A System Theoretic Safety Analysis of Friendly Fire Prevention in Ground Based Missile Systems

by

Scott McCarthy

B.S. Computer Science (2004)
Indiana University

Submitted to the System Design and Management Program in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management
at the
Massachusetts Institute of Technology

February 2013

Signature of Author_____
Scott McCarthy
System Design and Management Program
February 2013

Certified by_____
Nancy Leveson
Thesis Supervisor
Professor of Aeronautics and Astronautics and Engineering Systems

Accepted by_____
Patrick Hale
Director
System Design & Management Program

Acknowledgements

I would like to express my gratitude to my professor and thesis advisor, Dr. Nancy Leveson, for introducing me to a new way of thinking about system safety. Her model, System Theoretic Accident Model and Processes (STAMP), has forced me to examine accidents and systems in a more holistic manner. This knowledge will help to guide my career and will enable me to more effectively deal with the safety issues that arise in complex systems.

I would also like to thank Katie Hawes, who was there to support me from near and far during my entire time at MIT. I know it wasn't always easy to deal with me through late nights and stressful deadlines, but her support and encouragement kept me going.

Abstract

This thesis used Dr. Leveson's STAMP (Systems-Theoretic Accident Model and Process) model of accident causation to analyze a friendly fire accident that occurred on 22 March 03 between a British Tornado aircraft and a US Patriot Missile battery. This causation model analyzes system constraints, control loops, and process models to identify inadequate control structures leading to hazards and preventative measures that may be taken to reduce the effect of these hazards. By using a system-based causation model like STAMP, rather than a traditional chain of events model, this thesis aimed to identify systemic factors and component interactions that may have contributed to the accident, rather than simply analyzing component failures. Additionally, care was taken to understand the rationale for decisions that were made, rather than assigning blame. The analysis identified a number of areas in which control flaws or inadequacies led to the friendly fire incident. A set of recommendations was developed that may help to prevent similar accidents from occurring in the future.

Thesis Supervisor: Nancy Leveson
Title: Professor of Aeronautics and Astronautics and Engineering Systems

Table of Contents

Chapter 1. Introduction

On 22 Mar 03 a British Tornado aircraft was incorrectly identified as an Anti-Radiation Missile (ARM) and engaged by a nearby Patriot missile battery. Both crewmembers were killed in the accident. A subsequent investigation by the British Ministry of Defence cited a number of contributory factors that led to this incident, including a presumed fault in the Identification Friend or Foe (IFF) system aboard the aircraft.

This thesis aims to examine this incident from a more holistic system-based approach in order to identify any systemic factors or component interactions that may have played a role in this incident. By using a system-based approach to safety analysis, the emergent properties of this complex socio-technical system can be examined. By examining the accident from a systems perspective, more focus can be placed on component interactions, rather than component failures. Additionally, this type of analysis can help to determine why each action in the system was taken, rather than simply detailing what happened.

This thesis begins in Chapter 2 with an examination of the motivation behind system-based causation models. Then, the accident description and proximal event chain are described in Chapter 3. Chapters 4 and 5 provide an overview of the investigations performed by the Ministry of Defence and a Defense Science Board Task Force, respectively. Chapter 6 provides a full accident analysis using the system-based causality model (CAST), including a description of the safety control structure, an examination of the control flaws or inadequacies at each level of the

structure, and a set of recommendations drawn from these inadequacies. The thesis concludes with Chapter 7, which recommends a path forward based on the results of the CAST analysis.

Chapter 2. Motivation for System-based Causation Models

This section will examine the differences between two fundamental sets of causation models: Event Chain-based models and System-based models. A brief overview of the limitations of Event Chain models is given and a new approach is discussed that eliminates many of these limitations.

Event Chain Models

In most traditional safety models, accidents are presented as the result of a linear chain of failure events, where each failure is the direct cause of the next event in the chain [2]. In these models, accidents are explained as a sequence of events that occur over time and almost always involve component failure, human error, or energy-related events (e.g. explosions or fires) [4].

The Trouble with Event Chain Causality Models

Dr. Leveson presents several reasons why these traditional chain of event models are no longer adequate for complex socio-technical systems [3]:

1. Confusion of reliability with safety – Traditional accident models often assume that if a system is reliable, then it is safe. However, in more modern complex systems accidents can occur even if no individual component has failed. Instead, serious accidents can occur because of unsafe interactions between system components.
2. Event Chain-based Causation – Traditional accident models assume that system behavior can be explained as a series of linearly related events over time. However, in complex

systems indirect events, inadequate system controls, and organizational factors can play a prominent role in understanding accidents.

3. Limitations of Probabilistic Risk Assessment (PRA) – There is typically a strong desire to quantify the probability of risk in a system, such that the system can be analyzed and decisions be made based on the result of risk assessment calculations. Many risk assessment tools, such as Fault Tree Analysis are based on such quantifications. One of the major failures of PRA in complex systems is in treating initiating events as mutually exclusive and independent. In reality, the initiating events of an accident are often the result of a migration to a higher state of risk over time due to systemic factors.
4. Role of Operators in Accidents – Most event chain-based accident analyses stop when they find an operator to blame for the accident, often blaming the operator for not following a documented process or procedure. These models often stop here because it is difficult to find an event that led the operator to make a particular decision. The reality is that the decision may have been influenced by the design of the system or by the organizational safety culture.
5. Role of Software in Accidents – Most complex systems built today have a large software component. Traditional causation models view software as just another system component and only attempt to apply reliability and correctness techniques. The reality is that software allows us to build more flexible and complicated systems than we ever have before and software cannot be isolated as an independent system component; it must be viewed in terms of its interactions with other parts of the system.
6. Static vs. Dynamic View of Systems – Traditional accident models often treat accidents as a simultaneous occurrence of random events. These models fail to recognize that

systems are dynamic and that over time they migrate toward a higher state of risk, making an accident more likely.

These limitations of traditional causation models and their underlying assumptions led Dr. Leveson to rewrite the assumptions and determine what would be needed to develop a new accident causation model based on systems theory [3]:

Old Assumption	New Assumption
Safety is increased by increasing system or component reliability; if components do not fail, then accidents will not occur.	High reliability is neither necessary nor sufficient for safety.
Accidents are caused by chains of directly related events. We can understand accidents and assess risk by looking at the chains of events leading to the loss.	Accidents are complex processes involving the entire sociotechnical system. Traditional event-chain models cannot describe this process adequately.
Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information.	Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis.
Most accidents are caused by operator error. Rewarding safe behavior and punishing unsafe behavior will eliminate or reduce accidents significantly.	Operator error is a product of the environment in which it occurs. To reduce operator "error" we must change the environment in which the operator works.
Highly reliable software is safe.	Highly reliable software is not necessarily safe. Increasing software reliability will have only minimal impact on safety.
Major accidents occur from the chance simultaneous occurrence of random events.	Systems will tend to migrate toward states of higher risk. Such migration is predictable and can be prevented by appropriate system design or detected during operations using leading indicators of increasing risk.
Assigning blame is necessary to learn from and prevent accidents or incidents.	Blame is the enemy of safety. Focus should be on understanding how the system behavior as a whole contributed to the loss and not on who or what to blame for it.

Systems Approach to Safety

By using a systems-based approach to safety, many of the limitations of chain event-based causation models can be eliminated. Instead of focusing on linear causation and component failures, systems-based approaches to safety aim to consider interactions between system components. It is through these component interactions that systems achieve their emergent properties (i.e. properties that are not the direct result of any particular component, but exist due to the interactions of one or more components). Safety is one such emergent property of a system, and as such the safety of a system can only be examined by considering the entire system operating in the context of its environment. Safety depends on imposing constraints on the behavior of the components in the system and their interactions [3].

STAMP Overview

In order to analyze system safety from a more holistic point of view, Dr. Leveson developed the STAMP (Systems-Theoretic Accident Model and Process) model of accident causation. In the model, "systems are viewed as interrelated components kept in a state of dynamic equilibrium by feedback control loops". Systems are also treated as dynamic processes that adapt to internal as well as external changes [3]. STAMP analyzes system constraints, control loops, and process models to identify inadequate control structures leading to hazards and preventative measures that may be taken to reduce the effect of these hazards. The three basic concepts – safety constraints, a hierarchical safety control structure, and process models – are discussed in greater detail below:

1. Safety Constraints – In the STAMP model, constraints are important because they are the actions that were not enforced that allowed the events leading up to an accident to occur. These controls can come in the form of human, automated, physical design, processes, and/or social controls. If enforced, these controls have the potential to prevent unsafe conditions.
2. Hierarchical safety control structure – In a hierarchical control structure, each component of the system is arranged according to increasing levels of responsibility and control, where each level of the hierarchy imposes constraints on the level below it. In this view, "constraints or lack of constraints at a higher level allow or control lower-level behavior" [3]. Inadequate control may result from missing constraints, inadequate safety control commands, commands not executed properly at a lower level, or inadequately communicated or processed feedback about constraint enforcement. To ensure safety, sufficient communication must exist between levels of the control structure in both the downward reference channel and the upward measurement channel.

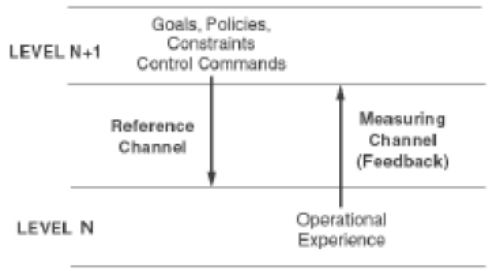

Figure 1 - Hierarchical Safety Control Structure Communication Channels [3]

3. Process models – Every process that is controlled requires that a process model be present in the system. This is true whether the controller is automated or a human

operator. The specific STAMP model conditions that must exist to control a process are [3]:

a. Goal – The safety constraints that must be enforced by each controller in the safety control structure
b. Action condition – The control action provided in the downward reference channel
c. Observability condition – The feedback provided in the upward measurement channel
d. Model condition – The controller's model of the process being controlled

In the STAMP model, accidents most often occur when the process model does not match the process being controlled. The accident is attributed to one of the following conditions [3]:

1. The safety constraints were not enforced by the controller:
    a. The control actions necessary to enforce the associated safety constraint were missing or not provided;
    b. The control actions necessary to enforce the associated safety constraint were provided at the wrong time (too late/too early) or stopped too soon; or
    c. Unsafe control actions were provided.
2. Appropriate control actions were provided but not followed.

Application of STAMP

Because STAMP is better suited to analyzing complex systems than more traditional causality models, it was chosen to investigate the friendly fire accident examined in this thesis. Specifically, it is believed that STAMP will be better suited to analyze the many socio-technical interactions present in the multi-national and multi-force command structure that existed at the time of the accident. In the following sections of this thesis an investigation of the accident will be performed using the accident causality procedures known as CAST (Causal Analysis based on STAMP). This approach to accident investigation aims to get away from assigning blame for an accident and to identify why certain actions or interactions within the system led to a hazardous state. Using CAST, the entire socio-technical structure is examined to help determine why the accident occurred and to produce a set of recommendations that may help to prevent related, and possibly unrelated, future accidents. The nine steps of CAST are [3]:

1. Identify the system(s) and hazard(s) involved in the accident.
2. Identify the system safety constraints and system requirements associated with that hazard.
3. Document the safety control structure in place to control the hazard and enforce the safety constraints. This structure includes the roles and responsibilities of each component in the structure as well as the controls provided or created to execute their responsibilities and the relevant feedback provided to them to help them do this.
4. Determine the proximate events leading to the loss.
5. Analyze the loss at the physical system level (e.g. in the case of ZG710, the aircraft, the flight crew, the Patriot battery, and the battery crew). Identify the contribution of each of the following to the events: physical and operational controls, physical failures,

dysfunctional interactions, communication and coordination flaws, and unhandled disturbances. Determine why the physical controls in place were ineffective in preventing the hazard.

6. Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level. This step contains the bulk of the analysis and will include:
    a. For each system safety constraint, determine if responsibility for enforcing the constraint was never assigned to a component in the safety control structure, or if a component did not exercise adequate control to enforce the constraint.
    b. Develop an understanding of any human decisions or flawed control actions in terms of: the information available to the decision maker as well as what information was *not* available, the context in which the decision-making occurred, the reasons for the underlying decision, and any flaws in the process models of those making the decisions.
7. Analyze the overall coordination and communication contributors to the accident.
8. Determine if there were any changes to the safety control structure over time that may have contributed to the migration of the system toward a higher state of risk.
9. Generate recommendations.

Chapter 3. Case Study Accident Description – Proximal Event Chain

On 22 Mar 03 a pair of Tornado aircraft from the Royal Air Force were returning from a combat mission over Iraq [5]. At 2348 hrs the second aircraft, ZG710, was incorrectly identified as an Anti-Radiation missile and destroyed by a US Patriot missile. Both crewmembers were killed instantly. Below is an approximate timeline of the events leading up to the missile intercept:

ZG710	Patriot Missile Battery
Flight preparation, including inspection of Identification Friend or Foe (IFF) system	Monitored airspace for Iraqi Tactical Ballistic Missiles (TBMs)
Engine startup and takeoff	
Completed mission over Iraq	
Returned to Kuwaiti airspace	Detect ZG710 in airspace
Completed aircraft checks; crew noted that IFF switches were set correctly	
Aircraft began descent towards Ali Al Salem airbase	System classified ZG710 as an incoming Anti-Radiation Missile (ARM)
	ZG710 interrogated for IFF; no response received
Aircraft was struck by Patriot missile	Patriot crew launched a surface-to-air missile in self-defense

Examination of the ejection seats confirmed that neither crewmember initiated ejection and both were killed instantly.

Chapter 4. Ministry of Defence Investigation and Findings

After the accident an official Royal Air Force (RAF) Board of Inquiry was conducted to determine the cause of the accident and to make recommendations about how accidents like this may be prevented in the future [5]. The inquiry was conducted in parallel with investigations performed by the US Army. Information was shared openly between the two investigating bodies. Data was obtained from the flight data recorder and from interviews with British and US personnel.

The RAF Board concluded that the following factors contributed to the accident: Patriot Anti-Radiation Missile classification criteria; Patriot Anti-Radiation Missile Rules of Engagement; Patriot firing doctrine and crew training; Autonomous Patriot battery operation; Patriot IFF procedure; ZG710's IFF serviceability; aircraft routing and airspace controls measures, and Orders and Instructions.

Patriot System Anti-Radiation Missile Classification

The Patriot system identifies ARMs based on several criteria, including flight profile and lack of an IFF response. In order to classify a wide variety of ARMs throughout the world, the range of ARM criteria in the Patriot system can be very broad. The Board determined that in this accident the ZG710's flight profile met the Patriot ARM criteria as it began to descend into Ali Al Salem. Additionally, the Board determined that the ARM criteria should have been narrowed to more closely match that of threats known to be in the Iraqi theater.

Patriot Anti-Radiation Missile Rules of Engagement

The Board determined that the Rules of Engagement (ROEs) governing the engagement of ARMs were not robust enough to prevent friendly aircraft from being classified as ARMs and then engaged in self-defense.

Patriot Firing Doctrine and Training

The Patriot operators had been trained to react quickly to threats and engage early. Additionally, they were trained to trust the system. In this situation the crew had only about a minute to decide whether to engage; had they waited, the Board determined that the track might have been reclassified. Even though the crew had been fully trained, their training had focused on recognizing generic threats, not those that were present in the Iraqi theater. The Board also determined that the crew had not been trained on identifying false alarms.

Autonomous Patriot Battery Operation

At the time of the accident, the Patriot battery was operating autonomously, protecting ground troops from missile attack. Since the battery's communications kit was still being shipped from the US, the battery had no direct method to communicate with the Battalion HQ. Instead a radio relay was set up with another Patriot battery that did have full voice and data links with Battalion HQ. Because of this lack of communication, the Patriot crew did not have access to the full air picture. They had no redundant methods to determine the identity of ZG710. Even in this reduced operational state the ROEs allowed the battery to engage tracks in self-defense. The Board considered it likely that a better understanding of the overall air picture would have helped the crew and made them more likely to correctly identify ZG710 as a friendly aircraft.

Patriot IFF Procedures

IFF is used to automatically identify friendly aircraft. A signal is sent to the aircraft, which replies with a particular code. This code is then checked against a known set of codes to determine if the aircraft responded correctly. Of the 5 different IFF modes, Mode 1 (an unencrypted code used in Iraq by all Coalition aircraft) and Mode 4 (encrypted) were used in the theater.

An investigation concluded that the Mode 4 interrogator at the Patriot battery was working properly throughout the engagement period, but that Mode 1 codes were not loaded. The Board concluded that the lack of a data link to the Battalion likely contributed to the difficulty of acquiring and loading Mode 1 IFF codes. This lack of Mode 1 codes increased the probability of misidentification.

ZG710's IFF System

The Board examined the following aspects of ZG710's IFF System:

IFF Serviceability

A satisfactory ground check was performed on ZG710's Mode 4 IFF and a Rapier Missile unit that regularly checked the IFF of departing aircraft did not log a fault. There is no evidence that ZG710 responded to any IFF interrogations during the mission. However, there is evidence that the navigator checked the IFF switches at appropriate times. The Board deduced that ZG710 experienced an IFF fault, since a positive Mode 4 response would have prevented the ARM classification and subsequent engagement.

Failure Modes

After the investigation, it was discovered that an indication of certain IFF power failures might not be displayed to the crew. The Board determined that a power failure would also be the most likely explanation of the absence of an IFF response.

Aircrew Actions

The Board determined that the navigator did not accidentally or consciously disable the IFF system.

Ultimately, the Board concluded that ZG710 experienced an IFF fault, which was unknown to the aircrew and which prevented an IFF response. This lack off IFF was determined to be a contributory factor.

Aircraft Routing and Airspace Control Measures

The Board determined that ZG710 followed the established speed and altitude procedures for an approach to Ali Al Salem. They also speculated that had the position of the Patriot batteries and "likely" missile arcs been taken into account in the writing of the procedures, ZG710 might have taken a different route. Additionally, procedures were in place to deal with IFF failures, but the crew would have needed to be aware of the failure to implement the procedures.

Instructions

The Board determined that the instructions available to aircrew operating without IFF were misleading.

Recommendations

In addition to standard recommendations about distributing the report and sharing information with US partners, the Board made the following recommendations:

- Conduct further research into the failure modes, reliability and serviceability of the Tornado IFF system.
- Implement closer coordination between planning and operations regarding airspace usage.

The Commander-In-Chief of the Royal Air Force Strike Command reviewed the report and made the following additional recommendations:

- Complete a positive challenge and response IFF check on every aircraft after takeoff.
- Modify the Tornado IFF installation to ensure that the cockpit warning is triggered in all failure modes.
- Examine operational doctrine to enhance airspace coordination.

In the end, the RAF board found no fault with the soldiers operating the US Patriot battery. It was determined that this was an unfortunate accident in an otherwise successful and efficient war. ZG710 was the only RAF aircraft lost during the war. The Board highlighted various complex, contributory factors and made recommendations to correct any shortcomings found through the investigation.

Chapter 5. Defense Science Board Task Force Findings

In January 2005, the Defense Science Board Task Force issued a report on Patriot System Performance during Operation Iraqi Freedom (OIF). Detailed in the report were lessons learned regarding the Patriot system as well as the general topics of combat identification and situational awareness [1].

The Task Force first assessed Patriot's overall performance as a defense against Tactical Ballistic Missiles (TBMs). 62 Patriot fire units (40 US and 22 coalition) were deployed in the theater, utilizing a combination of upgraded PAC-2 missiles as well as the new PAC-3 missiles. In total, all nine TBMs that threatened areas defended by the Patriot system were successfully engaged. None of the TBMs caused any damage or loss of life.

Despite Patriot's success in defending against TBMs, there were three unfortunate fratricide incidents, one of which was discussed in the previous chapter. Again, the report cited a complex chain of events and failures, and identified several shortfalls to be corrected.

First, the Task Force cited poor combat identification performance of the Mode IV IFF system. Poor Mode IV performance had been seen in many training exercises, yet had not resulted in a robust fix. Given that there were over 41,000 flights of coalition aircraft and over 60 Patriot fire units deployed, the number of possible friendly observations was in the millions. Even low-probability issues are likely to surface given several million opportunities. The Task Force stated

the need to fix Mode IV IFF and institute additional protection measures, such as safe return corridors.

Next, the report identified a serious lack of situational awareness by air defense units in OIF. Major systems, such as Patriot, AWACS, and AEGIS are not always able to share and assimilate all available battle space information. The Task Force believed that the US military was still a long way from the vision of seamless information sharing and correlation. In the case of Patriot, the closest source of air picture information is the Patriot Battalion HQ, yet in the accident involving ZG710, that link was weak, at best.

Finally, the Task Force cited shortfalls in the Patriot operating philosophy, protocols, displays, and software. At the time, Patriot was designed to withstand heavy missile attacks; much of the system operated automatically, with no user input, and the operators were trained to trust the system. However, this was not the environment seen in OIF. Instead, during the 30 days of operations, there were only 9 engagements of TBMs in a battle space that contained 41,000 coalition aircraft sorties. The ratio of friendly-to-enemy aircraft was 4,000-to-1. Such an environment does not necessitate the need for a mostly automated system. The Task Force cited the need for changes in software, displays, and training to deal with Patriot's ever-changing mission.

In order to fix these shortcomings, the Task Force recommended that Mode IV IFF problems must be fixed and that air defense systems need improved situational awareness. They also

recommended that the Patriot system needs to shift its operational protocols to allow for more operator oversight and control of major system actions.

Chapter 6. CAST Analysis

As outlined in Leveson's *Engineering a Safer World* [3], the Causal Analysis based on STAMP (CAST) approach to accident investigation aims to get away from assigning blame for an accident and to identify why certain actions or interactions within the system led to a hazardous state. Using CAST, the entire socio-technical structure is examined to help determine why the accident occurred and to produce a set of recommendations that may help to prevent related, and possibly unrelated, future accidents. The nine steps of CAST are [3]:

1. Identify the system(s) and hazard(s) involved in the accident.
2. Identify the system safety constraints and system requirements associated with that hazard.
3. Document the safety control structure in place to control the hazard and enforce the safety constraints. This structure includes the roles and responsibilities of each component in the structure as well as the controls provided or created to execute their responsibilities and the relevant feedback provided to them to help them do this.
4. Determine the proximate events leading to the loss.
5. Analyze the loss at the physical system level (e.g. in the case of ZG710, the aircraft, the flight crew, the Patriot battery, and the battery crew). Identify the contribution of each of the following to the events: physical and operational controls, physical failures, dysfunctional interactions, communication and coordination flaws, and unhandled disturbances. Determine why the physical controls in place were ineffective in preventing the hazard.

6. Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level. This step contains the bulk of the analysis and will include:
    a. For each system safety constraint, determine if responsibility for enforcing the constraint was never assigned to a component in the safety control structure, or if a component did not exercise adequate control to enforce the constraint.
    b. Develop an understanding of any human decisions or flawed control actions in terms of: the information available to the decision maker as well as what information was *not* available, the context in which the decision-making occurred, the reasons for the underlying decision, and any flaws in the process models of those making the decisions.
7. Analyze the overall coordination and communication contributors to the accident.
8. Determine if there were any changes to the safety control structure over time that may have contributed to the migration of the system toward a higher state of risk.
9. Generate recommendations.

Step 1 – System Definition and Hazards

System Definition

The system being analyzed is the prevention of friendly-fire incidents between a ground-based air defense missile system and friendly aircraft operating in the same theater.

System Hazard

The accident in question occurred because several hazardous conditions exist. First, a friendly aircraft was operating within range of an air defense missile system. The accident could not occur if the aircraft were outside of the engagement range of the missile system. Second, that aircraft was incorrectly identified as hostile after being misclassified as an ARM. While the misclassification lead to the hostile identification, this condition is not strictly a necessary criterion. A missile system could presumably fail to identify or classify a target and still allow for an engagement. Finally, the friendly aircraft was engaged and the missile intercepted the aircraft. Therefore, the three system level hazards associated with this accident are:

1. A friendly aircraft was operating within range of an air defense missile system.
2. The aircraft was not correctly identified as a friendly aircraft.
3. The aircraft was engaged by the missile system.

Step 2 – System Safety Constraints and System Requirements

System Safety Constraints

The system level safety constraints that must be enforced to address these hazards are:

1. Friendly aircraft must be properly identified as friendly.
2. Measures must be taken to ensure that missiles are not launched at friendly aircraft.
3. In the event of a missile launch against a friendly aircraft, there must be a way to terminate the engagement.
4. All friendly activity must be coordinated between air and ground forces to control interactions.

It should be noted that while the one of the hazards identified was "a friendly aircraft was operating within range of an air defense missile system", there is no way to remove this hazard while still performing the mission required in the battle space. In fact, the removal of this hazard removes the necessity for the system in question (i.e. preventing friendly-fire incidents between a ground-based air defense missile system and friendly aircraft operating in the same theater). There are, however, actions that can be taken to reduce the potential consequences of this hazard.

System Requirements

The system requirements necessary to prevent the system hazards and enforce the safety constraints are:

1. Aircraft must positively identify themselves as friendly when requested.
2. Positive identification codes must be displayed to the operators of the missile system when received.
3. Alternative methods for aircraft identification must be available in case the primary identification channels have failed.
4. Operators must be trained on identification criteria.
5. Operators must be trained on Rules of Engagement.
6. The missile system must allow the operator enough control to terminate ongoing engagements.

A mapping of system hazards to system-level requirements and constraints is provided in Table 1.

	Hazards	System Requirements
1	A friendly aircraft was operating within range of an air defense missile system.	All friendly activity must be coordinated between air and ground forces to control interactions
2	The aircraft was not correctly identified as a friendly aircraft.	Friendly aircraft must be properly identified as friendly Aircraft must positively identify themselves as friendly when requested. Positive identification codes must be displayed to the operators of the missile system when received. Alternative methods for aircraft identification must be available in case the primary identification channels have failed. Operators must be trained on identification criteria.
3	The aircraft was engaged by the missile system.	Operators must be trained on Rules of Engagement. Measures must be taken to ensure that missiles are not launched at friendly aircraft. The missile system must allow the operator enough control to terminate ongoing engagements.

Table 1 - System Hazards and Requirements

Step 3 – Hierarchical System Safety Control Structure

The hierarchical system safety control structure for combat operations in Iraq is contained in Figure 2. A brief overview of the command structure follows; more detailed descriptions of roles and responsibilities at each level of the hierarchy are provided later in the CAST analysis.

Overview of System Hierarchical Control Structures Roles and Responsibilities

According to the report issued by the Ministry of Defence following the accident, the command and control arrangements in the theater were based on standard Allied and UK Joint doctrine [5]. At the highest level was the Combined Operational Headquarters in Qatar, commanded jointly by a 4-star US officer and a 3-star UK National Contingent Commander. Below this were two operations commands: one for air and one for land forces. The air campaign was handled by the US-led Combined Air Operations Center at Prince Sultan Air Base in Saudi Arabia, commanded by a USAF 3-star General with an RAF 2-star on staff. The center was responsible for all air operations, including airspace co-ordination and control of all air defenses. The Land Component Commander at Camp Doha, Kuwait, was responsible for US Army ground-based air defense. Liaison elements were positioned at both Land and Air Component HQs.

At the tactical level, the Tornado aircraft was operating out of an RAF combat air wing based at Ali Al Salem in Kuwait. The Patriot battery emplaced at Camp Doha, Kuwait fell under the direct command of its Battalion HQ.

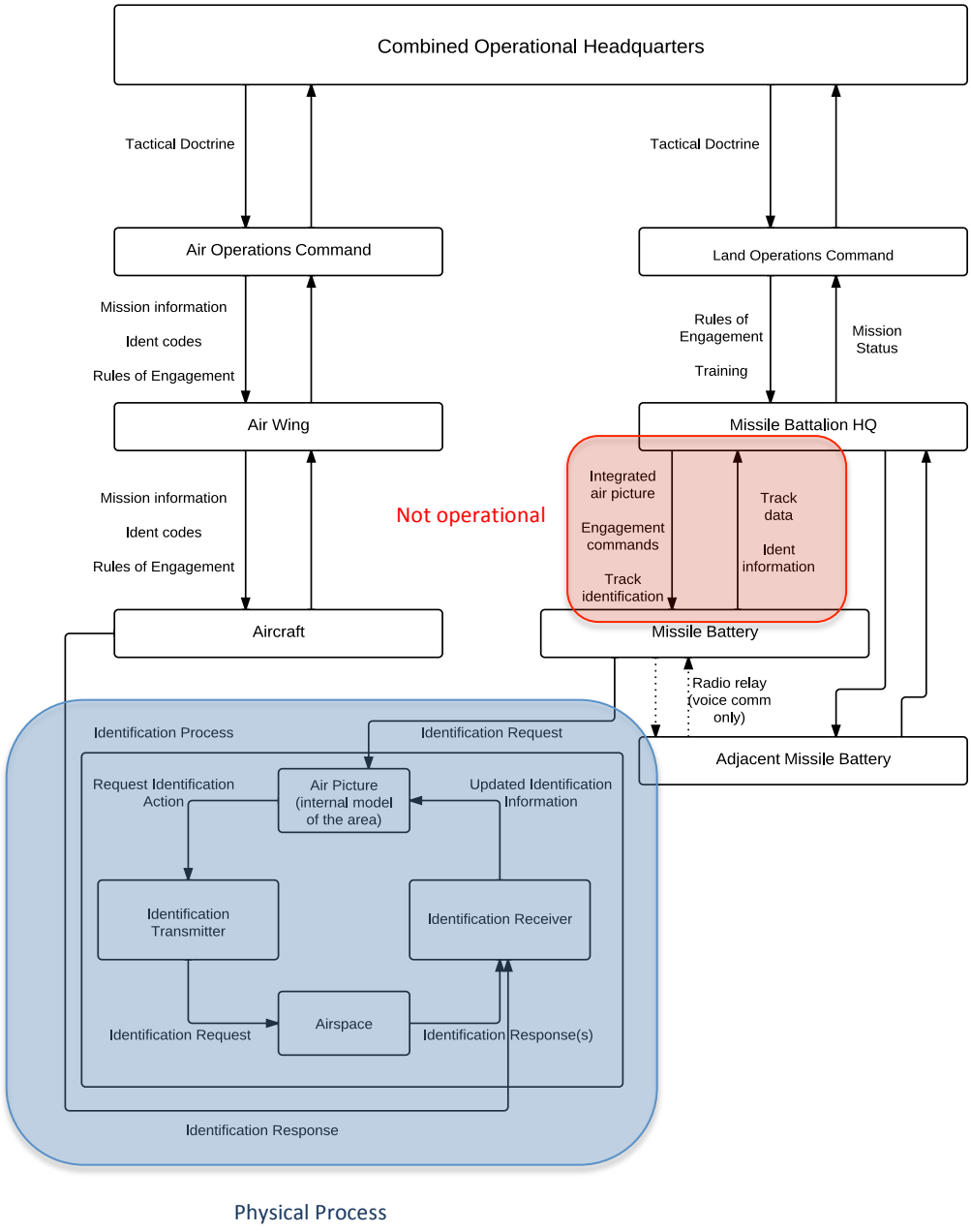

Figure 2 - Operational Control Structure

Step 4 – Proximal Event Chain

The proximal event chain was discussed in Chapter 3 of this thesis and is based on the Ministry of Defence Aircraft Accident Summary.

Step 5 – Analyzing the Physical Process

In this part of the CAST analysis, the physical system (i.e. the interaction between the Patriot battery and ZG710) is analyzed with the purpose of identifying unsafe system interactions, component failures, or inadequate system controls that contributed to the events. The goal is to determine why the controls in place at the time of the accident were not sufficient to prevent the incident [3].

Figure 3 provides a summary of the safety requirements and constraints violated within the physical system, the safety equipment present in the system, the physical failures and inadequate controls, and the physical contextual factors. Several items within the analysis should be discussed in further detail:

Inadequate Controls to Prevent the Engagement of a Friendly Aircraft:

Based on the findings presented by the MOD [5], it is clear that at least two system inadequacies contributed greatly to the engagement of ZG710: 1) the incorrect ARM classification by the Patriot system; 2) the failure to identify ZG710 as a friendly aircraft. Each of these shortcomings was directly responsible for the accident.

First, as ZG710 rapidly descended toward the Ali Al Salem airbase, the Patriot battery's computer system determined that ZG710's flight path matched the programmed criteria for an ARM. This classification was most likely caused by the need for Patriot to be able to detect a wide variety of ARMs. Patriot units are emplaced all around the world and the system needs to be able to detect and classify a large number of different ARMs with

varying flight characteristics. The MOD report cited a need for ARM classification criteria to be narrowed down to those expected to be encountered in a given operating theater [5].

Next is the failure to identify ZG710 as a friendly aircraft. This shortcoming was likely caused by two distinct factors. First, the accident investigation showed that ZG710 never responded to the IFF Mode IV interrogation requests from the Patriot battery. It is believed that a power supply failure was responsible for the lack of response. Second, the Patriot battery had no data link with the Patriot Battalion HQ. This meant that no IFF Mode 1 codes were loaded and that the battery could not receive external identification information, such as that provided by an AWACS or any other similar system. Therefore, the Patriot battery was reliant on one source of target identification (IFF Mode IV), which ultimately failed.

Inadequate Feedback to Aircrew:

Throughout the preflight, the mission, and the landing approach, the crew of ZG710 thought that their IFF equipment was working properly and would indicate a friendly status to any coalition systems interrogating them. The crew was never notified that a power supply failure was causing their IFF Mode IV system to stop functioning.

Safety Requirements and Constraints Violated:

- Aircraft must positively identify themselves as friendly when requested
- Alternative methods for aircraft identification must be available in case the primary identification channels have failed
- Measures must be taken to ensure that missiles are not launched at friendly aircraft

Emergency and Safety Equipment (Controls):

- Fault detection equipment
- Operator displays for status of IFF equipment

Failures and Inadequate Controls:

- IFF system on ZG710 never responded to IFF Mode IV interrogation
- Inadequate indicators of IFF Mode IV failure on ZG710. The crew was never notified that the system was not operational. It is suspected that a power supply failure caused the non-operational state.
- Inadequate data links between Patriot battery and Patriot Battalion HQ. The Patriot battery had no source of external identification information.
- ARM classification criteria at the Patriot battery were too broad for the operating theater.

Physical Contextual Factors:

- The Patriot battery's communication equipment was still in transit from the US. This led to the degradation of the battery's communication status and eliminated the battery's external data links.
- The Patriot battery's main role at the time of the incident was to protect Camp Doha from incoming missiles.
- Patriot personnel were trained to trust the system's classifications.

Figure 3 - Physical Plant Level Analysis

Step 6 – Analyzing the Higher Levels of the Safety Control Structure

Now that the inadequacies in the physical system have been investigated it will be helpful to examine the higher levels of the hierarchical safety control structure to understand why the inadequacies in the physical system occurred. Using the CAST procedures previously outlined, each level of the safety control structure will be examined, focusing on why failures occurred at each level and why the operators at lower levels acted they way they did [3].

Patriot Missile Battery

The Patriot missile battery was emplaced near Camp Doha and was executing its primary mission of protecting ground troops from missile attacks coming from Iraq. The battery crew was positioned inside the battery's control station and was responsible for monitoring the air picture displayed on the station's displays and making identification and engagement decisions. They controlled the system through a series of switches and tabular displays used to input data.

Figure 4 summarizes the violated constraints and requirements, failures and inadequate controls, operational context, and process model flaws at the Patriot battery. The Patriot battery crew is the component in the safety control structure with the most direct control over the events leading up to the accident. The safety requirements and constraints violated include not properly identifying ZG710 as a friendly aircraft, misclassifying

ZG710 as an ARM, and not having alternate identification methods available. The CAST analysis of this level of the safety control structure identified several inadequate controls:

- IFF Mode 1 codes were not loaded – Since Mode 1 codes were not loaded at the Patriot battery, the system was relying solely on IFF Mode IV to provide identification of friendly aircraft. The Mode 1 codes would have served as a double-check to the lack of Mode IV response by ZG710. The primary reason for the absence of IFF Mode 1 codes seems to be the lack of a data link to the Battalion HQ. Normally this link is used to transmit operational setup information to the battery. The absence of the link would have required the battery crew to manually obtain the IFF codes from another source and then to manually enter the codes through the system's tabular displays.
- No data link to Battalion HQ – Because the battery's communication suite was still in transit, the system had no way of receiving external identification information and was reliant only on directly observable identification information (e.g. IFF codes). Without a data link, the battery crew was reliant on a voice communication relay through an adjacent Patriot battery. However, this voice relay would have been ineffective during the presumed ARM attack because of the long delays in transmitting and receiving voice communications over this link. It is unlikely that there would have been an adequate amount of time for the battery crew to speak with someone at Battalion HQ and determine that ZG710 was not a true threat.

- Broad ARM classification criteria – The ARM classification criteria that were pre-programmed into the system were not modified to more accurately represent the expected threats in the Iraqi theater.

To address the control inadequacies, this CAST analysis recommends the following actions be taken:

- Since two of the inadequate controls were the direct result of the Patriot battery operating in autonomous mode (no Mode 1 IFF codes and no external identification information), the US Army should examine its operating procedures to determine if allowing this type of operation is prudent when operating in a theater where friendly aircraft greatly outnumber potential threats. When there is only one source of classification and identification, there is a much greater chance of safety-related accidents.
- Modify Patriot battery operational procedures to ensure that ARM classification criteria are sufficiently limited to match the expected threats in the theater and to avoid improperly classifying aircraft.

Safety Requirements and Constraints Violated

- Friendly aircraft was not properly identified as friendly
- Friendly aircraft misclassified as Anti-Radiation Missile
- No alternative identification methods available

Failures and Inadequate Controls

- IFF Mode 1 codes were not loaded
- No data links to Battalion HQ, resulting in an incomplete air picture
- Broad ARM classification criteria misclassified Tornado as ARM

Operational Context

- Broad ARM classification criteria were based on many ARMs observed worldwide.
- Rules of Engagement allowed Patriot crew to engage ARMs in self-defense.
- The battery's communication suite still in transit from US. Contact with Battalion HQ was via radio relay with a nearby battery, which was equipped with voice and data links to Battalion HQ. No data link was present between the involved battery and Battalion HQ.
- The battery was running in autonomous mode (no external data link) to protect ground troops from missile attack. Missile defense was the battery's primary mission and explains why the battery was allowed to operate in autonomous mode.
- Crew had been trained to trust the classifications determined by the system.

Process Model Flaws

- Battery crew believed that they were engaging an ARM in self-defense.
- Battery crew believed that IFF Mode IV would be sufficient to identify friendly aircraft.

Figure 4 - Patriot Battery Level Analysis

ZG710 (Aircraft) Crew

The RAF aircraft was operating in Iraqi airspace as part of a package of Coalition aircraft just prior to the incident. While performing a combat landing (maintaining a high altitude

until just prior to approach and then diving rapidly toward the runway) at Ali Al Salem, the aircraft was misclassified as an ARM.

The safety constraint violated at this level of the safety control structure was a failure to positively identify the aircraft as friendly when interrogated by an IFF system. The CAST analysis of this level of the safety control structure identified several inadequate controls:

- Presumed IFF Failure – It is presumed that a power supply failure led to the failure of ZG710 to provide a valid response to the IFF Mode IV interrogation, since no other IFF failure was reported and no IFF responses were received by the Patriot battery (which was equipped with an embedded data recorder). There is no firm evidence that ZG710 responded to any IFF interrogations throughout its mission.
- All IFF modes were not checked before takeoff – The IFF Mode IV system was checked prior to engine start by the ground crew. However, the other IFF modes were not checked. Additionally, according to the MOD report [5] an RAF Regiment Rapier Missile unit that regularly checked the IFF of departing aircraft did not report the aircraft or log a fault.
- Crew received no indication of IFF failures – The crew of the aircraft received no visual feedback that their IFF system had failed. According to the MOD report, this was presumably caused by a power supply failure. The IFF system on ZG710 was set up to report failures within the IFF system to the aircraft crew, but investigation of the aircraft's systems concluded that if a power supply failure occurred, then no indication would have been presented to the crew.

To address the control inadequacies, this CAST analysis agrees with the MOD report and recommends that the ZG710 IFF system should be modified to ensure that a visual indication is provided to the aircraft crew in all failure modes. Had the crew known of the IFF failure, then measures could have been taken to prevent misidentification of the aircraft.

Safety Requirements and Constraints Violated

- Aircraft did not positively identify itself as friendly

Failures and Inadequate Controls

- Presumed IFF failure
- All IFF modes were not checked before takeoff
- Crew received no indication of IFF failure

Operational Context

- Flight profile matched ARM classification at Patriot battery.
- Only IFF Mode 4 was checked on the ground.

Process Model Flaws

- Tornado crew believed that IFF was working properly. The IFF Mode IV system was checked by ground crew prior to takeoff. Checks were performed in the aircraft when returning to Kuwait airspace, including noting that IFF switches were set correctly.

Figure 5 - ZG710 Level Analysis

Patriot Battalion HQ

The Patriot Battalion HQ is the component of the safety control structure responsible for coordinating the operations of all Patriot batteries in the area. In this incident the battalion HQ was located at Camp Doha, near the Patriot battery. However, unlike most tactical operations, the battalion HQ had limited control over the Patriot battery, due to a non-functional data link between the two units. Normally, this data link allows the battalion HQ to provide the battery with external identification information, IFF codes, and a more integrated air picture.

The safety constraints violated at this level of the safety control structure were: 1) a failure to provide alternate identification information to the Patriot battery, 2) a failure to properly train Patriot operators on identification criteria. The CAST analysis of this level of the safety control structure identified several inadequate controls:

- Did not provide instructions to Patriot batteries to restrict ARM classification criteria – There were two conditions leading to this failure. First, the data link to the Patriot battery was not operational, which inhibited the transfer of theater-specific threat information that could have been used to narrow the broad ARM classification criteria. Second, even though the data link was down, the battalion HQ failed to provide these instructions to the battery through the voice communication relay that had been established through an adjacent battery. Had the crew been instructed, they could have manually entered pertinent ARM classification criteria into the system through a series of tabular displays.
- Allowed Patriot Battery to operate without alternative identification methods – The battalion HQ allowed the battery to operate in an autonomous mode, which restricted the battalion's ability to transfer identification information to the

battery. Additionally, the battery was allowed to operate without IFF Mode 1 codes loaded. These two failures resulted in the battery operating in a state in which IFF Mode IV was the only source of identification information. The battery was allowed to operate in this mode to defend the ground troops at Camp Doha against Iraqi missile attacks. It is unclear whether the Battalion HQ considered the potential for the misclassification and misidentification of a friendly aircraft when deciding to allow this mode of operation.

- Did not provide adequate training on target identification – The crew of the Patriot battery were not provided with sufficient training related to target identification while running in an autonomous state. Instead they were instructed to trust the classifications provided by the system.

Two recommendations for the Patriot system have already been addressed in the CAST analysis of the Patriot battery component. In addition to the recommendations at the battery level, this CAST analysis recommends the following actions be taken:

- Ensure that ARM classification criteria are restricted to correctly classify the types of threats in the operating theater without being so broad as to increase the likelihood of false positives. It may be necessary to transmit this information via alternative means when the primary communication link is not functional.
- Provide operators with sufficient training on target identification. This training should concentrate on identification when the primary identification mechanisms are not functional. Rather than trusting the system to make the correct classifications, battery crews should be trained to identify flight characteristics

and determine whether it is necessary to override the system's automatic classification.

Safety Requirements and Constraints Violated

- Did not provide alternate identification information to Patriot battery
- Operators were not properly trained on identification criteria

Failures and Inadequate Controls

- Did not provide instructions to Patriot batteries to restrict ARM classification criteria
- Allowed Patriot Battery to operate without alternative identification methods
- Did not provide adequate training on target identification

Operational Context

- Allowed Patriot battery to operate autonomously to meet a mission requirement of protecting ground troops from missile attacks

Process Model Flaws

- It is possible that the Battalion believed that operating autonomously would not hinder the ability to identify friendly aircraft, since the IFF system should have been able to make such an identification.

Figure 6 - Patriot Battalion HQ Level Analysis

RAF Air Wing

The RAF Air Wing at Ali Al Salem airbase was responsible for the execution of combat missions and for the maintenance of all aircraft in the Air Wing. It is here that ground crew checked the IFF Mode IV system on ZG710. Despite this action, the Air Wing

violated a safety constraint by not ensuring that ZG710 would be able to properly identify itself as friendly. Specifically, the Air Wing had the following inadequate controls:

- All IFF modes were not checked prior to takeoff – Only IFF Mode IV was checked on the ground. The other IFF modes, including Mode 1, which was to be used by all coalition aircraft, were not verified. This is important, because there is no evidence that ZG710 responded to any IFF interrogations throughout the duration of the mission.
- IFF responses were not checked while the aircraft was in flight – According to the MOD report [5], it was normal procedure for all aircraft to be checked for IFF responses by a Rapier missile unit immediately after takeoff. For unknown reasons, it appears that this did not happen on the day of the incident. The MOD report states that the Rapier unit "did not report the aircraft or log a fault." It is possible that the Rapier unit experienced an IFF fault similar to the presumed IFF fault on ZG710, or that the unit failed to interrogate the aircraft or note the lack of a Mode IV response. Furthermore, ZG710 was not checked for IFF responses at any other control point during the mission. Because of this, no one was aware of ZG710's IFF fault.

To address the control inadequacies, this CAST analysis agrees with the MOD report and recommends that all IFF modes must be checked prior to takeoff. IFF is one of the primary methods used to prevent friendly-fire incidents. Given the crucial nature of the IFF system and the potential for faults, proper operation of a unit's IFF system should be a mandatory criterion for that unit's participation in a combat mission.

Additionally, a positive challenge and response check should be performed immediately after takeoff and at any handoff to a new control authority. An aircraft's pilots must be made aware of the status of any faulty IFF system responses so that appropriate actions may be taken to correct the issue, or make up for lack of such an important safeguard.

Finally, an investigation should be performed to determine why the lack of IFF responses by ZG710 was not reported during the mission. It is common practice for aircraft entering a controlled airspace to be interrogated by some type of air traffic control system (e.g. an AWACS controller). There is no mention in the MOD report or the Task Force report of ZG710 being interrogated by such a control system. It is possible that a series of IFF checks at appropriate control points could have identified ZG710's presumed IFF fault and measures could have been taken to prevent the fratricide.

Safety Requirements and Constraints Violated

- Did not ensure that ZG710 would be able to properly identify itself as friendly

Failures and Inadequate Controls

- All IFF modes were not checked prior to takeoff
- IFF responses were not checked while the aircraft was in flight

Process Model Flaws

- Believed that ZG710's IFF system was performing correctly based on the IFF Mode IV check that was performed prior to takeoff.
- Believed that any IFF faults that occurred during the flight would be reported to the pilots

Figure 7 - RAF Air Wing Level Analysis

Land Operations Command

The Land Operations Command was based at Camp Doha, Kuwait, and was responsible for US Army ground-based air defense. In this role, they ensured that all US troops were protected from missile attacks and enemy aircraft. According to the MOD Report [5], the Land and Air Operations centers contained liaison elements to help ensure coordination between the two units. In spite of this, it appears that the Land Operations Command violated the safety constraint and did not notify its air defense units of the close proximity of friendly aircraft. The failures at this level of the safety control structure were not providing a complete air picture to missile defense units and not properly coordinating friendly activity between air and ground forces.

The root cause of these control failures appears to be a lack of communication and coordination with the Air Operations center in spite of the liaison elements that were positioned at each command. It is unclear from the reports why such a breakdown in communication occurred, but this type of breakdown is not uncommon when dealing with multi-national troops from different branches of the armed services.

To address these control failure, this CAST analysis recommends that current operational protocol be reviewed with respect to providing complete air picture information to missile defense units. During this incident the Patriot battery had no external identification information. A review of operational protocol could provide an insight into why the battery was allowed to operate in such a detached method of operation. Additionally, the communication between the Air Operations Command and the Land Operations Command should be improved. Areas of concern include the definition and enforcement of airspace control measures, such as safe-passage corridors and the coordination of identification information, especially IFF codes.

Safety Requirements and Constraints Violated

- Did not notify air defense units of close proximity of friendly aircraft.

Failures and Inadequate Controls

- Did not properly coordinate friendly activity between air and ground forces
- Did not provide complete air picture to missile defense units

Context

- A liaison element existed between Air Operations and Land Operations, but appeared to be ineffective in coordinating activities.

Figure 8 - Land Operations Command Level Analysis

Air Operations Command

The Air Operations Command was based at Prince Sultan Air Force Base in Saudi Arabia and commanded by a USAF 3-star General with an RAF 2-star on staff. This unit was responsible for air operations including airspace coordination and tactical control of all air defenses, however they did not have direct control over the Patriot batteries at Camp Doha, which fell under command of the Land Operations center. The primary safety constraint violated by the Air Operations command was the inability to limit interactions between air and ground units. It appears that there was very limited coordination of coalition aircraft missions between this unit and the Land Operations Command, even though there were liaison elements positioned at each unit. The specific control inadequacy at this level of the safety control structure was that speed and height

procedures for approach to Ali Al Salem air base did not account for position of Patriot batteries. These procedures were one of the contributing factors to the Patriot battery's misclassification of ZG710 as an Anti-Radiation Missile.

To address this control inadequacy, this CAST analysis recommends that approach patterns and published speed and altitude restrictions must take into account the presence of any nearby missile defense systems. Other airspace control measures such as the definition and enforcement of safe-passage corridors may also help to ensure the safety of aircraft entering or leaving a controlled airspace.

Safety Requirements and Constraints Violated

- Did not limit interaction between air and ground units

Failures and Inadequate Controls

- Speed and height procedures for approach to Ali Al Salem air base did not account for position of Patriot batteries

Figure 9 - Combined Air Operations Command Level Analysis

Combined Operational Headquarters

At this level of the safety control structure, the oversight of Land Operations and Air Operations are combined into a single Operational Headquarters. This command was based in Qatar, and was led by a 4-star US officer and a 3-star UK National Contingent

Commander and had overall command of the war in Iraq. The primary safety constraint that was violated at this level was that friendly air and ground activities were not coordinated to limit the interactions between the two operational entities. Specifically, the following inadequate controls were uncovered by this CAST analysis:

- Policies for IFF checkout were not complete –The primary identification mechanism employed by friendly aircraft is IFF. Because of the importance of this system, policies need to be in place to ensure the proper functioning of this system at all times. Yet, ZG710 was allowed to fly its mission without all IFF modes being checked prior to takeoff and without its IFF responses being checked throughout the mission. Even if all of ZG710's IFF modes had been checked on the ground, chances still exist for a misconfigured IFF system since the verification of IFF codes would be performed by the personnel responsible for loading IFF codes into the aircraft. The ground crew performing this verification would presumably use the same codes they just loaded into the IFF system to verify its proper operation. This type of check is adequate to verify that the IFF system is operational, but inadequate in ensuring that the proper code set was loaded. Additionally, the Patriot battery was allowed to operate without a full set of IFF codes.
- Policies for interactions between air and ground forces operating in close proximity were inadequate –Airspace control procedures were not in place to limit the interactions of coalition aircraft and missile defense systems. Airspace control measures were not identified and commanded down to subordinate units.

- Policies surrounding ARM classification were not restrictive enough to prevent misclassifications – Because the ARM classification criteria is so broad in the Patriot system, policies should have been in place to restrict the criteria to match those of expected threats in the operating theater.

To address these control inadequacies, this CAST analysis recommends the following:

- Policies regarding the use of IFF systems should be investigated to ensure that this important safeguard is fully operational at all times. Specifically the policies should address potential system failures, positive challenge and response checks at various points during a mission, and system operation without a full set of codes. It is important that any IFF verification be performed by an independent system to verify that the correct IFF code sets were loaded into all systems present in the theater.
- Policies regarding airspace coordination should be investigated to ensure that they fully consider the operation of missile defense systems in the vicinity of friendly airbases. Specifically the policies should consider mandating the use of coordination measures, such as safe-passage corridors and weapon control volumes. All systems operating in the theater should be capable of displaying and honoring these measures.
- Policies regarding the restriction of ARM classification measures should be investigated. The difficulty with these policies is ensuring that the classification criteria are broad enough to detect a wide variety of ARM characteristics while ensuring that false positives are not produced.

Safety Requirements and Constraints Violated

- Friendly air and ground activities were not coordinated

Failures and Inadequate Controls

- Policies for IFF checkout were not complete.
- Policies for interactions between air and ground forces operating in close proximity were inadequate.
- Policies surrounding ARM classification were not restrictive enough to prevent misclassifications

Process Model Flaws

- Believed that ground based IFF system checkout was adequate to ensure proper IFF operation.

Figure 10 - Combined Operational Headquarters Level Analysis

Step 7 – Examination of Overall Communication and Coordination

As shown in the analysis of each level of the hierarchical safety control structure, communication problems existed throughout the system. Rather than continuing to focus on each component in the control structure individually, this section will examine the communication and coordination problems that existed between components. These problems fall into three primary categories: IFF system coordination, Airspace coordination, and Air picture communication.

Perhaps the most crucial communication breakdown occurred with the IFF system in place in the theater. IFF checkout policies were not stringently enforced, IFF codes were not always properly loaded at each platform, and IFF system status was not always directly observable by the operators of the systems being employed. By its nature, IFF is a system that relies on the communication of a set of codes used to identify friendly aircraft. When this communication system breaks down, aircraft operators are no longer protected from friendly fire.

Next, there was a distinct lack of airspace coordination between the various components of the safety control structure. Even with the existence of liaison units between the Air Operations and Land Operations command, it seemed that neither command was fully aware of the activities of the other. This lack of coordination directly contributed to the accident involving ZG710, placing the aircraft within range of the Patriot battery during a crucial phase of flight. Even if liaison units had not existed between the two commands, the Combined Operational Headquarters was in a position to coordinate, or ensure coordination of, any activities in the airspace.

Finally, the Patriot battery did not possess a complete air picture because of a lack of communication with the Patriot Battalion. As discussed earlier, this communications hole existed because the battery's communication suite was still in transit from the US. The result was that the battery did not possess a means to verify the identity of ZG710 and was forced to rely only on what was directly observable by the battery. A more complete

air picture could have helped the battery crew to realize that ZG710 was not an ARM, but instead was a friendly aircraft.

Step 8 – Dynamics and Migration to a High Risk State

Over time, all systems naturally migrate toward a state of higher risk. This can be caused by system degradation (e.g. component wear or failures), changes in the operating environment, or changes in the organizational structure surrounding the system. In the accident involving ZG710 the two most prominent areas of system migration were changes in the IFF system state and changes to the communication channels.

The most obvious change in the IFF system was the presumed failure of ZG710's onboard IFF system. The inability of ZG710 to respond to IFF interrogations prevented it from more easily being identified as a friendly aircraft. These IFF responses were critical to the prevention of friendly fire. But it was not only the IFF failure at ZG710 that migrated the system toward a higher risk state. It was also confirmed that the Patriot battery did not have Mode 1 IFF codes loaded at the time of the accident. The design of the IFF system allows for multiple modes to be interrogated simultaneously. In some cases the responses can lead to ambiguous results (e.g. a positive Mode 1 response and a negative Mode IV response), but in some cases the multiple responses allow for an element of redundancy. By not having one of these modes available, the chances of misidentification were increased.

The other area of risk migration involved the communication channel between the Patriot battery and the Patriot Battalion HQ. Typically when a Patriot battery is emplaced in the field it is commanded by the battalion HQ and voice and data links are established between the units. These links allow for the transmission of operational control data such as IFF codes and ARM classification criteria. However at the time of the accident, the Patriot battery was allowed to operate without this data link. This was not an oversight during the setup process, but a conscious decision made when the shipment of the battery's communication equipment was delayed. In order to allow the battery to perform its air defense mission and protect the troops stationed nearby, it was decided that the battery could operate autonomously even though it would have a reduced air picture.

Both of these areas of migration helped to contribute to the accident involving ZG710.

Step 9 – Recommendations

In summary this CAST analysis of the friendly fire accident involving ZG710 recommends that the following actions be taken to address inadequacies in the safety control structure:

- As stated in the MOD report [5], the IFF system in the Tornado aircraft should be modified to alert the crew to a failure in all fault modes, including power supply failures.
- All IFF modes should be checked prior to takeoff. Any codes loaded into the aircraft should be checked by an independent source and should not rely on the same information source that was used to load the codes into the aircraft. By

verifying the IFF codes independently, it can be assured that the proper code sets were distributed to all units in the same theater.

- In addition to the pre-takeoff checks, a positive IFF challenge and response should be initiated at appropriate control points during the aircraft's flight (e.g. handoff to a new control authority). The aircraft crew must be notified if a response is not received or is incorrect.
- Along these lines, an investigation should be performed to identify why the lack of IFF responses from ZG710 was not reported by any unit during the mission. The MOD report states that there is no indication that a response was ever received from ZG710, but does not indicate why this was not reported before ZG710 attempted to land.
- Operational protocols should be modified to ensure that the published speed and altitude restrictions take into account any missile defense units within range of the operating environment.
- Operational protocols should be reviewed with regards to allowing a missile defense unit to operate in autonomous mode. The lack of any external identification information increases the risk to friendly aircraft in the area. Specific operating criteria and procedures, such as the proper functioning of all IFF modes, should be put in place to reduce the impact of operating in this degraded state.
- The procedures related to the restriction of ARM classification criteria should be modified to ensure that missile defense systems are operating with a set of criteria

that reflects the types of threats that are expected in the operating theater. Care should be taken to ensure that the criteria are neither too broad nor too narrow. The operational protocol should also discuss the transmission of these criteria via alternate methods if the primary communication method (in this case the Patriot data link) is not available.

- Patriot battery crewmembers must be trained to identify target classifications independent of the automated classification performed by the system. In the event of a misclassification, the operators should be able to identify the error and override the system classification.
- Communications between land and air operation commands should be improved regarding the coordination of airspace operations. Specifically, airspace control measures, such as safe-passage corridors, should be used to provide a measure of safety when operating in the vicinity of missile defense systems. Additionally, IFF procedures and codes must be coordinated to ensure that this important system is operated to its full potential.

Chapter 7. Conclusion

This thesis analyzed the friendly-fire incident that occurred on 22 March 03 between a British Tornado aircraft and a Patriot missile battery using a system-based accident causality model. This analysis examined all levels of the hierarchical safety control structure in order to find flaws and inadequacies in the control actions provided at each level of the hierarchy. By examining the interactions between each component of the control structure a deeper understanding of each entities action's was developed. Further, the analysis uncovered the rationale behind many of the decisions that were made leading up to the incident.

It is the author's hope that some of the recommendations provided in this thesis can be used to help ensure the safety of aircraft operating in the vicinity of ground-based missile defense systems. Protecting friendly aircraft is not an easy task, but implementing some of the recommendations of this analysis may help to make such operations safer for those involved. Additionally, it is hoped that future accident investigations or pre-deployment safety analyses may use system-based causation models, like STAMP, in order to more fully understand the interactions of complex socio-technical systems.

References

1. Department of Defense. Report of the Defense Science Board Task Force on Patriot System Performance. January 2005.
2. Leplat, Jacques. Occupational accident research and systems approach. New Technology and Human Error, cd. Jens Rasmussen, Keith Duncan, and Jacques Leplat, 181-191. New York: John Wiley & Sons. 1987.
3. Leveson, N. Engineering a Safer World. MIT Press.2012
4. Leveson, Nancy. Safeware: System Safety and Computers. Adison-Wesley. 2005.
5. Ministry of Defence. *AIRCRAFT ACCIDENT TO ROYAL AIR FORCE TORNADO GR MK4A ZG710,* May 2004.