate:		
1	3. Decision Systems	· Evaluation methods shall be established to confirm Patriot crew capability to handle lethal decisions and coordinate	1
		· Certification levels shall be commensurate with increased responsibility up to autonomous Patriot operations.	1
1	4. Communications	· Recommend direct communication channels between the Patriot Battalion HQ and aircrew.	1
		· In more routine cases or when Battalion HQ does not have the workload bandwidth for direct communication with aircrew	1
		· If the workload may be too high for aircrew, then assign a communication node to facilitate real-time coordination efforts	1
		· Communication channels must handle the data load and information update rates needed for Patriot and aircrew coordination.	1
		· Real-time information display and integration of battlefield operations was not a reality of the time.	1
0	5. Group Decision-Making	There shall be protocols for Patriot and aircrew	

1	Without language communications, verbal or digital, group decision-making could not occur.	group decision-making for transit through protected airspace.	1	
1	6. Observation of Common Objects	<ul style="list-style-type: none"> Aircrew shall observe Patriot interactions, such as with radar warning receivers or data link information. Patriot system must observe friendly coalition aircraft. Strategy protocols shall confirm 	1	
			1	
0	7. Authority, Responsibility, Accountability	<ul style="list-style-type: none"> Roles and responsibilities for Patriot and aircrew in lateral coordination shall be established, either with high level strategy There shall be confirmation from each decision system of the assignment of roles and responsibilities for transit through protected airspace. 	2	
1			<ul style="list-style-type: none"> While the Patriot had an individual role and responsibility to protect ground forces and friendly aircrew, lateral coordination roles and responsibilities did not exist. 	1
1			<ul style="list-style-type: none"> Accountability that coordination was established was inadequate. 	
1			<ul style="list-style-type: none"> Accountability requires confirmation. 	
0	8. Common Understanding	<ul style="list-style-type: none"> Common understanding shall be addressed with a common picture of the battlespace operations and airspace layout. Some examples include: <ul style="list-style-type: none"> A means to ensure updated and consistent information is received by Patriot and aircrew shall be established. 	3	
2			<ul style="list-style-type: none"> The Patriot crew fired upon a target following standard arrival procedures to a friendly air base—common understanding was missing. 	1
0	9. Predictability	<ul style="list-style-type: none"> Direct planning between decision systems shall be considered Adequate information update rates and communication channels needed to ensure changes 	1	
1	For mutual adjustment coordination applicable to the accident, predictability is important.		3	
Component Commander Flawed Coordination Influences		Component Command Coordination Recommendations		
1	1. Coordination Goals (Case 2 inadequate)	Avoiding fratricide shall be a Component Commander priority coordination goal.	1	
0	2. Coordination Strategy (Case 2 inadequate)	<ul style="list-style-type: none"> Strategy to develop the AADP (Area Air Defense Plan) and ACP (Airspace Control Plan) shall be flexible to needs of the campaign The AADP and ACP shall be evaluated for conflicts in strategy. A layered approach to coordination is recommended, Coordination strategy shall provide unambiguous guidance related to the degrees of freedom 	1	
1			<ul style="list-style-type: none"> There may have been alternative non-IFF strategies (i.e. the safe passage routes) 	1
1			<ul style="list-style-type: none"> High level direction on when lower-level commanders should or were authorized to refine coordination strategies was inadequate. 	1
				1
0	3. Decision Systems	<ul style="list-style-type: none"> Air and land staff familiar with joint operations and establishing joint coordination strategy. Theater air defense command staff familiar with air defense doctrine. Expert pilots familiar with aircraft limitations and defensive system operations. 	1	
1			<ul style="list-style-type: none"> Inadequate decision systems involved in developing theater level coordination strategy may have influenced the accident. 	1
0				1

		· Expert patriot operators familiar with tactics and systems.	1
		· Patriot system technical experts	1
0	4. Communications	No recommendations.	
1	5. Group Decision-Making	A coordination framework shall be used for development and evaluation of air defense (AADP) and airspace control (ACP) coordination strategies	1
1	6. Observation of Common Objects	· Observation channels of the coordinated processes and outcomes shall be established.	1
		· Observation update rates shall be commensurate with system dynamics.	1
		· Air and land component hierarchies shall ensure their observation channels on the coordinated process are of common objects.	2
0	7. Authority, Responsibility, Accountability · Roles and responsibilities for the coordination of protected airspace. There was potential for overlapping and ambiguous coordination responsibility implementing the Area Air Defense Plan. · Authority and responsibility were inadequate for development of theater level and more refined airspace control strategy.	· The authority chain and responsibility for the implementation of the area air defense plan shall be unambiguous.	1
1		· Responsibility and authority shall be assigned to lower supporting coordination to develop strategy where degrees of freedom were afforded in the AADP or ACP.	1
1		· Accountability. Confirmation of receipt and implementation of the coordination strategy from each joint force level is needed.	1
		· Authority and Responsibility shall be assigned to manage the coordination strategy and ensure it is updated	1
2	8. Common Understanding	· Ensure scheduled opportunities exist (e.g. weekly meetings) to update staff on the coordination strategy implementation	1
		· Experts shall be involved in coordination to assist in common understanding of system operations	1
3	9. Predictability	· Developing the high level strategy shall use liaison elements and subject matter experts to help predict	1
		· Maintaining and updating the air defense and air control coordination strategy shall refer to theater level near and far term plans	1
	Air Component		
1	· 2. Coordination Strategy.		
1	· 5. Group DM.		
1	· 7. Authority, Responsibility, Accountability. JFACC staff needed to assign responsibility and authority to refine the AADP/ACP for implementation by the joint air forces.		
	Vertical Coordination land component		

2	· 7. There was inadequate accountability and confirmation that the Patriot algorithms and fire protocols were integrated with known threat and friendly information.	
1	· 8. Common understanding of friendly air forces	
Missing Lateral coordination		
2	· 5. Group Decision-Making (and 2. Coordination Strategy)	
Coordination Elements		Supporting Coordination Recommendations
1. Coordination Goals	· Vertical coordination of goals	red
2. Coordination Strategy	· Vertical coordination strategy	3
3. Decision Systems	no recommendations	0
4. Comms	· Unambiguous vertical communication channels shall be established in each Service component hierarchy from top to bottom.	1
5. Group DM	· Establish formal lateral coordination at a hierarchical level closer to the physical process.	2
6. Observation of Common Objects	· Vertical Coordination. Information of the physical processes must flow to and from Patriot and aircrew decision systems.	2
7. Authority, Responsibility, Accountability	· The Patriot automation must be coordinable, which means vertical coordination with the Patriot system influences its decisions.	1
	· Confirmation that Patriot algorithms were successfully modified to integrate current theater air defense	1
	· Confirmation of coordination information shall be received at each decision system level.	1
	· Autonomous Patriot operations shall have approval from authority that has a theater level perspective and influence.	1
8. Common Understanding	No recommendations	0
9. Predictability	No recommendations	0

F2. Coding the USCENTOM Accident Investigation for Comparison

The USCENTCOM report was reviewed and coordination-related contributing factors identified for comparison against CAST-Coordination. The coding results are given in Table 53, with column two indicating the *coordination element* coding and the last column providing the USCENTCOM report excerpt.

Table 53. USCENTCOM Coordination-Related Contributing Factors to the Patriot Incidents

Count	Coordination Elements	Coordination-Related Contributing Factors (US Central Command 2004)
1	2. Coordination Strategy	<p>“The Airspace Control Orders (ACOs) did not implement airspace control measures (ACMs) to mitigate the possibility of friend-on-friend engagements.” (p. 29)</p> <p>“A critical mitigation factor that was not applied to avert the possible engagement of an aircraft was the use of Return to Base / Return to Force Airspace Control Measures (RTB/RTF ACMs) to avoid over-flight or to control flight profiles of aircraft that had to transit Charlie Battery’s missile engagement zone (MEZ). [redacted]...If an RTB/RTF ACM had been planned and in effect, [redacted] would not have presented a flight profile consistent with the criteria for ARM [anti-radiation missile] classification.” (p. 22)</p>
2	2. Coordination Strategy	<p>“...failure to respond to IFF interrogations deprived Charlie Battery of its organic identification means ... and enabled the aircraft to be misclassified.” (p. 22)</p>
3	2. Coordination Strategy	<p>The Area Air Defense Plan (AADP) was highlighted as a general contributor the Patriot friendly fire with prescribed “...command relationships and procedures that exceeded the Joint Forces’ abilities to execute.” (p. 27)</p>
4	3. Decision Systems	<p>“The crew of Battery C/5-52 completed their certification just prior to deployment. ...they did not possess the skill set to operate in an [redacted] in OIF’s complex battlespace.” (p. 33)</p>
5	4. Comms	<p>“Connectivity between SADC, airspace controllers, and Patriot units is essential.” (p. 30)</p>
6	8. Common Understanding	<p>It was suggested that a “device” was “active on” that may have contributed to the Patriot anti-radiation missile classification (p. 23). In this section, the report discussed electronic counter measures and turning them off as part of return to base checklists, and much of the section was redacted to include a discussion on this device.</p>
7	9. Predictability	<p>Lack of situational awareness by decision systems discussed throughout.</p>

The coding results for coordination-related recommendations found in the USCENTCOM accident investigation are given in Table 54.

Table 54. USCENTCOM Coordination Behavior Recommendations

Count	Coordination Elements	Coordination-Related Recommendations (US Central Command 2004)
1	2. Coordination Strategy	AADP Recommendation 1. “The AADC’s CCIR should include the inability of failure to execute a planned AADP action and any degradation in communications between C2 nodes and air defense units.” (p. 28)
2	2. Coordination Strategy	Airspace Control Measure Recommendation 1. “For rear area operations establish and implement a ROZ out to ranges that are commensurate with published self-defense criteria or operationally supportable. If aircraft must transit these areas, implement strict RTF Transit Corridors...” (p. 30)
3	2. Coordination Strategy	Airspace Control Measure Recommendation 1. “Ensure positive control of transiting aircraft...” (p. 30)
4	2. Coordination Strategy	“The implementation of Restricted Operating Areas (ROAs) or Missile Engagement Zones (MEZs), and Return To Force Transit Corridors developed in concert with the air and ground schemes of maneuver will help mitigate risk. Aircrew, airspace controllers aboard AWACS or in SADCs, and Patriot crews are informed of these ACMs through the Daily ACO” (p. 29)
5	2. Coordination Strategy	Airspace Control Measure Recommendation 2. “Air defense operators and all joint/coalition members must continually evaluate risk and recommend the creation of MEZ/ROA in the forward area as required.” (p. 30)
6	3. Decision System	“When the mission dictates autonomous operations, commanders should ensure they place experienced crews who possess the special skills required for the mission.” (p. 33)
7	4. Comms	AADP Recommendation 2. “Branches and sequels should be developed to ensure responsive and redundant communications and C2 architectures are developed, in the event key assumptions prove invalid or combat losses are sustained.” (p. 28)
8	4. Comms	<ul style="list-style-type: none"> • Airspace Control Measure Recommendation 1. Ensure “...connectivity to Patriot units.” (p. 30) • Airspace Control Measure Recommendation 3. “In all operations, airspace controllers and SADCs must be positioned and resourced with adequate communications equipment (in include Patriot units) to ensure reliable responsive command and control can be applied.” (p. 31)
9	8. Common Understanding	AADP Recommendation 3. “The AADP must be synchronized with the Ground Component's scheme of maneuver to ensure proper prioritization of movements. (p. 28)
10	8. Common Understanding	“Any degradation in connectivity must be elevated up command channels and corrected to ensure positive control and situational awareness is maintained.” (p. 30)

11	8. Common Understanding	GR-4 Incident Recommendation: “When the operational situation dictates a battery operate in independent or autonomous operations it is essential: that fact be promulgated throughout the command via ATO SPINS and the ACO...” (p. 23)
12	8. Common Understanding	Intelligence Recommendation: “AADP...must include all aerial threats coalition forces are expected to face to ensure proper defense design and system configuration” (p. 32)
13	9. Predictability	Airspace Control Measure Recommendation 2. “As a minimum the ACO should specify a ROA [restricted operating areas] for all Patriot Batteries, based on potential missile interceptor-aircraft collision...” (p. 30)
14	9. Predictability	Conclusion. “...the key concept was increasing situational awareness of joint warfighters using weapons systems with varying degrees of integration in the electronic battlespace.” (p. 41)

F3. Coding the United Kingdom Ministry of Defence Accident Investigation for Comparison

The coding results for coordination related contributing factors in the UK Ministry of Defence report are given in Table 55. Table 56 provides the coding results for coordination related recommendations found in the UK report.

Table 55. UK MOD Coordination-Related Contributing Factors to the Patriot Incident

Count	Coordination Element	Coordination-Related Contributing Factors (United Kingdom Ministry of Defence 2004)
1	2. Coordination Strategy	“...the Patriot Anti-Radiation Missile Rules Of Engagement were not robust enough to prevent a friendly aircraft being classified as an Anti-Radiation Missile and then engaged in self-defence” (p. 3)
2	2. Coordination Strategy	“...ZG710’s IFF had a fault, which was unknown to the aircrew” (p. 5) Note: the MOD report deduced the GR-4 IFF had a failure condition noting “there is no firm evidence that ZG710 responded to any IFF interrogations throughout the entire mission” (p. 4). However, factors besides IFF reliability may have caused the interrogate/respond IFF communications to degrade.
3	2. Coordination Strategy	“...airspace routing, airspace control measures and a breakdown in planning and communication were contributory factors in the accident” (p. 5)
4	4. Communications	“...a breakdown in planning and communication were contributory factors in the accident” (p. 5) (emphasis added)

5	8. Common Understanding Note. Vertical coordination was the emphasis for this contributing factor	“...autonomous operation of the Patriot battery” (p. 3) Note: There was a speculative logic chain. The MOD report claimed that because communications to Battalion HQ was through radio relay, this “meant” the “...Patriot crew did not have access to the widest possible ‘picture’ of the airspace around them to build situational awareness” (p. 3)
6	8. Common Understanding	Patriot automation had “generic Anti-Radiation Missile classification criteria” that may not have been indicative of Iraqi threats
7	9. Predictability	“Situational awareness” (p. 3)

Table 56. UK MOD Coordination Recommendations on the Patriot Incident

Count	Coordination Element	Coordination-Related Recommendations (United Kingdom Ministry of Defence 2004)
1	2. Coordination Strategy	“...research the failure modes, reliability and serviceability of the Tornado IFF system.” (p. 5)
2	2. Coordination Strategy	“A positive challenge and response IFF check be completed after take-off between every aircraft and an appropriate control authority.” (p. 5)
3	3. Decision Systems Note: this recommendation applies to component level lateral coordination	“Operational doctrine is examined to enhance inter-component Combined Air Operations Centre liaison and air space co-ordination.” (p. 6) Note: To “enhance...co-ordination” was ambiguous.
4	5. Group DM	“Closer co-ordination is implemented between planning and operations organisations regarding airspace usage.” (p. 5) Note: “Closer co-ordination” is ambiguous.
5	8. Common Understanding Note. Within decision system coordination	“The Tornado IFF installation be modified to ensure that the cockpit warning is triggered in all failure modes.” (p. 5)