Hierarchical Causal Accident Analysis of a Complex System

By

David G. Bancroft

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

May 2002

©2002 David G. Bancroft. All Rights Reserved.

The author hereby grants MIT permission to reproduce and distribute publicly paper and electronic copies of this thesis document in whole or in part.
DISCLAIMER

Page has been ommitted due to a pagination error by the author.
Hierarchical Causal Accident Analysis
of a Complex System

By

David G. Bancroft

May 2002

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

ABSTRACT

On August 7, 2001, the United States Navy lost two developmental torpedoes in the test range of the Atlantic Undersea Test and Evaluation Center (AUTEC), located off the coast of Andros Island in the Bahamas. The torpedoes were sequentially launched from hovering US Navy SH-60F helicopters, entered the water, sank to implosion depths, and were not recovered. From underwater sound recordings it was determined that neither unit attempted to start its engine and in both cases the onboard recovery system failed to activate. The decision was made to halt the remainder of the testing (an additional 3 torpedoes were planned to be launched that day) and to conduct an extensive (and expensive) failure analysis. Each torpedo was worth in excess of $1.5 million dollars but more importantly; the accident nearly caused the cancellation of the program.

The failure investigation conducted by the Naval Undersea Warfare Center resulted in a finding of “no fault found” due mostly in part because a definitive failure mechanism or “smoking gun” could not be identified. A shortcoming in the engine start sequence software was found that could potentially explain how the incident occurred but extensive testing could not replicate the failure mode. What caused the accident and what could be done to prevent it from happening again? Was the accident a result of a compressed schedule and a minimal budget? Was it the result of poor management or communications? The purpose of this paper is to explore why such a failure occurred in light of in-place system engineering, safety and CMM level 2 processes and to use the concept of hierarchical causality to identify the root causes. Hierarchical causality examines the accident in a holistic manner, expanding the investigative space beyond the mechanism of failure and into the technical, human, organizational and regulatory components of the US Navy’s torpedo enterprise. All of these program components are addressed in the curriculum of the System Design and Management (SDM) program at MIT, and it is the intent of the author to identify which have the greatest capacity to be the root cause.

Thesis Advisor: Nancy Leveson
Title: Professor of Aeronautics & Astronautics and Engineering Systems
ACKNOWLEDGEMENTS

I will never forget the memories I’ve accumulated over the past 2 years while in the SDM program. Contrary to everyone’s belief, I did not stuff the IBT ballot box with votes for Ireland! Nevertheless, a special thanks to Ben and Hans for your “help” in letting me steer the IBT in the direction I wanted. Denny and Ted for keeping all of us on track. Thomas for keeping me laughing during design challenge 2. The Naval Undersea Warfare Center for allowing me to attend the SDM program and to Peter Harrigan for paving the way.

A special thanks to Professor Leveson for being so patient during my thesis development.

And finally, my wife Suzanne and children Jared and Chelsea, for which this would not have been possible without their love and support. I promise to fix the fence and paint the trim this summer!
TABLE OF CONTENTS

ABSTRACT ........................................................................................................................ 3
ACKNOWLEDGEMENTS ............................................................................................... 4
TABLE OF CONTENTS ................................................................................................. 6
LIST OF FIGURES ........................................................................................................ 8
LIST OF TABLES ............................................................................................................ 8
1 Thesis Goal and Outline ........................................................................................... 10
  1.1 Thesis Goal ........................................................................................................... 10
  1.2 Thesis Problem Statement ................................................................................... 10
  1.3 Motivation and Plan for the Thesis ....................................................................... 14
  1.4 Thesis Outline ....................................................................................................... 14
2 A Discourse on Torpedoes ....................................................................................... 16
  2.1 Historical Overview ............................................................................................. 16
  2.2 The Basics of Underwater Acoustics .................................................................. 16
  2.3 The Mission .......................................................................................................... 17
  2.4 Littoral versus Deep Water .................................................................................. 19
3 The Accident .............................................................................................................. 20
  3.1 AUTEC ................................................................................................................... 20
  3.2 The Test Plan ......................................................................................................... 21
  3.3 Pre-Flight Checks ................................................................................................ 22
  3.4 The Launch ............................................................................................................ 22
  3.5 All Stop ................................................................................................................ 24
4 The Investigation ....................................................................................................... 25
  4.1 NUWC Investigation ............................................................................................ 25
  4.2 Buoyancy System Failure ..................................................................................... 26
  4.3 Engine Start Failure .............................................................................................. 27
  4.4 No Fault Found ..................................................................................................... 34
5 A Hierarchical Approach to Causality ................................................................. 35
  5.1 Flaws in the Safety Culture - Priorities ............................................................... 37
  5.2 Organizational Structure ..................................................................................... 39
LIST OF FIGURES

Figure 1 Torpedo Enterprise Funding ................................................................. 12
Figure 2 Simplified Kill Chain ........................................................................... 18
Figure 3 Launch of MK54 Torpedo From SH60F ............................................... 23
Figure 4 Launch Mode Decoding ....................................................................... 32
Figure 5 Engine Start Sequence ....................................................................... 33
Figure 6 Hierarchical Model ........................................................................... 36
Figure 7 NUWC Torpedo Organization ............................................................ 40
Figure 8 Probability of Communication ........................................................... 42
Figure 9 Simplified FTA ................................................................................ 46

LIST OF TABLES

Table 1 Hazard Classifications ....................................................................... 44
Table 2 Safety Precepts ................................................................................ 44
1 Thesis Goal and Outline

"If eternal vigilance is the price of liberty, then chronic unease is the price of safety"

James Reason, “Managing the Risk of Organizational Accidents” [1]

1.1 Thesis Goal

The goal of this work is to examine, using hierarchical causality, the various components of an engineering project and their potential for unforeseen accidents that could seriously jeopardize the success of the project. This thesis considers a US Navy development program that the author is currently the project manager of while in the System Design and Management (SDM) program. The MK54 (pronounced “mark 54”) Lightweight Hybrid Torpedo (LHT) Development Program is used as a case study to investigate the hierarchical approach to causality and to minimize/eliminate the potential for future accidents.

1.2 Thesis Problem Statement

The cold war was the catalyst to the creation of many mega-dollar defense related programs. The United States (US) Navy has had many such programs, two of which are germane to this thesis: the MK48 Advanced Capability (ADCAP) and the MK50 Advanced Lightweight (ALWT) torpedo programs. Both programs were initiated to counter a new undersea threat: the Russian Alpha submarine. The Alpha broke new ground with respect to submarine performance with its deep diving, high speed and low radiated noise capabilities. The ADCAP, a submarine launched torpedo, and the ALWT, launched from aircraft, focused on the development of new propulsion systems to combat...
the deep diving and high-speed capability of the Alpha and on new sonar systems to locate the stealthy Russian submarine. The non-technical characteristics of both programs were very similar: a development timeline of approximately 10 years, a total budget exceeding $1.5 billion each, and the start of the program coinciding with the Reagan Administration buildup of defense spending.

The 1990’s ushered in a change to the political landscape with election of a Democratic president and the loss of the DoD’s most prominent enemy – the Soviet Union. Along with these changes came a realization that DoD programs would no longer operate like ravenous bears, devouring billions of taxpayer dollars without regard. A wave of acquisition of reform came crashing over the walls of the Pentagon and suddenly programs were required to espouse concepts such as software and hardware reuse, Commercial Off The Shelf (COTS), and earned value measurement to be considered for approval.

The fall of the Soviet Union in 1991 triggered a reversal in government spending on defense related projects, especially torpedoes. Figure 1 shows the various funding components of the torpedo enterprise and the sudden drop off in funding beginning in fiscal year 1991. [2] The largest drop off occurs in weapon procurement (WPN) followed by Research Development Test and Evaluation (RDTE). The ADCAP and ALWT programs were developed during the Reagan Administration’s defense buildup whereas the MK54 Lightweight Hybrid Torpedo (LHT) program was developed during the lowest levels of torpedo funding on record. Acquisition reform, as a result of the end of the Cold War, created a new torpedo program with a development timeline of 7 years and a

Massachusetts Institute of Technology – System Design and Management
total budget of $100 million. This represented a reduction in development time of 30% and a budget reduction of 94%.

![Figure 1 Torpedo Enterprise Funding](image)

**Figure 1 Torpedo Enterprise Funding**

The MK54 program was initiated in 1996 to create an affordable torpedo that would be effective against diesel-electric submarines operating in littoral environments. The collapse of Russia resulted in a change in the undersea warfare landscape. Large, nuclear powered submarines that cost billions to construct and more importantly billions to maintain, gave way to smaller diesel electric submarines that are cheaper to build and maintain. No longer was the threat moving quietly along at depths of greater than 600 fathoms. This new threat now lie in less than 100 fathoms of water, hidden amongst the

---

*Massachusetts Institute of Technology – System Design and Management*
acoustic backdrop of crashing waves, snapping shrimp, noisy fishing trawlers and coral covered sea bottoms.

While the challenges facing the ADCAP and ALWT programs were for the most part technological in nature, the challenges of the LHT program came from three well-known program metrics: cost, schedule and performance. The reduced timeline and budget draws attention to the fact that while today’s managers are required to “do more with less” it is not clear if developments in management have allowed them to accomplish that. Systems being developed today are sometimes orders of magnitude more complex than those developed twenty years ago, due largely to advancements in software engineering. Yet, this rapid rise in complexity has not been offset with increased timelines and budgets but rather it has been offset by a greater acceptance of risk, both perceived and unknown.

On August 7, 2001, off the waters of the Bahamas, two developmental MK54 torpedoes were permanently lost, each carrying an estimated value of 1.5 million dollars. Such an event would have hardly raised an eyebrow had this happened to either the ADCAP or ALWT programs but to the MK54 program, outfitted with 6% of the budget and 70% of the schedule of the Reagan era programs, it was nearly fatal. Was the accident a result of the program constraints or was it a result of poor systems management?
1.3 Motivation and Plan for the Thesis

Given the problem statement in section 1.2, the motivation for this thesis is to consider the challenges associated with the development of complex systems in today’s fiscally constrained climate and to highlight the roles of engineering and management necessary to mitigate the apparent high levels of risk. This thesis considers the United States Navy’s MK54 Lightweight Hybrid Torpedo (LHT) program as a case study to emphasize the risks, both programmatic and human, associated with reduced budgets and accelerated schedules characteristic of many development programs today. A hierarchical approach to the cause of the 7 August accident will be used piece together the root causes of the failure.

This thesis provides the author, as the manager of the MK54 program, with a mechanism to take a holistic view of the program and its surroundings and identify what went wrong. More importantly, this work will highlight areas, both technical and managerial, in need of improvement and identify possible solutions.

1.4 Thesis Outline

Section 2 provides an overview of torpedoes including historical developments, mission profile and a short treatise on underwater acoustics.

Section 3 provides the details surrounding the accident

Section 4 details the US Navy led failure investigation and findings.

Section 5 looks at the failure using hierarchical causality analysis.

Section 6 provides the findings of the hierarchical analysis.

Section 8 is the conclusion of the research.
Section 9 is the list of references.

Appendix A is the executive summary of this research in the format required by the MIT System Design and Management program.

Appendix B is a list of acronyms.

Appendix C is a section of the MK54 launch software requirements.
2 A Discourse on Torpedoes

2.1 Historical Overview

The development of the first torpedo is credited to an Englishman, Robert Whitehead, who in 1860s created a radical new weapon concept that ultimately revolutionized the way naval warfare was to be conducted. [3] The torpedo provided a new system concept that gave an impetus to developing new platform types, from torpedo boats and destroyers to submarines, which would play a major role in modern naval warfare. [4] During World War II, the Mark 14 torpedo alone sank over four million tons of ships and played a major role in the defeat of the Japanese. [5] This is an impressive fact when one considers that the Mark 14 was a line of sight torpedo and required the steady eye and hand of the launcher. The follow-on developments in underwater acoustics would eventually separate the weapon from the launch platform and introduce sophisticated, autonomous undersea weapons.

2.2 The Basics of Underwater Acoustics

With the exception of a swimming pool, most of us are aware that our range of sight becomes nonexistent as one goes deeper, away from the surface of a body of water. Visible light is scattered and extinguished by the very richness of the dense sea life. [6] Since visual information is not available, the use of acoustic echo ranging, similar to methods used by bats, is used to “see” underwater. Acoustic echo ranging is, simply, the transmission of a sound into a medium and then waiting for the echo to return. The basic idea is that the knowledge of speed of sound in water, and the time of travel of the sound, permits the calculation of the distance between the source and the reflector. [6]
Sound Navigation and Ranging (SONAR) is the term most commonly used to identify the transmission and reception of sound underwater. [7] Unlike Radar, which transmits energy through a nearly homogeneous medium (atmosphere), the problem of transmission of sound in the ocean is quite complex because of the wide variability of the physical properties of seawater. [8] The velocity with which sound travels in water varies with the temperature, salinity and depth pressure. An empirical expression for the velocity of sound in sea water is: \( c = 141,000 + 421t - 3.71t^2 + 110S + 0.018d \) where \( c \) is the velocity in centimeters per second, \( t \) is the temperature of the sea water in centigrade, \( S \) is the salinity in parts per thousand and \( d \) is the depth below the surface in centimeters. [8] The difficulty in acoustic echo ranging is because the ocean is an inhomogeneous medium and the conditions are typically not known apriori.

2.3 The Mission

The mission of a torpedo, whether fired from a submarine or aircraft, is to seek and destroy a hostile target that has previously been detected by the firing craft. Submarine launched torpedoes (also known as heavyweights) are used to destroy both surface vessels and submerged targets. Torpedoes delivered via aircraft (otherwise known as lightweights) are designed with the sole purpose of destroying submerged targets. The terms heavyweight and lightweight come from the physical differences between the two. Heavyweight torpedoes are typically 21 inches in diameter, 20 feet in length and carry warheads weighing nearly 750 pounds. In comparison, lightweight torpedoes are generally 12.75 inches in diameter, 10 feet long and carry warheads weighing approximately 100 pounds. The main size differential is due to the enormous explosive
charge needed to sink a surfaced vessel vice the relatively small amount of explosive
needed to rupture the hull of a submerged submarine. Hull rupture is aided by the
addition of localized seawater pressure on the hull. Lightweight torpedoes are only used
for anti-submarine warfare (ASW).

The phases of the torpedo mission are often referred to as the kill chain. Since the
ultimate mission of the torpedo is to destroy an enemy target, kill chain is an appropriate
but possibly politically incorrect terminology. Two major sequences in the kill chain are
critical to having any chance of locating and destroying the target. The first is engine start
and the second is target acquisition. Without the first the mission never begins, without
the second the mission never ends. The major phases of the kill chain are depicted in
Figure 2 below.

![Figure 2 Simplified Kill Chain](image)

The names of each phase are for the most part self-explanatory. Engine start is a
sequence of events that bring the torpedo a dormant state to an operational state. The
search phase is characterized by the broadcasting of acoustic transmissions in various
directions in an attempt to locate the target. The role of acquisition is to examine the echo
returns and locate the target signature amongst the background noise. Once properly
classified as a target, the torpedo then begins to home on the target using each echo return
to update estimates on the target's bearing and speed. The torpedo will continue on an intercept path until finally hitting the target, exploding on contact.

2.4 Littoral versus Deep Water

The demise of the Soviet Union resulted in a gradual paradigm shift in undersea warfare. No longer were the Soviets, with their large, deep diving submarines, considered the primary threat. The cost of maintaining the Soviet fleet could not be supported by the new government. The war fighter focus now lay on the smaller, more cost effective diesel electric submarine. The battle for “blue water” superiority had been won by the United States. Now undersea warfare moved in close to shore, into an environment altogether different from the deep depths of the world’s oceans.

As was stated previously in section 2.2, the basic premise for operating undersea is acoustic echo ranging. In deep waters (>800 ft) the sound velocity profile (SVP) is iso-velocity due to the near constant water temperature. Additionally the propagation paths of the sound are far away from boundary discontinuities such as the surface and the ocean floor. Littoral or shallow water environments bring into play numerous complications due to the effects of non-iso-velocity SVPs and surface and bottom interactions. As sound travels through the water, the path is bent due to the variation in the speed of sound. The spatial resolution of a target echo becomes much more complicated due to multi-path echo returns.
3 The Accident

"My God, Thiokol, when do you want me to launch, next April?"

- Lawrence Mulloy, Manager, Challenger Solid Rocket Booster Program [9]

3.1 AUTEC

Torpedo testing takes place on instrumented ranges or in the open ocean. An instrumented range consists of a body of water that either has a network of hydrophones placed in a grid pattern on the sea floor or a network of hydrophones suspended on cables from the floor, depending on the water depth. The torpedo is outfitted with a transducer that is keyed to the operating frequency of the hydrophones. The range is capable of tracking the torpedo in X, Y and Z space and the progress is reported to a screen in the range house. An open ocean test would not have the instrumented network and post run analysis is accomplished using internal data recorded by the torpedo.

The Atlantic Undersea Test and Evaluation Center (AUTEC) is an instrumented range situated to the south of Nassau, in the Commonwealth of the Bahamas. Its unique feature is that it is located on a piece of the Atlantic Ocean called the Tongue of the Ocean (TOTO), a name derived from the shape of a natural cul-de-sac cut into the ocean floor. The water depth of the TOTO is over 1,400 fathoms (8,400 feet) at the north end and decrease uniformly in depth to about 700 fathoms at the southern end.[10] The Navy's interest in this ocean floor cul-de-sac comes from the fact the phenomenon that this area provides one of the best acoustic test sites in the world as it isolates all of the ocean artificial noise.[11]
3.2 The Test Plan

The planned tests consisted of firing five (5) MK54 EDM torpedoes from two versions of the US Navy’s SH60 helicopter. The torpedoes were to enter the water, startup and proceed with the search mission, trying to locate the USS Memphis, a US Navy nuclear fast attack submarine. The submarine was at a depth of 350’, with strict orders not to go deeper while the torpedo was operating. The torpedo was programmed to not go shallower than 375’, creating a safety stratum of 25’ between the weapon and the keel of the submarine.

The first two launches were to be launched from two SH60F helicopters, in the Helicopter Attack Torpedo System (HATS) mode. The remaining three torpedoes were to be launched in fly-in mode by a pair of SH60B helicopters. Fly-in mode is simply the releasing of the torpedo at a certain altitude air speed to deliver the torpedo to a predicted location based on trajectory calculations. The release of the weapon in fly-in mode starts a chain reaction involving lithium based thermal batteries that provide power to the electronics prior to the starting of the engine.

HATS mode differs from fly-in mode in that the 60F helicopter hovers above the drop point and electrically starts the thermal battery while the torpedo is still attached. As the torpedo’s thermal battery produces power, the electronic sub system start up and the torpedo’s inertial measurement system determines which direction the helicopter is pointing. Upon water entry and engine start, the torpedo will return itself onto the same bearing that the helicopter was pointing prior to launch. A HATS launch is also referred to as directed search (DS), meaning the torpedo will search down a given bearing. In fly-
in mode the torpedo has no pre-launch bearing information and will start the search at whatever bearing it hits the water. Fly-in is also known as non-directed search (NDS).

3.3 Pre-Flight Checks

Prior to the start of any military mission, regardless of whether the mission is an exercise or a real combat situation, pre-briefs are conducted to lay out the roles and responsibilities of the participants and to review the test plans. This test series was the first ever interaction between the MK54 torpedo and a USN fleet helicopter. Prior to this test series, all helicopter launches were conducted from a specially made launcher hanging from a commercial helicopter. Commercial helicopters are often used for development tests because it is easier to schedule them and often times more cost effective.

As part of the pre-flights checks, the fire control system of each helicopter involved was tested using a torpedo simulator. This simulator uses actual torpedo interface hardware to communicate with and measurement responses from the helicopter.

3.4 The Launch

On 7 August 2001, at 0645 EDT, a US Navy SH60F helicopter hovered above the AUTEC test range and launched MK54 torpedo serial number 54021 in accordance with run plan 1035 (see Figure 3). Sonar operators, along with the author onboard the USS Memphis, recorded the splash of the torpedo as it entered the water. The captain of the boat ordered a change in direction and speed according to the evasion tactic identified in
the test plan. The sonar men continued to listen for the tell tale sound of engine start and the torpedo's acoustic homing "pings". Nothing was heard.

![Figure 3 Launch of MK54 Torpedo From SH60F](image)

Figure 3 Launch of MK54 Torpedo From SH60F

At approximately 3:25 seconds a series of distinct sounds were recorded by the towed array of the USS Memphis and the AUTEC range hydrophones. The sound and location of the torpedo on the range display indicated that the unit had entered the water continued on the same glide slope to a depth that caused the outer hulls to implode. At the test event pre-brief, plans had been made to determine what plan of actions would take place if a mishap occurred. In the event that the first torpedo failed to start, the plan called for proceeding with the second firing as planned. The thought process was that if the first unit failed, the problem could possibly be attributed to a mechanical or assembly
problem. If the second unit failed in a similar manner, then a systemic problem was highly likely and the remaining tests would be scrapped.

At 0828, the US Navy helicopter SH60F launched MK54 torpedo serial number 54024 according to run plan 1036. As before, the men aboard the USS Memphis heard the splash of water entry and made the planned evasion tactics. As before, the sonar operators continued to listen for the sound of the engine start. As before, the observers in the range control house watched the display and saw the unit continue on a glide path to the bottom of the range. At 3:35 minutes from water entry, the distinctive sounds of the hull implosions were heard and the glide path altered itself to a greater angle of attack as the torpedo began to fill with water.

3.5 All Stop

With the failure of the second unit under seemingly identical conditions and circumstances, the planned testing of the MK54 torpedo was halted. Phone calls were made “up the chain” and the team at AUTEC hurriedly made plans to get back to Newport, Rhode Island. While the team prepared to exit Andros Island, senior leadership hastily made plans to convene a failure investigation “tiger” team meeting for Thursday, August 9.
4 The Investigation

4.1 NUWC Investigation

Two days following the incident, a tiger team was established. Membership included engineers and senior level management from NUWC Divisions Newport and Keyport, the prime contractor Raytheon, and the program sponsor from Washington DC. The tiger team was lead by the autopilot systems engineer and the manager of lightweight torpedo programs. It should be noted that the neither of the program safety engineers were included in the composition of the tiger team.

The team identified two critical functions that failed during the tests. The first was the failure of the unit to start. The second, and most damaging, was the failure of the onboard buoyancy system to deploy and return the torpedo to the surface for recovery. The process used for the investigation was to perform a systematic breakdown of the launch and buoyancy activation sequences and create a matrix of fault modes which would require follow on investigation to prove or refute the failure mode. In addition to the launch and recovery sequences, the team also focused on the quality aspect of each unit by examining the experience of the personnel responsible for testing and assembling the torpedoes and reviewing the procedures and build records.

The team noted a number of “firsts” associated with the AUTEC event:

- New software build for this test series
- First cross country transport for MK54 units
- First operational use after exposure to high heat and humidity
- First firings of MK54 with USN SH-60F fire control system
• First tests against manned targets (submarines)
• First tests in water deeper than crush depth

To identify any potential issues with the fire control interface, a series of tests were conducted using first a torpedo emulator, a specially instrumented torpedo and finally an actual torpedo. Throughout all of these tests, no interface issues were discovered. To refute the heat and transportation “firsts”, the remaining three units were tested and found to be operational.

4.2 Buoyancy System Failure

The recovery system failure was easily identifiable based on the limited evidence recorded by the AUTEC range facility. Since the torpedo’s range tracking system was functioning, it could be determined that battery power from the internal lithium thermal battery was present. A major flaw had existed in the recovery system since its creation. The fleet exercise section (FES), or recovery system, used the presence of torpedo power to determine if the vehicle was still operating. The premise of torpedo power was that once the engine stopped the alternator would stop spinning and the power would quickly extinguish.

The flaw came from the fact that the thermal battery that was used to power the electronics prior to engine start was diode-or’d to the alternator and provided sufficient power to the electronics for several minutes after the engine stopped. Since the thermal battery was essentially not loaded while the alternator provided power, the battery remained active but dormant until the voltage of the alternator was below the battery.
voltage. A look at the system requirement for the battery revealed that it was required to provide power for a minimum of 70 seconds from activation. The FES designers incorrectly interpreted this as a life expectancy measurement. Thermal battery manufacturers on the other hand are not typically concerned about how long the battery will last but rather with how many cells are required to meet the output voltage and rise time requirements.

Since the range tracking equipment was working and the torpedo did not start, it was presumed that the FES requirement for power was satisfied and there was no need to deploy the buoyancy system. The FES system was satisfied until the battery voltage went away, most likely, when the torpedo hull buckled when it reached crush depth. The sensing of torpedo power vice engine revolutions per minute (RPM) was known prior to the start of the AUTEC testing and had been identified as an outstanding issue. Due to time and budget constraints, a software change was made to the operational software to detect when the torpedo RPM level dropped to below 500. If low RPM were detected, a shutdown message would be sent to the FES requesting that the run be terminated and the buoyancy system activated. The RPM detection loop would begin monitoring RPM after water entry was sensed.

4.3 Engine Start Failure

The major focus of the team turned to the operational software changes and the engine startup sequence. Why focus on software and not some more tangible piece of "hard" evidence? Because software is the least understood mechanism of failure due to its inherent invisibility. The fact that software is logically brittle rather than physically...
brittle as hardware makes it more difficult to see how easily it can be broken. [12] The management of both NUWC and the Washington program office least understands the impact of software because none of them has had much exposure to the development process other to require that a process exist.

The engine start sequence for a Helicopter Attack Torpedo System (HATS) mode launch is a combination and sequencing of both physical and software interfaces. It is part state machine and part automatic timed sequence of events, all of which must be satisfied to start the engine. The engine start logic is classified as safety critical software due to its ability to create a hazardous event (engine start, propellers spinning). It should be noted that failure of the engine to start is not considered a safety precept.

The torpedo is connected to the launch platform fire control system through a breakaway cable. The term breakaway comes from the fact the cable does not release from the weapon until the gravitational force created as the torpedo is released “breaks the cable away”. The operator uses the fire control system to preset the weapon for initial tactics. Presets typically include the initial search depth and in the case of HATS mode the initial search bearing. Presets are sent to the weapon by applying power to various pins on the breakaway connector. The weapon in turn decodes the inputs, stores them in non-volatile memory and returns a weapon ready signal to the fire control system. If the helicopter is in position to fire, the weapon is now ready to start the launch process.

At time of launch, the operator closes the launch switch located on the fire control panel. This action starts three independent actions. The switch closure starts an automatic and irrevocable four-second delay. Once the four-second timer has expired,
the bomb shackles holding the weapon are released. Simultaneous to the starting of the timer, power is applied to Pins O, A and M on the breakaway connector. Pin O is used to fire the start squibs of the lithium based thermal battery that provides power to the weapon prior to engine start. Depending on the operator selections, the power on pins A and M will be decoded by the torpedo to determine what launch platform is being used. When a torpedo is started via the thermal battery (pin O), the state of pins A and M determine is the torpedo is being launched from a surface vessel torpedo tube (SVTT) or from a helicopter in HATS mode. If power on pins A and M is not present and the torpedo has been started by Pin O, then the torpedo decodes this as a SVTT casualty launch. A casualty launch is used when a surface ship launches a torpedo without presetting it in an attempt to get the torpedo out of the tube (and off the ship) as quickly as possible in an emergency. The SVTT casualty mode will result in a non-directed search (i.e. no initial search bearing). Figure 4-1 depicts the start sequence normally associated with an electric start (Pin O).

There is no tactical difference between the SVTT and HATS launch modes however, the engine start logic for each one is slightly different. In both modes the engine start sequence progresses through a series on safety interlocks that must be satisfied before the engine start command is given and power applied to the pyrotechnic squibs in the engine. The slight difference in engine start logic was eventually identified as a potential hole in the system’s design.

To meet the no inadvertent engine start safety requirement, the systems engineers developed requirements based on existing mechanical devices and the laws of physics. A
torpedo is launched from a SVTT by means of releasing high-pressure nitrogen into the rear of the tube, pushing the torpedo the same way a child would propel a spitball through a straw. The attitude measurement device of the torpedo senses the forward acceleration and the software logic uses this as the first interlock in the engine start logic. When the torpedo impacts the water, a negative acceleration is sensed and the requirement for the second interlock, water impact, is met. At this point the two mechanical interlocks, sea water sense and fifteen feet depth, are engaged when sea water makes contact across the exposed contacts of the sea water sensor and the hydrostatic switch closes at a depth of fifteen feet. The mechanical interlocks are not required to be sequential like the tube impulse and water impact interlocks are. Having met the interlocks, power is applied to the engine squibs and the combustion process begins.

In a HATS mode launch, all of the SVTT interlocks exist with the exception of the tube impulse requirement. When a torpedo is launched from a helicopter, it drops away after the holding shackles are released. While the attitude measurement unit senses the release from the platform, it was not considered to be of sufficient magnitude to be relied upon as an interlock. The engine start sequence for HATS begins at water impact.

As noted in Figure 4, the torpedo decodes the voltages applied to pins A and M to determine which mode the unit is being launched in. If there is no voltage on the pins when the torpedo processor scans the pins, the default mode is SVTT casualty. As can be seen in Figure 5, this results in a major flaw in the design of the engine start system. If the voltages to pins A and M are inadvertently removed during a HATS launch, the torpedo will think it is being launched in SVTT casualty mode and expect to see tube
impulse. Should this situation occur, the unit will be launched from the helicopter but
will not start due the engine start logic waiting for the tube impulse interlock to be
satisfied. The torpedo will continue to sink and as previously mentioned, the buoyancy
system will not command a shutdown since the thermal battery is supplying power to
simulate engine on. This was considered by the NUWC investigative team to be the most
likely cause of what happened at AUTEC. Repeated testing of the torpedo and the
helicopters involved could never create this failure mode. The mode was real and was
simulated but never proven.

Since the design deficiency of the buoyancy system was known prior to the start
of the AUTEC tests, a software “fix” was implemented to identify when the engine had
stopped operating. The electronics, once powered up by the thermal battery, would issue
an under-speed shutdown for situations when the RPM had dropped to below 500. The
logic was that even if the engine did not start, the processor would recognize this fact and
issue a shutdown command to the FES. The flaw in the logic was realized later when an
analysis of the code revealed that the RPM check routine was triggered by the sea sense
flag and not sea sense status. Sea sense flag is set during the engine start sequence,
immediately after the water impact interlock is met.
Operator Presets Weapon

Weapon Decodes Presets "Weapon Ready"

Operator Closes Launch Switch

Four (4) Second Delay

Apply Power To Pin O

Apply Power To Pins A & M

Weapon Released from Platform

Fire Thermal Battery Squib

Power Supplies within Spec

Reset Processor

Decode A & M

A = 28, M = 19 Mode = SVTT

A = 28, M = -19 Mode = HATS

A & M = 0 Mode = SVTT Casualty

A

B

C

Figure 4 Launch Mode Decoding

Massachusetts Institute of Technology – System Design and Management
Sea sense flag checks the status of sea sense status, which is based on the actual sea sense hardware and is not conditional. The systems engineer who created the requirement identified the wrong sea sense logic bit to monitor. Since it is speculated that the torpedoes were launched in SVTT casualty mode and where waiting for tube...
impulse, the sea sense flag was never set because it was further down stream in the processing logic.

4.4 No Fault Found

Although a flaw was found in the logic of the casualty launch mode that would potentially explain why the two units never started at AUTEC, a series of tests on the actual helicopters used could not reproduce the failure mode. A number of successful launches were conducted with special instrumentation but in no instance did the voltages on pins A and M appear out of the required levels.

The final recommendation from the investigating team was one of “no fault found” with respect to the engines not starting. With respect to the buoyancy system, the recommendation was to monitor the actual engine RPM vice the torpedo power. The rationale was that it was imperative that the unit be returned to the surface should another no start condition be encountered.
5 A Hierarchical Approach to Causality

Accidents rarely have single causes and specifying all necessary conditions may be impractical. [13] The purpose of the MK54 investigation was to identify the root cause of the failure and determine what changes were necessary to ensure that a repeat failure did not occur. While a great deal of testing of the performance of the torpedo can be achieved via simulation, the non-homogeneity associated with the ocean and the physical boundaries make simulation an unrealistic way of measuring the effectiveness of the weapon under real world conditions. With the AUTEC failure, the concern was centered on the possibility of the existence of a systemic problem with the launch sequencing (both software and hardware). Since the units were not recoverable to accomplish a post mortem, all planned launches of the MK54 were cancelled pending the outcome of the investigation. Without in-water tests and the associated data, systems and software development efforts were also temporarily halted.

Leveson proposes that to prevent future accidents the investigation must be carried out on multiple hierarchical levels including technical, human, organizational, and regulatory perspectives. [14] Figure 6 is the Lewycky hierarchical model of accident causes used by Leveson to illustrate the layers of causality. [15]
The problem encountered with the AUTEC investigation was that it was centered entirely on the technical and human aspects of the incident since these parameters are easily understood by engineers. Organizational and regulatory constraints require a holistic approach to failure analysis and oftentimes lead to root causes that management does not like to accept. Blame is more likely to be placed on operator errors or on a specific component than on management deficiencies. [16] The so-called quick fix typically does not address the root cause of the problem but rather a causal factor.

Level 1 of Figure 6 addresses the mechanisms of the accident. In the case of the AUTEC accident, the chain of events associated with the launch process. Level 2 identifies the conditions or lack of conditions that have led to the accident. Failure to due to the temperature extremes or the vibration levels induced from the cross-country trip or being attached to SH60F helicopter are conditions associated with the MK54 failures. Level 3 addresses the constraints or lack of constraints introduced by technical, physical, social, managerial, organizational, governmental or human conditions. It is at this third
level that the failure analysis should climb to properly identify the root cause or most likely causes. Root causes left untended, will in all likelihood, result in future failures. Leveson divides the root or level three causes of accidents into three categories: (1) deficiencies in the safety culture of the industry or organization, (2) flawed organizational structures, and (3) superficial or ineffective technical activities. [17] The following sections use these three categories as lenses to look at the AUTEC failure from aspects not identified by the engineering community at NUWC.

5.1 Flaws in the Safety Culture - Priorities

The term safety is prevalent in all aspects of weapon systems, regardless of what country is the developer or what potential damage an accident could cause. Safety culture, as described by Leveson, is the general attitude and approach to safety. The US Department of Defense attempts to establish this culture through requirements of standards such as MIL-STD-882B. [18] This standard outlines tasks that must be described in the program contract to satisfy Department of Defense regulations for system safety. The tasks are separated into three areas: management, system design and software. Standards such as this do not require specific techniques but rather describe what must be achieved to satisfy the DoD requirements.

The use of standards does not guarantee that the system under development will receive equal amounts of attention from those involved. At NUWC and at the program office level in Washington, DC, the importance of safety is not equally distributed amongst all the programs. The submarine launched, or heavyweight, torpedoes receive the lion’s share of safety priority and funding compared to the above surface launched
lightweight torpedoes. This stems from two facts: (1) the potential for loss of life and property is much greater with a heavyweight torpedo due to the sheer size differential in explosive power (approximately 6 to 1) and (2) program managers in the Washington, DC office are typically captains in the submarine force.

The military, like society, is comprised of a number of subcultures. In the US Navy, the submariners are considered by most (especially themselves) to be the elite corps. Being on board a submarine, hundreds of feet below the surface, is not a situation that most people will encounter. Crewmembers must rely on each other and the machinery to ensure that they will return to the surface after completing a mission. Should a mishap occur while at sea, the outcome would most likely be disastrous and result in the loss of several lives and a billion dollars worth of equipment.

Contrast the submariner’s priority for safety with that of the surface navy. While accidents can occur, the potential for the loss of all life onboard as well as the loss of the entire ship is perceived to be not as great. The lightweight torpedo is a fire and forget weapon with a destructive capability aimed at submarines. If something goes wrong during the launch process, the operator has the ability to jettison the weapon with little regard for potential damage if the unit attacks the firing ship. While precautions are built into the torpedo to prevent own-ship attack, the damage would be much less than that caused by a submarine launched weapon.

The difference in priorities is most notable in the approval process used to release software. While the processes associated with the development of the software are identical, a software release for the heavyweight torpedo must go through a Mission
Control Panel (MCP) chaired by a Rear Admiral in the US Navy. The MCP will evaluate the changes made to the software and will review the adequacy of testing and the test results. The final release for Lightweight torpedo software on the other hand, is through a Test Control Group (TCG) chaired by the chief engineer (a civilian) in the Torpedo Department at NUWC. The TCG, like the MCP, reviews the changes and the associated testing of the new software version. The heavyweight torpedo software must also go through the TCG but that is just a checkpoint on the way to the MCP.

The lower priority given to the MK54 program and lightweight torpedoes in general is in itself not a root cause. What it does though is establish an attitude or cultural bias, that when combined with organizational and human factors, can lead to complacency with respect to safety’s role in the organization and the project.

5.2 Organizational Structure

Safety is no different from other components of a development program when it comes to such basic management principles as clear lines of communication, responsibility and accountability. The success or failure of these principles is often dependant on the organizational structure that houses the members of the development team. To understand how a program functions, a good starting point is to identify the organizational structure that encompasses team members. The torpedo department at NUWC is a balanced matrix organization aligned by functionality. A balanced matrix is creates a sharing of power between functional managers and the program manager / team leader. [19] The team leader has control over how an individual’s time is to be spent and
the functional manager is responsible for the team member’s professional growth and development within the company. [20]

Figure 7 depicts the balanced matrix organization of the torpedo department and highlights how the MK54 team cuts across functional boundaries. It is important to note that the safety component of the team does not reside within the organizational confines of the torpedo department. The intent of the separation is to ensure that safety is an independent team member, unaffected by any political overtures from the torpedo department. The Rogers Commission on the Challenger disaster stressed this point in one of their findings on the safety program that was in place at NASA. They found that the organizational structures had placed safety, reliability and quality assurance offices under the supervision of the very organizations and activities whose efforts they were to check. [21]
The problem that can manifest itself from this “independence” is a separation in collaborative efforts with the development team. Organizations that require high levels of lateral communications, coordination and rapid problem solving must allow for multiple opportunities for social and task-related interactions to develop among individuals and groups that would not normally interact if traditional bureaucratic rules or hierarchical reporting structures prevail. [22] Unless the entire team is collocated, which, given the global make-up of most teams today is nearly impossible, team members that are not in the same organizational unit will tend to not be collocated. This is typically due to concerns about a lack of space or permanent office, lack of status in the functional organization or from functional managers concerned about losing control.

At NUWC, the core of the MK54 development team is made up of the systems, integration engineers, and the program manager. They are collocated with adjoining offices and are located in the same office building with other members of the team, most importantly the software engineers. The safety engineers, who are not in the Code 81 torpedo department, are located with other members of their organization in a separate building, approximately 200 yards away. Figure 8 is from Professor Tom Allen’s quantification of the effect of distance on technical communications. The graph shows that technical communication is much more likely to occur between team members if they are located close together. [23]
While a strong case can be made for the independence of the safety organization, care must be taken not to make the independence a deterrent to communications and the decision making process. All design changes, including software and hardware, made within the MK54 program, include safety in the review cycle. It is clear however that the quality of these reviews is contingent on the systems knowledge of the safety engineer. At NUWC, the independence in both organizational reporting and physical location has created a safety team well versed in the machinations of the safety requirements such as the Weapon System Explosives Safety Review Board (WSESRB) but weak in practical knowledge of the system under development. The apparent holes in the engine start sequence and the low RPM shutdown commands were caught after the fact by the systems and not the safety engineers. The requirements were not complex but required a working knowledge of how the system works to determine the adequacy of the design.
The lower priority of safety identified in section 5.1 helps contribute to the organizational separation experienced by the MK54 program. This is magnified in section 4.1 which stated that personnel from the safety organization were not part of the investigative team. The lower priority and physical/organizational separation further exacerbate the low level status of safety personnel and limit their potential for being considered as effective members in the decision making process.

5.3 Ineffective Technical Activities

Leveson defines a third group of level-three factors to be related to the poor implementation of activities necessary to achieve an acceptable level of safety. These factors can include superficial safety efforts; ineffective risk controls; failure to evaluate changes and failure to collect, record and use safety information. [24]

The technical activities of the MK54 program are governed by a System Safety Program Plan (SSPP). The objective of the SSPP is to establish a program that will assure the early identification and elimination or effective control of hazards. [25] The main thrust of the SSPP is the identification of hazard categories and safety precepts that guide the MK54 safety program and personnel. System safety precepts are established to ensure that safety features and considerations are designed directly into the system and are consistent with overall program objectives. Table 5-1 lists the hazard classifications and Table 5-2 lists the safety precepts.
<table>
<thead>
<tr>
<th>Description</th>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CATASTROPHIC</td>
<td>I</td>
<td>Death. Loss/severe damage to launch platform/target ship/IMA/Depot. Severe environmental damage.</td>
</tr>
<tr>
<td>MARGINAL</td>
<td>III</td>
<td>Minor injury. Minor occupational illness. Minor damage to launch platform/target ship/IMA/Depot. Loss/damage to Mk 54 Mod 0. Minor environmental damage.</td>
</tr>
<tr>
<td>NEGLIGIBLE</td>
<td>IV</td>
<td>Less than minor injury. Less than minor occupational. Less than minor damage to launch platform/target ship/IMA/Depot. Less than minor damage to Mk 54 Mod 0. Less than minor environmental damage.</td>
</tr>
</tbody>
</table>

### Table 1 Hazard Classifications

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inadvertent arming/detonation of the warhead (warshot torpedo only) - Positive safety features must include multiple depth measurement units.</td>
</tr>
<tr>
<td>2</td>
<td>Inadvertent actuation of the Buoyancy Subsystem (BSS)/Fleet Exercise System (FES) (exercise torpedo only)</td>
</tr>
<tr>
<td>3</td>
<td>Inadvertent launch and/or motor start</td>
</tr>
<tr>
<td>4</td>
<td>Own ship attack - Positive safety features must include the following: The software/hardware design will inhibit the torpedo from accepting and executing a Periscope Depth Attack (PDA) preset when launched from a Surface Vessel Torpedo Tube (SVTT) in the Non-Directed Search (NDS) Mode. The design shall incorporate the use of multiple independent depth sensors. Also, a safety barrier shall be implemented for Directed Search when PDA is selected.</td>
</tr>
<tr>
<td>5</td>
<td>Personnel injury or launch platform damage during torpedo firing operations A positive mechanical interlock shall preclude initiation of the weapon prior to clearing the launch platform. The launch/weapon interface shall allow safe jettison.</td>
</tr>
<tr>
<td>6</td>
<td>Personnel injury or equipment damage during handling, transportation, maintenance, testing or demilitarization operations. Positive safety features must include the following: The Mk 54 Mod 0 design shall incorporate the use of squib shorting plugs for the igniter, CO2 and fuel valve squibs. Shipping container shall meet the Performance Oriented Packaging (POP) Criteria. The Mk 54 Mod 0 design shall provide means for the torpedo, and its shipping and storage accessories to prevent and/or contain the release of hazardous materials.</td>
</tr>
</tbody>
</table>

### Table 2 Safety Precepts

*Massachusetts Institute of Technology – System Design and Management*
What is important to realize when looking at the precepts is how safety is concerned with the level I and II hazard conditions. This is critical to the causal investigation because Level III hazards, which include loss or damage to the MK54 torpedo, are not addressed by the safety precepts and ultimately are not addressed when the hazard analyses were done! Considerable efforts are made to ensure that the motor and the buoyancy system do not inadvertently activate, causing potential life-threatening situations, but the same efforts are not applied to the converse. An engine that does not start or a buoyancy system that does not deploy cannot create a hazardous situation to the operator or the ship. While programs are being asked to do with less funding, it is imperative that the hazard classifications be updated to reflect the potential financial loss and added risk to the overall health of the program.

If a failure to start the engine or deploy the buoyancy system were listed in the safety precepts (and elevated to a classification of II) then a Fault Tree Analysis (FTA) would have been completed by the safety engineer and provided to systems engineering review. While the FTA does not identify a hazard, it does provide focus on potential events that may cause a hazard. A simplified FTA with the top-level hazard identified as “Engine does not start” is shown in Figure 9. What the FTA does is to focus attention on the “Interlocks not Met” event. This event should still be further broken down using the engine start logic of Figure 4-2. If done completely (and by a competent safety engineer) the FTA would have identified the fault associated with the tube impulse interlock. However, since the safety precepts never included the top-level event of not starting the engine, the FTA was never done.
Another example of an ineffective technical activity is the reliance on software to overcome the shortfall of the buoyancy system. As was previously mentioned, the buoyancy system could not properly detect when the engine stopped, so a number of software shutdowns were added to compensate. At a high level this seemed to make
sense since the torpedo software measured the engine speed and could easily issue a shutdown command if the RPM level dropped too low. This also seemed to be an attractive fix to management because it could be implemented at nearly no cost (compared to the $100,000 needed to fix the hardware) and could be done in nearly no time (compared to the three months estimated for the hardware fix). Clearly, it can be seen that the versatility, speed and cost of the software solution became too appealing to management. Unfortunately, this fix was not given the proper analysis and the subtlety between sea-sense status and sea-sense flag was not caught. However, it should be noted that due to system complexity, software should not be used to offset known deficiencies in hardware systems.

5.4 Schedule Issues or a False Sense of Security

As noted in section 4-1, the tests at AUTEC featured a number of first time events. The two most glaring are the first time operation from US Navy helicopters and the first time operating in waters deeper than crush depth. Both were the result of schedule compression.

The MK54 program is schedule driven, with the end date anchored to March of 2003. The anchor is an event called Initial Operating Capability (IOC) and tied to it are millions of dollars slated for production. IOC approval determines that the weapon meets the requirements and is recommend for full rate production.

Like most programs, the MK54 had its share of development problems. The premise of shortened software development times because of the reuse of existing
software from the ADCAP and ALWT programs never materialized. In fact, the complications associated with merging the ALWT algorithms into the ADCAP software structure added nearly a year to the software development tasks. To help mitigate schedule delays, the at sea testing schedule was maintained by using assets available at the time. One of these assets was a torpedo-launching device that would allow a commercial helicopter to carry and launch a torpedo. Since this device was always available, as was the commercial helicopter, it was used extensively to conduct testing instead of trying to schedule a fleet asset.

The launching workaround, coupled with the software change to make up for the buoyancy system deficiency allowed the program to meet major program milestones. Nevertheless, as can be seen from the previous discussions, meeting the schedule milestones was not a true indicator of the technical health of the program. Disaster was just around the corner, waiting for an opportunity to expose the programmatic decisions already made.
6 Findings of Hierarchical Analysis

The hierarchical approach to causality is a method of taking an unbiased systems approach to failure or accident analysis. The key to this approach is to look beyond the typical mechanisms of failures, or “smoking guns”, to find the root causes. Left unresolved, root causes provide the potential for future mishaps.

At the beginning of this research, the aggressive schedule and minimal budget were the presumed root causes. While both are part of the root causes, schedule and budget acted as accomplices to other, deep routed issues.

6.1 Finding #1 – Low Priority of the Safety Program

Due to the cultural differences between the submarine and surface ship Navy, the MK54 safety program had a bias towards low priority. This is evident in the software approval process/chain used by submarine launched torpedoes compared to surface launched torpedoes like the MK54. Whereas the submarine launched torpedo software is approved by a two star admiral, the MK54 software is approved a civilian engineer.

This bias is also exacerbated by the destructive potential of the two types of torpedoes and the launching procedures. The net effect of the lower priority of safety is an underlying false sense of security throughout the entire MK54 development team. A sense of security that eventually finds it way through each finding of this investigation.

6.2 Finding #2 – Organizational Factors and Lack of Communications

These two root causes are consolidated because they have a cause and effect relationship. The torpedo safety organization is separate from the development
organization to ensure that the engineers have an independent voice in decision-making. Conceptually this is an excellent idea since the goals of the developing organization are typically driven by cost and schedule constraints. An independent safety organization allows for critical analyses without fear of retribution.

However, independence can also lead to a breakdown in communications, especially if the safety team members remain physically located with their organizational constituents. The 1977 work of Professor Tom Allen still holds true twenty-five years later in spite of developments such as e-mail and teleconferencing. A project with severe schedule constraints requires that the team members with decision-making capability be collocated. This ensures that information flow is continuous and daily and leads to a team with members who are cognizant of nearly all decisions and issues. The lower priority given to safety coupled with the physical separation of the safety team members resulted in a classic case of “out of sight, out of mind”. Without continuous inputs from the safety organization, the MK54 systems engineers eventually relied upon themselves to be responsible for safety, even during the failure investigation.

The capability to react quickly to changes on the project requires decentralizing control down to the team level. [26] In projects with compressed schedules, decision-making must be located at a level in the organization that has sufficient bandwidth or capacity to process them quickly. It is critical to deploy talent of the organization down in the trenches where the decisions are intended to be made. [27] If the functional organizations retain the most competent people and don’t allow them to become members
of the team, decision making will either be poor due to their inexperience / expertise or non-existent due to reluctance.

6.3 Finding #3 – Misapplication of Hazard Criteria

Tables 1 and 2 provide a list of the MK54 hazard classifications and safety precepts respectively. The hazard classifications were taken from previous torpedo programs. Table 1 emphasizes death, injury, environmental damage and loss/severe damage to launch platforms and targets as the major categories of hazards. Because of this, the issues of not starting the engine or not activating the buoyancy system were not included in the hazard/failure analyses conducted by the safety organization.

As budgets continue to decrease and eventually begin to shape programs, the physical loss of development hardware because increasingly critical. The budget for the MK54 allowed for the construction of twenty-one development units. Losing two at AUTEC was nearly 10% of the inventory and 3% of the total budget. Hazard classifications should not be reused from program to program but rather should be developed on a program-by-program basis to ensure that the risks are properly identified.

6.4 Finding #4 – Tight Coupling of Interfaces

The schedule of the MK54 program was milestone driven with a fixed end date. As situations and problems arise, the fixed end date creates schedule compression. To alleviate pressure and meet interim milestones, the program elected to use surrogate launch platforms to conduct tests. Conditions leading to hazards emerge in the interfaces between subsystems of a complex system. [28] Analysis shows that errors in identifying
or understanding functional and interface requirements frequently lead to safety-related software errors. [29]

The MK54 program used an artificial interface to meet schedule constraints. It was not until testing was conducted in deep water did the actual launch platform come into test. Although the surrogate launch platform was “functionally equivalent”, it was not representative of the complex US Navy SH60F helicopter. A popular slogan in the US Navy torpedo community is “train with what you fight with and fight with what you train with”. Unfortunately, this was not the case for the MK54 program.

### 6.5 Finding #5 – Don’t Use Software to Repair a Hardware Deficiency

The last finding is also the most damaging. The consensus of the Presidential Commission on the Space Shuttle Challenger Accident was that the loss was caused by a failure in the joint between the two lower segments of the right solid rocket motor. [30] While photographic evidence taken during the launch pointed the investigation in the direction of the solid rocket motor, it was the physical evidence recovered from the ocean floor that led the consensus decision.

The design deficiency of the buoyancy system was known prior to the AUTEC tests. Software requirements were added to alleviate the concern with the inability of the buoyancy system to properly monitor the engine status. Software was used because it was the most cost and schedule effective solution. Ultimately all of the evidence of why the torpedoes did not start ended up on the bottom of the ocean. Without physical evidence, the actual cause of the failure may never be determined.
7 Conclusions

What comes into focus when reviewing the major findings produced by the hierarchical causality analysis is that none of the findings is torpedo specific. The causal factors are similar to those found in the Rogers Commission report on the Challenger Accident. Both accidents suffered from forms of complacency: the Challenger in the form of solid rocket booster joint problems and the MK54 in the form of the overall priority of safety. The Challenger and the MK54 programs both suffered from management structure issues revolving around system safety. The Challenger program was cited by the Rogers Commission for lack of an independent role for safety. The MK54 program, with an independent safety role for safety, should be cited for not successfully integrating system safety into the decision making process. A parallel causal factor could also be drawn between the criticality rating of the o-ring problem and the hazard classification of damage/loss to the MK54 torpedo.

The Therac-25 is a well-documented case of accidental death caused by a misapplication of software in an updated version of a medical linear accelerator. [31] Since the circuitry of the buoyancy system did not properly sense when the engine stopped, the MK54 relied on software to make the decision. The Therac-25 used software to simplify the design and replace safety functions previously done with protective circuits. Both efforts suffered from software design flaws: the casualty launch mode in the MK54 and the race condition in the Therac-25. Leveson states that virtually all complex software can be made to behave in an unexpected fashion under some conditions. [32]
The theme at the outset of this research was to investigate the dynamic tension created by the increasing complexity of systems and the reduced development times and budgets. The research surmised that this tension would result in flawed management and technical decisions resulting in the increased potential for accidents and failures. The results of the research into the MK54 failure and other more well known incidents reveal that schedule and budget pressures are having a negative effect on the decision making process of management. Software, and its ability to be rapidly (and often inexpensively) changed, has become a panacea for today’s system development problems. The “do more with less” mentality has made the short term solution the solution of choice. Senge sums up the problem associated with short term solutions:

A short term solution is used to correct a problem, with seemingly positive, immediate results. As this correction is used more and more, more fundamental long term corrective measures are used less and less. Over time, the capability for the fundamental solution may atrophy or become disabled, leading to even greater reliance on the symptomatic solution.

Peter M. Senge – The Fifth Discipline [33]

Software is a disruptive technology that should be viewed and used as a systems tool and not a panacea. Foundations of a successful (and safe) program must still include fundamental precepts such as proper organizational structure, lines of communication, management commitment, and adequate priority given to safety. Schedule and budget compression will continue to be the norm for development programs but the overarching focus must be on the long term implications of the system.
8 References


[14] Ibid, page 48


[20] Ibid, page 144


[27] Ibid, page 191


Appendix A Executive Summary

Hierarchical Causal Accident Analysis of a Complex System

By

David G. Bancroft

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

Masters of Science in Engineering and Management

at the

Massachusetts Institute of Technology

May 2002

Signature of Author

David G. Bancroft
System Design and Management Program

Certified by

Nancy Leveson
Thesis Supervisor
Professor of Aeronautics & Astronautics and Engineering Systems

Accepted by

Steven D. Eppinger
Co-Director, LFM/SDM
GM LFM Professor of Management Science and Engineering Systems

Accepted by

Paul A. Lagace
Co-Director, LFM/SDM
Professor of Aeronautics & Astronautics and Engineering Systems

Massachusetts Institute of Technology – System Design and Management
Problem Statement

The 1990’s ushered in a change to the political landscape with election of a Democratic president and the loss of the DoD’s most prominent enemy – the Soviet Union. Along with these changes came a realization that DoD programs would no longer operate like ravenous bears, devouring billions of taxpayer dollars without regard. A wave of acquisition reform came crashing over the walls of the Pentagon and suddenly programs were required to espouse concepts such as software and hardware reuse, Commercial Off The Shelf (COTS), and earned value measurement systems to be considered for approval.

While the challenges facing previous U.S. Navy programs were for the most part technological in nature, the challenges and success of today’s programs are measured from the big three: cost, schedule and performance. The reduced timelines and budgets draws attention to the fact that while today’s managers are required to “do more with less” it is not clear if developments in management have allowed them to accomplish that. Systems being developed today are sometimes orders of magnitude more complex than those developed twenty years ago, due largely in part to advancements in software engineering. Yet, this rapid rise in complexity has not been offset with increased timelines and budgets, but rather offset with a greater acceptance of risk, both perceived and unknown.

On August 7, 2001, off the waters of the Bahamas, two developmental MK54 torpedoes were permanently lost, each carrying an estimated value of one million dollars. Such an event would have hardly raised an eyebrow had this happened to the large-scale torpedo programs initiated in the 1980’s, but to the MK54 program, outfitted with 6% of the budget and 70% of the schedule of previous torpedo programs, it was nearly fatal. This thesis uses that accident to examine the technical, human, organizational and regulatory components of the US Navy’s torpedo enterprise in attempt to identify the root causes to prevent future occurrences and reduce unforeseen risk.

Originality Requirement

This thesis meets the requirements of an original investigation by conducting an accident analysis of a complex system using principles and methods acquired while in the SDM program at MIT.

This research looks at causality through the lenses of a three-tiered hierarchical model of the system and the accident. The hierarchical approach to causality is applied to an undersea weapons program currently under development by the US Navy. This program experienced a catastrophic failure, which nearly resulted in the cancellation of the program. The hierarchical approach to causality investigates the entire enterprise, not limiting itself to the technical mechanism typically associated with failure analyses. This analysis results in a critical look at the principles, methods and tools used by the Naval Undersea Warfare Center.
Content and Conclusions

While the US Navy does not have a well-known slogan similar to NASA’s “better, faster, cheaper”, the Navy has undergone a similar paradigm shift due to the fall of the Soviet Union. The goal of this thesis is to consider that paradigm shift with respect to the perceived additional risk that comes from smaller budgets, shortened development times and increased complexity due to technical innovations. This thesis uses the US Navy’s MK54 lightweight hybrid torpedo program as a case study for three important reasons: (1) the MK54 program is being developed in the post Soviet Union era of acquisition reform; (2) the program suffered catastrophic failures during development; and (3) the author is the program manager of the program.

The failure analysis of the aforementioned catastrophic failure, conducted by the engineering community of the Naval Undersea Warfare Center, resulted in a finding of “no fault found”. This finding was due in part to the absence of a “smoking gun” and is a finding that can typically be attributed to an investigation conducted by engineers who limit their exploration to the technical matter at hand.

The hierarchical approach to causality resulted in a different conclusion to the accident and has provided the author with a number of lessons learned that will be promulgated to upper management. Unlike the Challenger space shuttle accident, no single cause of failure (or O-ring) was found by this research, but like the Challenger investigation, a number of root causes are identified.

The hierarchical causality model of the accident revealed that previous program delays had yielded a development schedule without slack and because of this, a number of “first” events occurred at the time of launch. The most significant “firsts” were the first use of US Navy helicopters with associated fire control systems and the first time in waters deeper than the outer hull crush limit. The former may have caused the failure; the latter disposed of any evidence.

Additionally, the hierarchical research identified a number of other issues: organizational differences in the priority given to safety; the independence and subsequent communication failures between system engineering and safety engineering; the reliance of software to make up for a hardware deficiency; and the focus of the safety program.

Most damaging of all the issues was the use of software to overcome a known hardware design deficiency. The decision to use software was a conscience one and made to meet the cost and schedule goals of the program. Unlike the hardware problem however, the complexity of the system and the software was not fully understood and yet the decision was made to alter the software because it was easy to accomplish. Software has become for short term solution for potentially long term problems.
System Design and Management Principles

The research relied heavily on the concepts learned and materials provided by the SDM program at MIT. In particular, the pedagogy of Systems Architecture referenced the principles of holistic thinking, complexity and pseudo-regulatory influences on the upstream process. Additionally the concepts of organizational structure and knowledge sharing/transfer learned in System and Project Management and Organizational Processes respectively were key to the research. Finally, Professor Leveson’s Advanced Software engineering class was the catalyst to the research, exposing the author to the importance of safety and its implications in the project development process.

Engineering & Management Content

Using the knowledge acquired through years of system development experiences and through the education experience of the SDM program, a hierarchical causality analysis was done on an accident involving a complex military system. The ability to take a holistic view of the accident, the system and the organizational structure required working knowledge of system architecture (hierarchy, complexity, interfaces), system engineering (requirements definition, risk benefit analysis, fault tree analysis) and project management (schedule compression, risk) concepts.

The construction of the fault tree to analyze the launch platform to weapon interface required an extensive use of the author’s electrical engineering background and years of torpedo systems engineering experience. The interface is a complex synthesis of software, timing and power requirements coupled with unique physical constraints placed on the launch platform and weapon. Additionally, the failure analysis of the buoyancy subsystem also required use of the author’s system level knowledge of torpedoes and recovery systems.

Statement of Authorship and Originality

The work performed to write this thesis is the author’s, and is original.
Appendix B List of Acronyms

ADCAP   Advanced Capability
ALWT    Advanced Lightweight Torpedo
ASW     Anti-Submarine Warfare
AUTEC   Atlantic Undersea Test and Evaluation Center
CMM     Capability Maturity Model
COTS    Commercial Off The Shelf
DoD     Department of Defense
DC      District of Columbia
DS      Directed Search
FES     Fleet Exercise Section
FTA     Fault Tree Analysis
HATS    Helicopter Attack Torpedo System
IOC     Initial Operational Capability
LHT     Lightweight Hybrid Torpedo
MCP     Mission Control Panel
MIT     Massachusetts Institute of Technology
NASA    National Aeronautics and Space Administration
NDS     Non-Directed Search
NUWC    Naval Undersea Warfare Center
RDTE    Research, Development, Test and Evaluation
RPM     Revolutions Per Minute
SDM     System Design and Management
SONAR   Sound Navigation and Ranging
SSPP    System Safety Program Plan
SVP     Sound Velocity Profile
SVTT    Surface Vessel Torpedo Tube
TCG     Test Control Group
TOTO    Tongue of the Ocean
WSES RB  Weapon System Explosives Safety Review Board
Appendix C Engine Start Sequence Documentation

3.2.2.11 (U) SVTT

(U) This function performs the launch sequence for an SVTT launch. The SVTT launch is defined as a surface ship launch in either Directed or Non-Directed search.

(U) In an SVTT launch the torpedo has the opportunity to initialize its Attitude Reference System while on the ship. This allows the Autopilot to execute pullout (MODE 1).

(U) An INTERLOCK, as used in this paragraph, is a requirement that must be met for engine start to occur. Should an INTERLOCK not be satisfied the engine will never start. The sequence of the INTERLOCKs ensures a single point of failure (SPOF) will not cause premature engine start. Each INTERLOCK is designated.

(U) Each INTERLOCK shall be executed in the order provided. Requirements for an INTERLOCK shall not be sought until the previous INTERLOCK has been satisfied.

(U) PROCESSING

(U) 1. [02-0012-0001] The program shall perform the Send Autopilot Messages function of Perform I/O Processing to send LW_INITIALIZATION_MSG_HI and the FIRE_CONTROL_DATA_MSG_HI to the Autopilot.

(U) 2. [02-0012-0002] The program will wait for the successful acknowledgment of both the LW_INITIALIZATION_MSG_HI and the FIRE_CONTROL_DATA_MSG_HI (i.e., ap_received_fire_control = TRUE) via the Receive Command Status Function.

(U) 3. [02-0012-0003] Wait for the AMU to be stable and ready (AMU_STABLE_TIME), then calculate quaternion presums for 200ms. The Process Inertial and Quaternion Data function shall calculate the quaternion presums.
(U) 4. [02-0012-0004] The program shall perform the Send Autopilot Messages function to send the QUATERNION_PRESUM_DATA_MSG_HI to the Autopilot.

(U) 5. [02-0012-0005] The program shall wait for successful acknowledgment of the quaternions. Upon receipt of the LW_COMMAND_STATUS_DATA_MSG_AP where quats_init_flag = TRUE, then the Hybrid Interface will send the SENSOR_DATA_MSG_HI every 20ms.

(U) 6. [02-0012-0006] Inform the platform that the torpedo is ready for launch by setting ready_to_launch_cmd = TRUE.

(U) 7. [02-0012-0008] In a ship board launch the first engine interlock is the tube impulse acceleration (INTERLOCK 1).

If there is TUBE_ACCEL_X acceleration in the X direction (i.e., amu_xaxis) for 60ms then

Set tube_acceleration_flag = TRUE.
    go to step 8
else
    continue checking for this interlock
end

(U) 8. [02-0012-0009] The second interlock looks for the deceleration at water entry. The nose of the torpedo should impact the water with sufficient force to fulfill this interlock (INTERLOCK 2).

If there is a 40ms period where the amu_xaxis is less than NOSE_IMPACT_X or |amu_yaxis| > NOSE_IMPACT_Y then
Set nose_impact_flag = TRUE
    go to step 9
else
    continue checking for this interlock
end

(U) 9. [02-0012-0011] If the torpedo has reached the minimum depth for engine start; when the depth switch input is true (i.e, switch_15ft_status = TRUE), the DSA input is at least 5 feet (i.e., 5ft < depth_hi ft), and the sea sense indicator in the Lanyard Start Assembly (LSA) indicates the presence of sea water (i.e., sea_sense_status = TRUE) for 200ms then (INTERLOCK 3 & 4)

Set minimum_depth_flag = TRUE and sea_sense_flag = TRUE when their respective requirement is met.
Start the engine.

a. Set the \textit{engine\_start\_permit} = TRUE.
b. Set the \textit{co2\_squib\_cmd} = FIRE.
c. Wait for 60ms
d. Set the \textit{co2\_squib\_cmd} = FALSE.
e. Set the \textit{ignitor\_squib\_cmd} = FIRE
f. Wait for 60ms
g. Set the \textit{ignitor\_squib\_cmd} = FALSE
h. Repeat steps b-g once more.

\textbf{else}

continue checking for this interlock

\textbf{end}

(U) 10. [02-0012-0018] The following events shall be sought simultaneously:

(U) a. [02-0012-0012] If the torpedo has reached a depth (i.e., \textit{depth\_hi}) greater than \textit{INITIAL\_DESCENT\_DEPTH} for 200ms, then set the \textit{initial\_descent\_complete\_flag} = TRUE. This flag is used in the maintain safe operation function to determine if the torpedo has reached sufficient depth within an acceptable time.

(U) b. [02-0012-0013] If the engine speed (i.e., \textit{r\_p\_m}) has reached 1000 rpm for 200ms, then the fins shall be unlocked and the Autopilot will begin the pullout maneuver. Power can now be applied to the forward electronics.

(U) -1- [02-0012-0014] Set the \textit{engine\_on\_flag} = TRUE.

(U) -2- [02-0012-0015] Unlock the fins by setting \textit{enable\_fins\_cmd} = TRUE and \textit{fins\_unlocked\_flag} = TRUE.

(U) -3- [02-0012-0016] Set the \textit{launch\_status\_2\_flag\_hi} = TRUE,

(U) -4- [02-0012-0017] Apply the forward power by setting the \textit{forward\_power\_cmd} = TRUE and \textit{forward\_power\_flag} = TRUE. Set \textit{forward\_power\_on\_time} to the current time.

(U) -5- [02-0012-0019] Set \textit{ls2\_time\_hi} to the current time.

\texttt{engine\_start\_permit: data\_out}
\texttt{nose\_impact\_flag: data\_out}
minimum_depth_flag : data_out
sea_sense_flag : data_out
initial_descent_complete_flag : data_out
launch_status_2_flag_hi : data_out
fins_unlocked_flag : data_out
enable_fins_cmd : data_out
engine_on_flag : data_out
forward_power_cmd : data_out
forward_power_flag : data_out
forward_power_on_time : data_out
ready_to_launch_cmd : data_out
tube_acceleration_flag : data_out
c02_squib_cmd : data_out
ignitor_squib_cmd : data_out
breakaway_flag : data_out
ls2_time_hi : data_out

3.2.2.1.2 (U) HATS

ap_received_fire_control : data_in
quats_init_flag : data_in
switch_15ft_status : data_in
breakaway_status : data_in
sea_sense_status : data_in
r_p_m : data_in
amu_yaxis : data_in
amu_xaxis : data_in
depth_hi : data_in

(U) This function performs the Helicopter Attack Torpedo System (HATS) directed mode launch sequence.

(U) In a HATS launch the torpedo has the opportunity to initialize its Attitude Reference System while on the aircraft. This allows the Autopilot to execute pullout (MODE 1).

(U) An INTERLOCK, as used in this paragraph, is a requirement that must be met for engine start to occur. Should an INTERLOCK not be satisfied the engine will never start. The sequence of the INTERLOCKs ensures a single point of failure (SPOF) will not cause premature engine start. Each INTERLOCK is designated.

(U) Each INTERLOCK shall be executed in the order provided. Requirements for an INTERLOCK shall not be sought until the previous INTERLOCK has been satisfied.

(U) PROCESSING
(U) 1. [02-0013-0001] The program shall perform the Send Autopilot Messages function of Perform I/O Processing to send _LW_INITIALIZATION_MSG_HI_ and the _FIRE_CONTROL_DATA_MSG_HI_ to the Autopilot.

(U) 2. [02-0013-0002] The program will wait for the successful acknowledgment of both the _LW_INITIALIZATION_MSG_HI_ and the _FIRE_CONTROL_DATA_MSG_HI_ (i.e., _ap_received_fire_control_ = TRUE) via the Receive Command Status function.

(U) 3. [02-0013-0003] Wait for the AMU to be stable and ready (AMU_STABLE_TIME), then calculate quaternion presum for 200ms. The Process Inertial and Quaternion Data function shall calculate the quaternion presum

(U) 4. [02-0013-0004] The program shall perform the Send Autopilot Messages function to send the _QUATERNION_PRESUM_DATA_MSG_HI_ to the Autopilot.

(U) 5. [02-0013-0005] The program shall wait for successful acknowledgment of the quaternions. Upon receipt of the _LW_COMMAND_STATUS_DATA_MSG_AP_ where _quats_init_flag_ = TRUE, then the Hybrid Interface will send the _SENSOR_DATA_MSG_HI_ every 20ms.

(U) 6. [02-0013-0006] Inform the platform that the torpedo is ready for launch by setting _ready_to_launch_cmd_ = TRUE.

(U) 7. [02-0013-0008] The torpedo shall record that a nose impact occurred. This requirement shall be sought concurrently with Step 8.

If there is a 40ms period where _amu_xaxis_ is less than _NOSE_IMPACT_X_ or 
\[|amu_yaxis| > NOSE_IMPACT_Y\] then
\[
nose_impact_flag = TRUE
\]
end

(U) 8. [02-0013-0010] If the torpedo has reached the minimum depth for engine start when the depth switch input is TRUE (i.e., _switch_15ft_status_ = TRUE), the DSA input is at least 5 feet (i.e., _5ft< depth_hi_ ft), and the sea sense indicator in the Lanyard Start Assembly (LSA) indicates the presence of sea water (i.e., _sea_sense_status_ = TRUE) for 200ms then (INTERLOCK 1 & 2).

\[
set minimum_depth_flag = TRUE \text{ and } sea_sense_flag = TRUE \text{ when their respective requirement is met.}
\]
Start the engine.
a. Set the `engine_start_permit` = TRUE.
b. Set the `co2_squib_cmd` = FIRE.
c. Wait for 60ms
d. Set the `co2_squib_cmd` = FALSE.
e. Set the `ignitor_squib_cmd` = FIRE
f. Wait for 60ms
g. Set the `ignitor_squib_cmd` = FALSE
h. Repeat steps b-g once more.
go to step 9
else
continue checking for this interlock
end

(U) 9. [02-0013-0017] The following events shall be sought simultaneously:

(U) a.[02-0013-0011] If the torpedo has reached a depth (i.e., `depth_hi`) greater than `INITIAL_DESCENT_DEPTH` for 200ms, then set the `initial_descent_complete_flag` = TRUE. This flag is used in the Maintain Safe Operation function to determine if the torpedo has reached sufficient depth within an acceptable time.

(U) b.[02-0013-0012] If the engine speed (i.e., `r_p_m`) has reached 1000 rpm for 200ms, then the fins shall be unlocked and the Autopilot will begin the pullout maneuver. Power can now be applied to the forward electronics.

(U) -1- [02-0013-0013] Set the `engine_on_flag` = TRUE.

(U) -2- [02-0013-0014] Unlock the fins by setting `fins_unlocked_flag` = TRUE and `enable_fins_cmd` = TRUE.

(U) -3- [02-0013-0015] Set the `launch_status_2_flag_hi` = TRUE.

(U) -4- [02-0013-0016] Apply the forward power. Set `forward_power_cmd` = TRUE and `forward_power_flag` = TRUE. Set `forward_power_on_time` to the current time.

(U) -5- [02-0013-0018] Set `ls2_time_hi` to the current time.

equipment

engine_start_permit : data_out
nose_impact_flag : data_out
minimum_depth_flag : data_out
sea_sense_flag : data_out

Massachusetts Institute of Technology – System Design and Management
initial_descent_complete_flag : data_out
launch_status_2_flag_hi : data_out
fins_unlocked_flag : data_out
enable_fins_cmd : data_out
data_out
engine_on_flag : data_out
forward_power_cmd : data_out
forward_power_flag : data_out
forward_power_on_time : data_out
ready_to_launch_cmd : data_out
c02_squib_cmd : data_out
ignitor_squib_cmd : data_out
data_out
breakaway_flag : data_out
ls2_time_hi : data_out

3.2.2.5.3 (U) Shutdown Processing

pda_status : data_in
exploder_isolated_status : data_in
exploder_charged_status : data_in
exploder_armed_status : data_in
time_of_last_ap_message : data_in
depth_hi : data_in
pullout_complete_hi : data_in
switch_15ft_status : data_in
minimum_depth_flag : data_in
initial_descent_complete_flag : data_in
sea_sense_flag : data_in
nose_impact_flag : data_in
wc_status : data_in

(U) This function will time the event initial_descent_complete_flag. Initial descent is defined as the time between when all the criteria for engine start are met and the initial crossing of the ceiling. If it does not occur in INITIAL_DESCENT_TIME then initiate shutdown.

(U) Shutdowns will also be initiated if the torpedo does not remain below PULLOUT_CEILING_DEPTH between initial descent complete and pullout_complete_hi, when the torpedo does not remain below 15 ft, or if the engine fails to start properly.

(U) This function operates every 20ms.

Massachusetts Institute of Technology – System Design and Management
(U) PROCESSING

(U) 1. a. [02-0026-0001] Time the initial_descent_complete_flag event from the engine start event (i.e., minimum_depth_flag = TRUE).

   b. [02-0026-0006] Time the engine_on_flag event from water entry (i.e., sea_sense_status=TRUE for a consecutive 200ms).

(U) 2. [02-0026-0011] If Decode Presets on Reset indicates that a reset has occurred then

   shutdown_class = CGA_RESET
   send the shutdown message and continue to step 10.
end

(U) 3. [02-0026-0007] If the time in step 1b exceeds NO_START_TIME then

   shutdown_class = NO_START1
   send the shutdown message and continue to step 10.
end

(U) 4. a. [02-0026-0008] Upon nose_impact_flag and switch_15ft_status both having transitioned to TRUE, initiate a timer, timing the time until engine_on_flag=TRUE.

   b. [02-0026-0009] If the time in step 4a exceeds NO_START_TIME then

   shutdown_class = NO_START2
   send the shutdown message and continue to step 10.
end

(U) 5. [02-0026-0002] If the time in step 1a exceeds INITIAL_DESCENT_TIME then

   shutdown_class = INITIAL_DESCENT
   send the shutdown message and continue to step 10.
end

(U) 6. [02-0026-0003] If initial_descent_complete_flag = TRUE and pullout_complete_hi = FALSE then

   If the average depth (i.e., depth_hi) for 12 samples is less than PULLOUT_CEILING_DEPTH then

Massachusetts Institute of Technology - System Design and Management
shutdown_class = PULLOUT_CEILING
continue to step 10.
End
end

(U) 7. [02-0026-0004] If initial_descent_complete_flag = TRUE and switch_15ft_status = OPEN for 12 samples then

shutdown_class = FIFTEEN FOOT
continue to step 10
else
exit the function.
end

(U) 8. [02-0026-0010] This shutdown will verify the correct operation of the DSA.
If the last 10 consecutive DSA samples produced an error then

shutdown_class = DSA_FAILURE
send the shutdown message and continue to step 10.
end

Keep a 10 point sample of depth change. If the average depth change exceeds ± 3.0 ft and engine_on_flag = TRUE then

shutdown_class = DSA_FAILURE
send the shutdown message and continue to step 10.
end

(U) 9. [02-0026-0012] If Weapon Control is not up (wc_status = BAD) for any 40 second period after the engine is on (i.e., engine_on_flag = TRUE) or Weapon Control goes down during the run (wc_status transitions from GOOD to BAD) then

shutdown_class = PGA_FAILURE
send the shutdown message and continue to step 10
end

(U) 10. [02-0026-0005] Send the SHUTDOWN_MSG_HI to MRECS at the maximum rate of one per second. Set shutdown_time to the time, in milliseconds, since the processor came up. The message consists of:

time_of_last_ap_message
exploder_armed_status
exploder_charged_status
exploder_isolated_status
pda_status.
shutdown_class
shutdown_time

(U) RECORDING

(U) Record the following item according to the requirements in Compose Record Message.

switch_15ft_status

SHUTDOWN_MSG_HI : data_out