A New Approach to Hazard Analysis for Rotorcraft

A New Approach to Hazard Analysis for Rotorcraft

Blake Abrecht
Massachusetts Institute of Technology
Engineering Systems Division Master's Student
2nd Lieutenant, United States Air Force
Cambridge, MA, USA

Dave Arterburn
Director, Rotorcraft Systems Engineering and Simulation Center
University of Alabama in Huntsville
Huntsville, AL, USA

David Horney
Jon Schneider
Massachusetts Institute of Technology
Aeronautics and Astronautics Master's Student
2nd Lieutenant, United States Air Force
Cambridge, MA, USA

Brandon Abel
Massachusetts Institute of Technology
Aeronautics and Astronautics PhD Candidate
Major, United States Air Force
Cambridge, MA, USA

Nancy Leveson
Professor of Aeronautics and Astronautics
Massachusetts Institute of Technology
Cambridge, MA, USA

ABSTRACT

STPA is a new hazard analysis technique that can identify more hazard causes than traditional techniques. It is based on the assumption that accidents result from unsafe control rather than component failures. To demonstrate and evaluate STPA for its application to rotorcraft, it was used to analyze the UH-60MU Warning, Caution, and Advisory (WCA) system associated with the electrical and fly-by-wire flight control system (FCS). STPA results were compared with an independently conducted hazard analysis of the UH-60MU using traditional safety processes described in SAE ARP 4761 and MIL-STD-882E. STPA found the same hazard causes as the traditional techniques and also identified things not found using traditional methods, including design flaws, human behavior, and component integration and interactions. The analysis includes organizational and physical components of systems and can be used to design safety into the system from the beginning of development while being compliant with MIL-STD-882.

INTRODUCTION

Systems Theoretic Process Analysis (STPA) is a new hazard analysis technique that was created in response to inadequacies that exist in traditional, widely used hazard analysis techniques. STPA differs from traditional safety analysis techniques in treating safety as a control problem rather than a component failure problem, as discussed in Ref. 1. By expanding the focus from failures to control, STPA is able to identify and address not only component failures that can lead to a hazardous system state, but also design flaws and other unsafe causes that current failure-based methods cannot.

STPA is an iterative, top-down modeling and hazard analysis technique based on system theory. The process starts the same as any hazard analysis technique, with identifying the accidents and high-level hazards to be considered. Then the system is modeled using hierarchical control loops, with each level controlling components at the level below. For example, in helicopters today, the pilot

Presented at the AHS Development, Affordability and Qualification of Complex Systems Specialists' Meeting, Huntsville, AL, Feb 9-10, 2016.

controls the automatic control systems, which in turn control the aircraft physical components. Because the model can include the overlying organizational structure (and not just the physical system), an organizational analysis can be performed on various organizational factors impinging on safety, such as guidelines, regulations, training, etc.

The analysis in this application is performed on the system model. Potential unsafe control actions are first identified that can lead to hazardous system states. Then the potential causal scenarios of the unsafe control actions are documented. The causal scenarios can be used to eliminate hazards from the system design and operations, to design mitigation and control measures for the causes that cannot be eliminated, and to create system and software safety requirements. Because the analysis is performed on a formal model, parts of it can be automated and assistance provided to the analyst, as shown in Ref. 2.

In this paper, the use of STPA is demonstrated on the Warning, Caution, and Advisory (WCA) system of the UH-60MU aircraft. Because of resource limitations, STPA was performed only on parts of the WCA associated with the electrical and fly-by-wire flight control system (FCS). This part of the system is complex and critical enough, however, that the advantages of STPA can be adequately demonstrated. The organizational safety control structure (safety management system) for both training and routine peacetime operations of the UH-60MU and for combat operations was also modeled.

STPA has been and is currently being used successfully to analyze systems in many fields, including aviation, spacecraft, automobiles, healthcare, nuclear power, and defense systems. One previous research study is of particular relevance to this paper. Reference 3 compares STPA and the ARP 4761 Safety Assessment Process widely used on aircraft. In particular, the wheel brake example in ARP 4761 is analyzed using STPA and the types of results obtained are compared. When comparing the results of the two approaches, some important differences found were:

- The ARP 4761 safety requirements are primarily quantitative, along with a few design assurance requirements and design requirements to support the independent failure assumptions of the quantitative failure analysis that is used to generate the requirements. In contrast, STPA generates functional design requirements to prevent hazards, including those that do not result from component or functional failures.

- ARP 4761 provides guidance in implementing fail-safe design, with an emphasis on redundancy and monitors whereas STPA has the potential for suggesting more general safe design features, including eliminating hazards completely.

- ARP 4761 places human operators outside the system boundaries, considering them primarily as mitigators of hazardous physical system failures. Human errors are not included. In contrast, STPA treats the human operator as a component of the system just like any other physical component and identifies hazard causes related to human behavior.

- ARP 4761 omits software from the quantitative failure analysis and references the use of a general software engineering standard (DO-178B/C) to ensure that the software development uses more rigorous software engineering processes for more critical software. STPA, in contrast, treats software like any other system component in the hazard analysis and is able to generate the functional safety requirements for the software.

The authors of Ref. 3 conclude that due to the increasing complexity and use of software in aircraft, the traditional hazard analysis methods described in ARP 4761 are no longer as effective on software-intensive systems where accidents may result from unsafe interactions among the components and not just component failures.

The UH-60MU WCA System

According to Ref. 4, the Blackhawk helicopter "performs a wide range of missions that encompass Air Assault, MEDEVAC, Combat Search and Rescue (CSAR), Command and Control, and VIP transport" (pp. 3). Sikorsky states that "the newest version of the Army's premier combat utility helicopter will ensure compatibility with the U.S. Army's Future Force and will bring new life to the existing fleet of helicopters, improve their effectiveness, reduce their vulnerability, and allow for future growth of the fleet while lowering operating and support costs" (pp. 3). The UH-60MU platform contains a Common Avionics Architecture System (CAAS) that gives the helicopter an entirely new cockpit and changes how the helicopter handles WCAs beyond that of the glass cockpit integration in the baseline UH-60M.

The WCA system has three functionally separate components. The first component is a master warning panel that communicates directly with aircraft subsystems and initiates a warning display to the Flight Crew if an issue arises, providing early notification of cautions and warnings. The second WCA component links different aircraft subsystems to various CAAS components that then process the data and display relevant information to the Flight Crew via the Multi-Function Displays (MFDs). These components determine if a warning, caution, or advisory needs to be displayed, how the warning, caution, or advisory will be displayed, and the priority that should be given to each occurrence based upon a set of criteria and priorities established as part of the design. The third component of the system is the audible tone and voice warnings transmitted to the Flight Crew through the intercommunication system (ICS) after being triggered by one of the subsystem components. The Master Caution System, CAAS integrated WCA system voice warnings, and aural warnings were

designed to provide up to date information about the state of the helicopter and its associated systems to the Flight Crew when responding to failures or exceedances outside of normal ranges.

UH-60MU STPA CASE STUDY

The focus of this analysis is on the warnings, cautions, and advisories that are associated with two specific subsystems: the electrical subsystem and the FCS. The following sections document the STPA process in applying this hazard analysis technique.

Defining Accidents and Hazards

Before any hazard analysis, the accidents (losses) to be prevented and the hazardous states that can directly lead to those losses must be identified. In Ref. 1, an accident is defined as an undesired and unplanned event that results in a loss, including a loss of human life or human injury, property damage, environmental pollution, mission loss, financial loss, etc. For the purpose of this effort, two relevant accidents were used: *A-1: Loss or major damage to aircraft* and *A-2: One or more fatalities or significant injuries.*

The definition of a hazard in MIL-STD-882 is vague and can include just about anything. To be more specific, Ref. 1 defines a hazard as a system state or set of conditions that together with a worst-case set of environmental conditions will lead to an accident (loss). Table 1 shows the hazards used in this analysis that can lead to the two selected accidents. Table 1 also illustrates the high-level safety constraints associated with these top level hazards.

Table 1. Hazards and derived high-level safety constraints

Hazard	Definition	Safety Constraint
H1: Violation of minimum separation requirements. *Can lead to: (A-1, A-2)*	Minimum separation is defined as the helicopter coming into close proximity with another source of mass (such as the terrain, another aircraft, etc.)	The aircraft must maintain adequate separation from potential sources of collision.
H2: Lack of aircraft control. *Can lead to: (A-1, A-2)*	Lack of control is defined as inability of the Flight Crew to control the aircraft	The aircraft must be under control of the Flight Crew at all times.

These accidents and hazards were selected based on the definitions of an accident and hazard contained within STPA guidelines. While the STPA accident definitions are similar to critical and catastrophic hazard definitions used in independently conducted traditional hazard analyses of the UH-60MU, the STPA hazard definitions do not correlate with the traditional hazard analysis approach. The difference in hazard definitions is important because they are not simply failures and thus allow for the identification of a wide range of unsafe control actions and causal scenarios in the analysis.

Creating the hierarchical control structure

After the system-level hazards have been identified, a hierarchical control structure for the system is created. This control structure can include the organizational structure (which we demonstrate in the next section) and the physical system functional control structure. A control structure is composed of hierarchically organized feedback control loops. For example, the pilot controls the automated control systems, which in turn control the physical components of the aircraft.

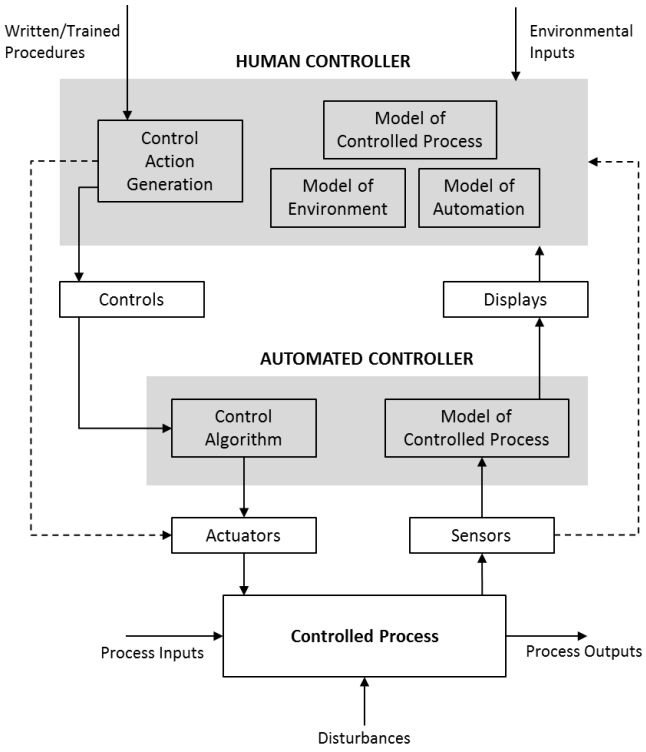

Figure 1.The Form of a Simple Hierarchical Control Structure (Ref. 1, pp. 269)

Figure 1 shows a simple control structure with a human controller at the top. Note that both human and automated controllers use a model of the controlled process in order to determine what control actions to provide. This process model is used by the control algorithm within the controller to determine what control actions are required. Human controllers must, in addition, have a model of the automation that informs control action generation, along with various written procedures, training, and environmental inputs. This model is often called a mental model and is important in situation awareness. The process (mental) models are updated using feedback from the controlled process. Depending on the system design, the human controller may or may not have the ability to directly control the controlled

process or to directly receive feedback about it. Otherwise, the control actions and feedback must go through the automated controller. Process models are used in the identification of unsafe control actions in STPA and allow humans to be included in the hazard analysis.

Organizational Control Structure

An organizational safety control structure for the training and routine peacetime operations of the UH-60MU system is shown in Figure 2. The overall system goal for this organizational control structure, as applicable for this effort, is to provide traceable guidance, regulations, and orders for army systems operations. The controls at the organizational level affect the control of the UH-60MU at the aircraft level.

Part of constructing the safety control structure is to document the safety-related responsibilities of each component within the organization. While each component contained in Figure 2 will not be discussed in detail as part of this paper, consider the following example. Depicted at the top right of Figure 2, Ref. 5 states that the Director of Army Safety (DASAF) manages the Army aviation accident prevention program and is responsible for "Army-wide aviation safety functions cited in AR 10-88 [and for] providing the functions of developing aviation risk control options for commanders" (pp. 1). The responsibilities and safety-related decisions made by the DASAF thus influence decisions and organizational control at various levels, including at the UH-60MU level.

The UH-60MU can also be used during combat operations and influenced by combat-specific guidance and regulations. Therefore, a separate combat operational safety control structure is needed for analysis and is shown in Figure 3. Because one of the goals of this project was to compare STPA with traditional hazard analysis methods, which do not include organizational factors in safety, only the aircraft level of the system model was analyzed. However, STPA can be used on any hierarchical control structure and therefore the organizational components impacting safety and hazards, such as command decision making, training regulations, guidelines, procedures, etc., can be included.

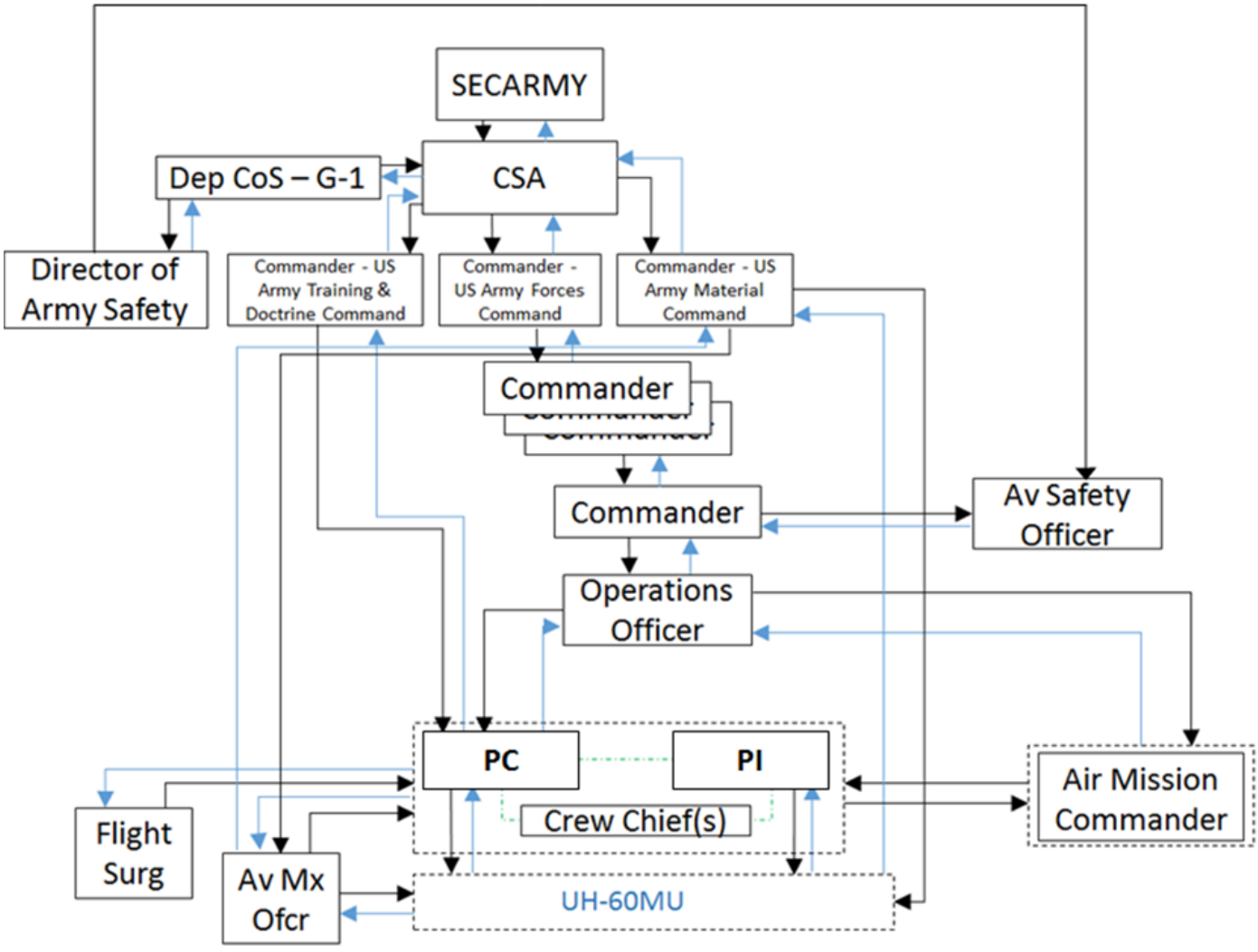

Figure 2. UH-60MU training and peacetime operational safety control structure

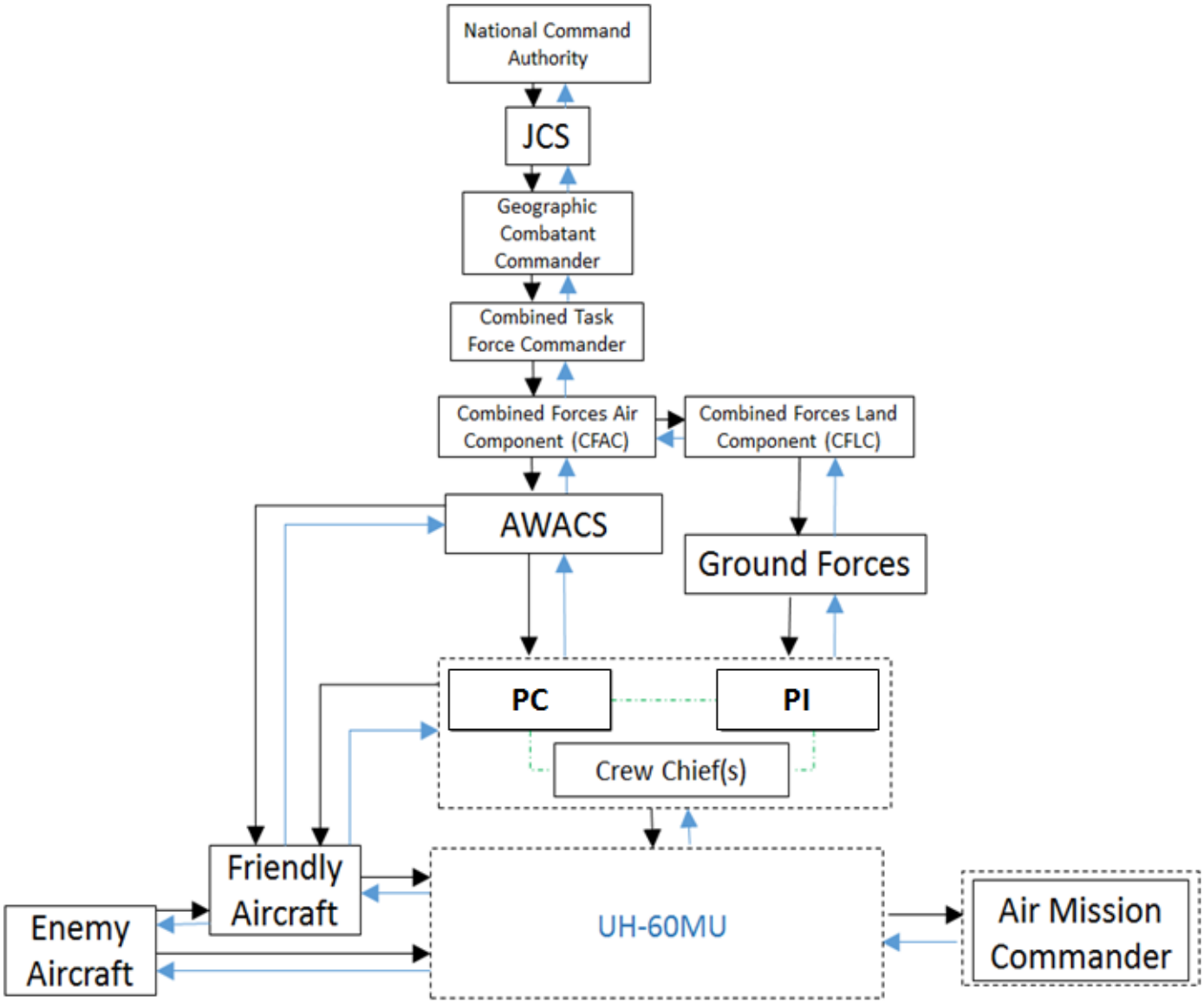

Figure 3. UH-60MU combat operational safety control structure

UH-60MU Functional Control Structure

The UH-60MU is shown only as a single block in Figures 2 and 3. One of the important aspects of modeling and analyzing complex systems is the ability to work at various levels of abstraction. In the remainder of the paper, the control structure within the aircraft itself is analyzed in more detail.

Figure 4 shows the aircraft-level UH-60MU control structure containing the main functional components of the aircraft. Because the analysis starts with a model of the entire system, a top-down system hazard analysis can be performed using STPA to identify how interactions among system components can lead to accidents. Not only can system interactions be considered, but much of the analysis of the detailed system can be eliminated by only considering those features that have a safety impact on the system as a whole. This is, of course, the great advantage of a top-down analysis method, such as STPA, versus a bottom-up one such as Failure Mode, Effects, and Criticality Analysis (FMECA).

As shown in Figure 4, the Flight Crew, which is composed of the Pilot-in-Command (PC), Pilot (PI), and Crew Chief (CE), is responsible for maneuvering the helicopter, providing system inputs through the pilot vehicle interface (PVI), providing the control system parameters for the helicopter's automatic control systems, managing internal communications, and managing external communications during operations. In order to perform these tasks, each of the members that make up the Flight Crew has various process (mental) models that inform them of the current state of the controlled process, including. a model of the state of the overall helicopter, a model of the state of the mission environment, a model of the state of the PVI

systems, and a model of the state of the automatic control systems. These models together inform the Flight Crewmembers' decisions and action generation. As stated earlier, a common cause of accidents involving humans and computers is that these models of the controlled processes become inconsistent with the state of the real system and unsafe control is provided. For example, the Flight Crew may be unaware that icing conditions exist or that the existing controls designed into the UH-60MU to mitigate icing conditions are not functioning properly. As a result of this flawed process model, the Flight Crew may therefore not take appropriate actions needed for safe helicopter operation.

The subsystems that comprise the PVI are responsible for providing an interface for Flight Crew control of automatic control systems, providing an interface for Flight Crew control of other aircraft subsystems; providing relevant feedback to the Flight Crew regarding the helicopter's status; and integrating sensor feedback to initiate warnings, cautions, and advisories through the various WCA systems. As is true for all controllers, the PVI components each have a process model of the mission equipment, the automatic control systems, and the physical components of the helicopter. These models inform their action generation. The helicopter subsystems that comprise the automatic control systems each have a process model of the mission equipment, the overall functioning of the helicopter, and the Flight Crew that is operating the helicopter. The automatic control systems use these process models to automatically regulate aircraft system functions, integrate Flight Crew control inputs to generate output commands, provide control mixing functions, and provide autopilot and flight director mode functions.

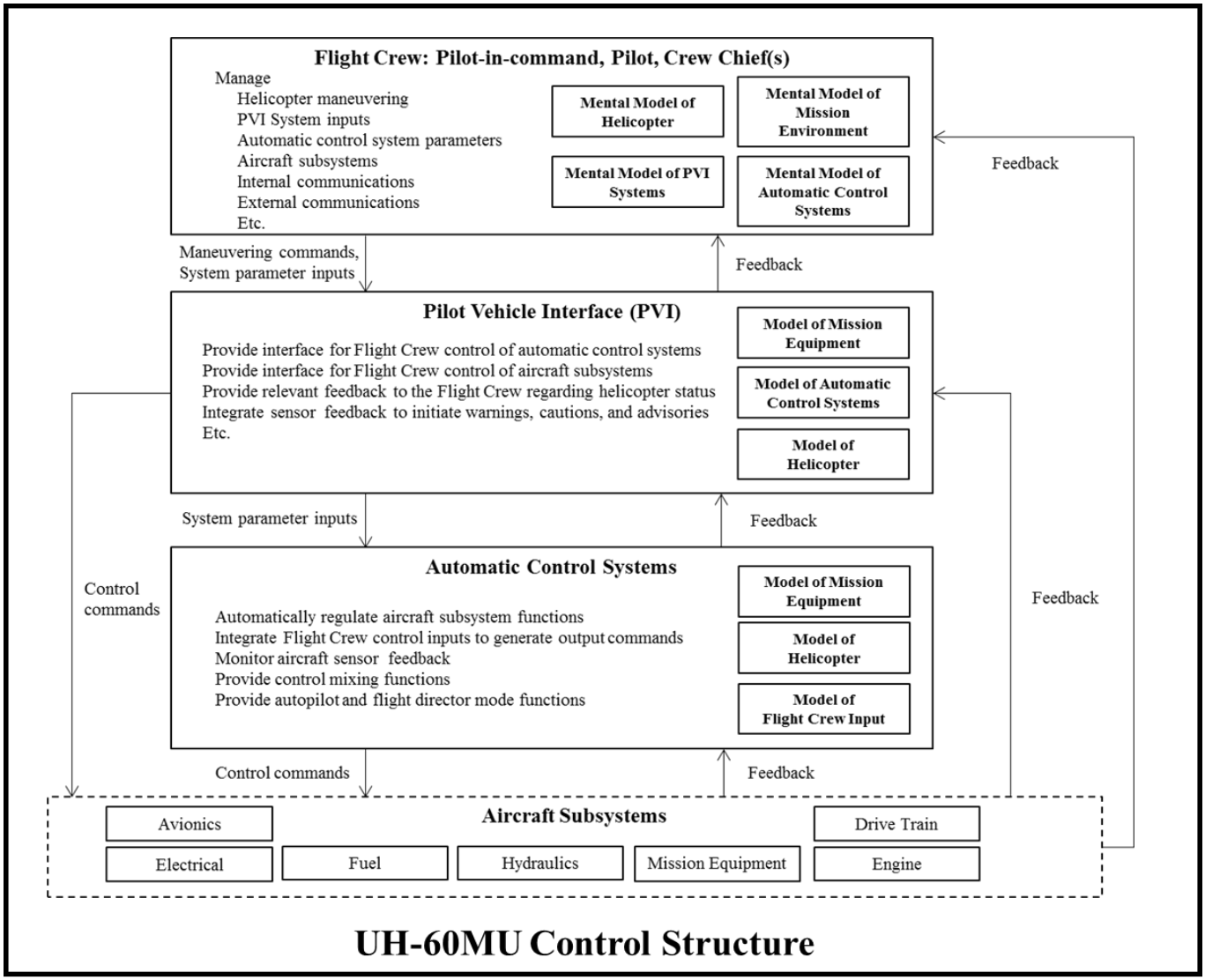

Figure 4. High-level control structure at the UH-60MU level

Figure 5 provides a more detailed model regarding the control actions between components and the feedback provided by the component. To reduce the scope of the analysis to fit the resources of this demonstration project (there are over 200 warnings, cautions, and advisories associated with all of the helicopters' functions), the analysis focuses on the control actions and feedback associated with two of the helicopters subsystems and applicable WCAs: the electrical system and FCS. The content of the control actions and feedback contained within each of the arrows depicted in Figure 5 are omitted to make the figure readable. However, a few examples will be given to highlight the information contained within each control and feedback arrow.

For instance, consider the control actions that the Flight Crew provides through each respective Pilot Vehicle Interface. Related to the electrical subsystem, the Pilot-in-Command (PC) and Pilot (PI) are responsible for controlling the main generator power, APU generator power, battery power, external power, and arming the standby instruments. Related to the FCS, the PC and PI are responsible for providing collective and cyclic control input along with pedal deflections to maneuver the helicopter. They are also responsible for inputting FCS trim changes, stabilator deselections, Direct Mode selections, and activating auto stabilator control.

The Flight Crewmembers also receive feedback from their respective PVI components as well as directly from the aircraft subsystems. For example, both the PC and PI receive tactile feedback from switches and active inceptors, auditory sensory feedback from audio warnings and tones, visual feedback from the multifunctional display and other cockpit displays, as well as visual feedback from the master warning panel and applicable WCA lights, to name a few. This feedback, along with all of the other feedback being presented is used by the Flight Crew to update their various mental process models that they have of the respective controlled processes. Furthermore, mission related communication occurs between the PC, PI, and CEs and allows for additional information to be passed between these controllers during operations. While these examples discuss control actions and feedback contained in the arrows between the Flight Crew and PVI, each control and feedback arrow contains similar information that is relevant for the identification of unsafe control actions in the analysis.

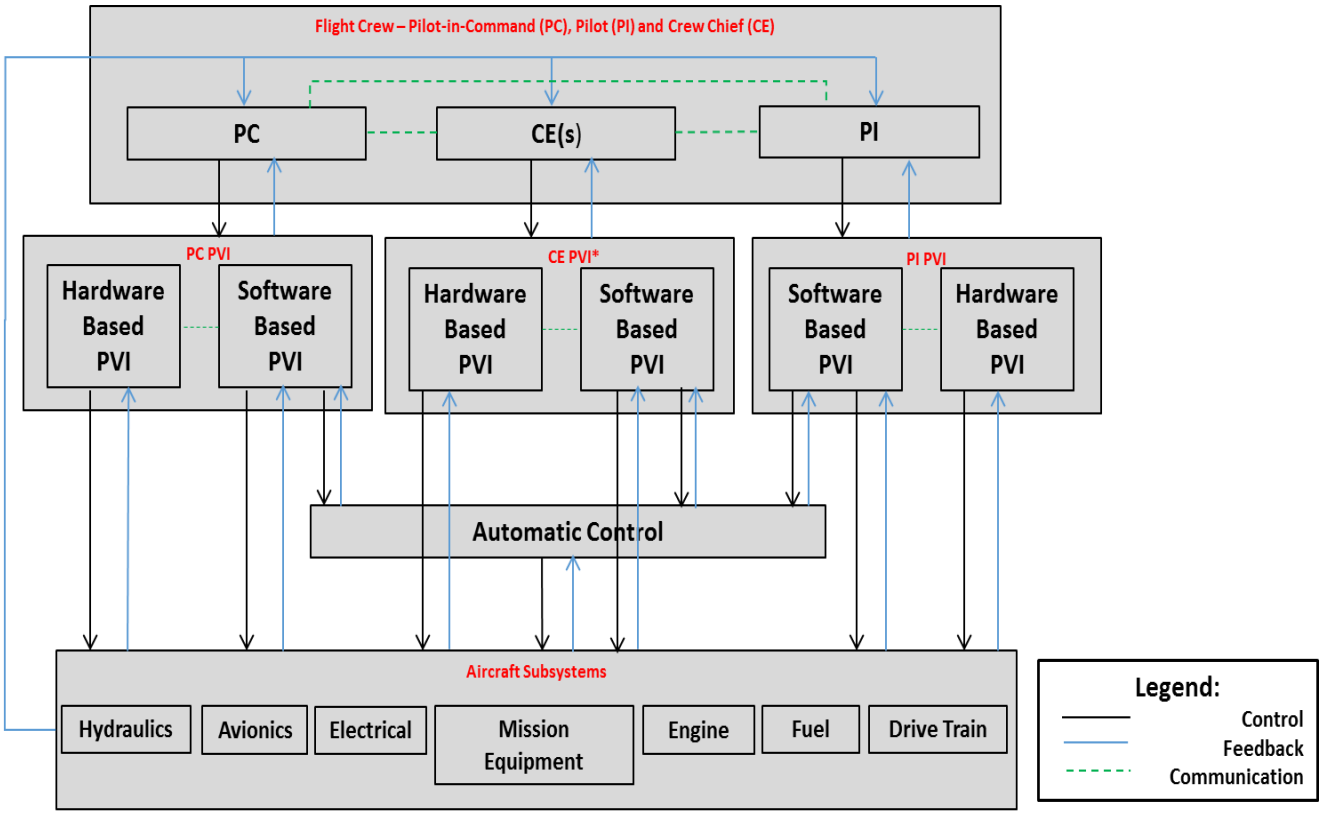

Figure 5. Functional control structure of the UH-60MU

Figure 6 expands upon the control structure of the electrical system and models the different electrical related systems in the PVI, automatic control, and aircraft subsystem components.

Looking at Figure 6, the Flight Crew provides control inputs to the electrical system through the helicopter's overhead console and eight circuit breaker panels. While the Flight Crew receives visual and tactile feedback from these sources, the main source of feedback related to the electrical system is through the pilot and co-pilot MFDs. There are four distinct components within the electrical automatic control subsystem: the auxiliary power unit (APU) generator control units (GCU), the AC generator GCUs, the external power monitor and the permanent magnetic generators (PMG) regulators.

The APU GCU regulates the helicopters' APU generator. The #1 and #2 GCU regulate the helicopters' #1 and #2 AC generators respectively. An external power monitor regulates power that is being provided to the helicopter from an external power source. The #1 and #2 PMG regulators provide control authority over the #1 and #2 PMG. The helicopter has multiple redundant sources that provide AC and DC power to the helicopter, as depicted in the aircraft subsystem section of Figure 6. The two AC generators provide AC as the primary source of power. The AC generators feed two independent AC primary buses and also provide a portion of their load to be converted to DC, which is distributed by two independent DC primary buses and two independent DC essential buses. In emergency situations that require power from a source other than the two AC generators, the APU generator is capable of providing flight-critical power to the AC and DC buses. The UH-60MU's electrical system has a hierarchical rank structure of its electrical power supplies, which allow for the main #1 and #2 AC generators to take precedence over the APU generator, which automatically takes precedence over external power supplies. The permanent magnetic generators (PMGs) provide flight critical DC power for the FCS while the two 24-volt batteries provide backup DC power to both the DC Converters for mission equipment and the flight critical systems.

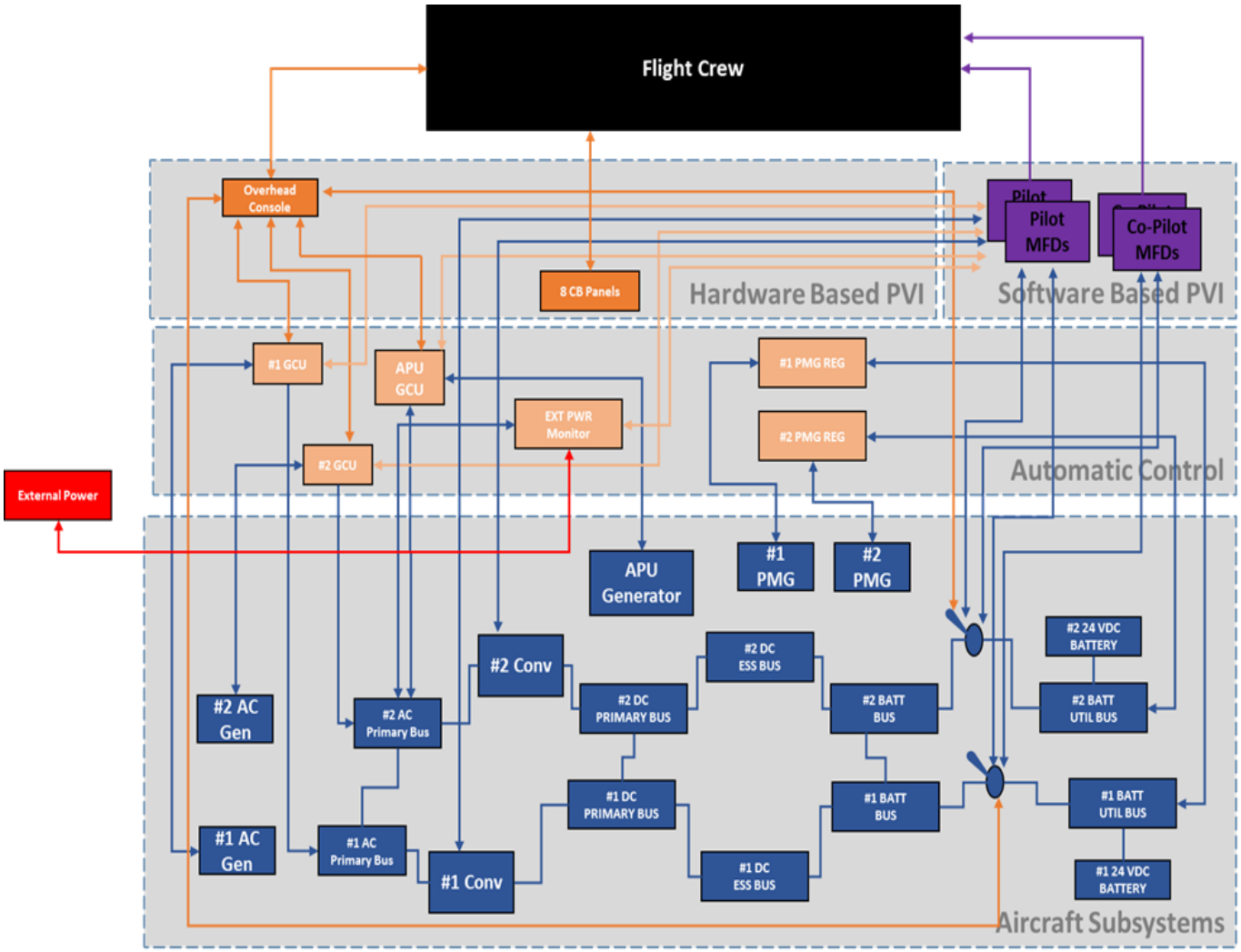

Figure 6. Detailed control structure applicable to electrical subsystems

Figure 7 shows more detail about the FCS and the different FCS related systems that are in the PVI, automatic control, and aircraft subsystem components. The Flight Crew provides hardware and software-based PVI flight control inputs and receives hardware and software-based PVI feedback through the helicopter's active cyclic, active collective, pedals, one engine inoperative (OEI) training panel, engine control panel, and master warning panels. The software based PVI consists of two pilot MFDs, two co-pilot MFDs, an ICS, two flight director display control panels (FDDCP), a FCS control panel, and two central display units (CDU) that receive Flight Crew input, process commands, and provide software-based PVI feedback to the Flight Crew.

The automatic control subsystem consists of dual redundant full authority digital engine control systems (FADEC), dual redundant inceptor control units (ICUs) and triple redundant flight control computers (FCCs). The FCCs receive all commands generated by the Flight Crew and PVI and process these commands to be implemented by the appropriate aircraft subsystem. The FCCs also receive feedback from all relevant subsystems, process the raw data, and send feedback through the respective hardware-based or software-based PVI to the Flight Crew.

The FCS includes redundant embedded global positioning/inertial navigation systems (EGIs), redundant rotor rpm (NR) sensors, triple redundant inertial navigation units (INUs), redundant air data computers (ADCs), an integrated vehicle health management system (IVHMS), a radar altimeter, weight on wheel switches, and various servos, actuators, and pumps that are used to implement control of the rotors.

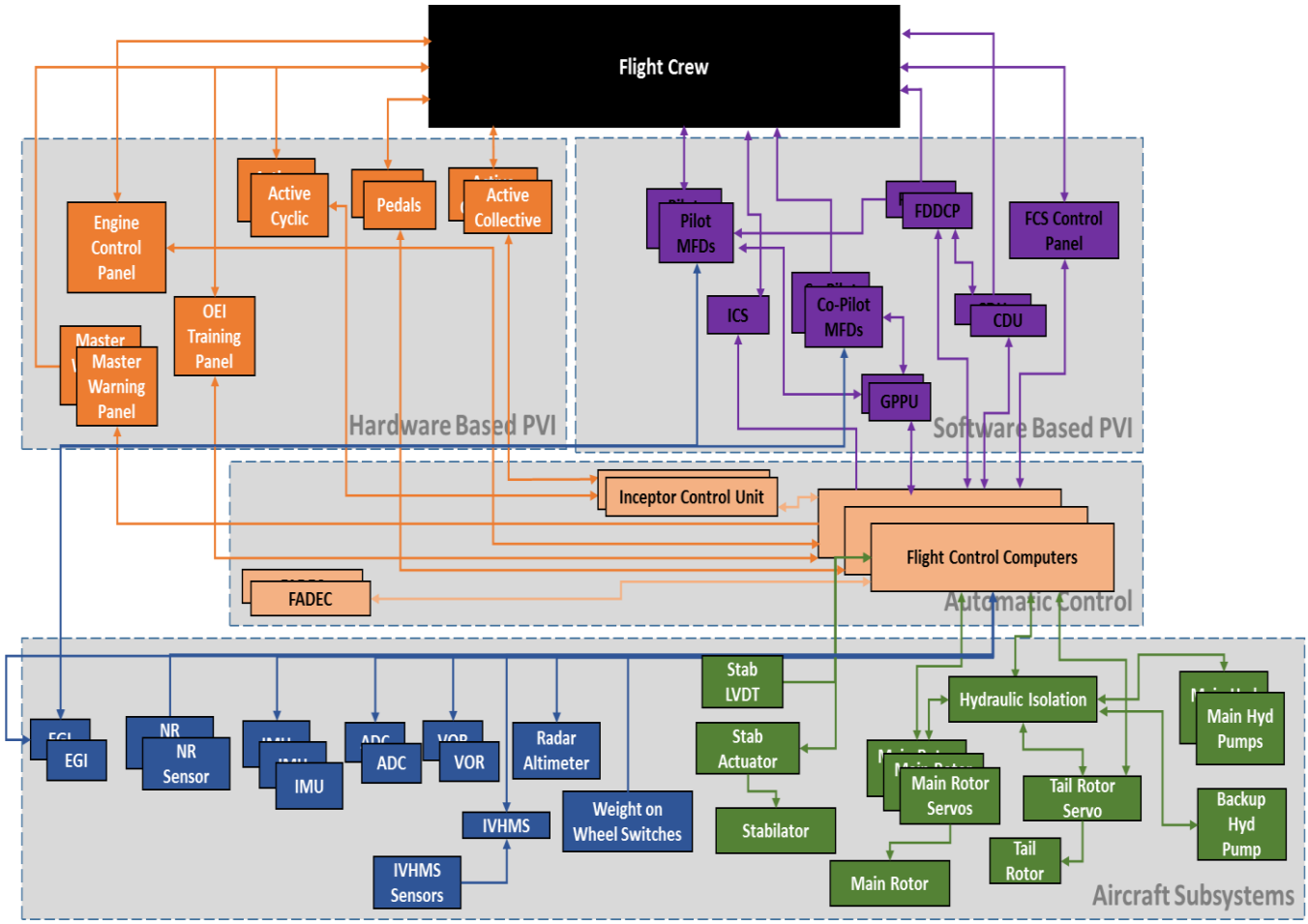

Figure 7. Detailed control structure applicable to FCS subsystems

Unsafe Control Actions

Using the modeled control structure, STPA identifies potential unsafe control actions leading to the identified hazards and scenarios that can lead to these unsafe control actions. An example of an unsafe control action is that "*Flight Crew arms standby instruments after main batteries have already been discharged thus depleting the standby batteries before landing [H-2].*" Note that the unsafe control action is just what is usually labeled a hazard or a hazard cause.

An unsafe control action can be divided into four parts: a source controller, the type of control action, the control action itself, the context in which the control action occurs. Each unsafe control action is also labeled with the system hazard to which it contributes in order to provide traceability. In this case: *inability to safely control the aircraft (H-2).* Note that complete traceability of hazards to the system design can be provided by this process.

The initial part of the unsafe control action is the source controller within the functional control structure that either provides (or does not provide) the control action that is being analyzed. In this analysis, the source controllers are the Flight Crew, various PVI components, or various automatic controllers. For the example above, the source controller is the Flight Crew.

The second part of an unsafe control action is type of unsafe control. There are four types of unsafe control: (1) not providing a control action leads to a hazard, (2) providing a control action leads to the hazard, (3) a control action provided with incorrect timing or in the wrong order creates the hazard, or (4) a control action stopped too soon or applied for too long (for a continuous control action) results in a hazard. Each relevant control action falls into one of these four categories. In the example above, the type is the first one, i.e., providing a control action that leads to a hazard.

The third part is the control action itself. In the example the control action is *arming the standby instruments*. The fourth and final part of the unsafe control action is the context or scenario that defines what actually makes the control action unsafe. In our example, the context is *after the main batteries have already been discharged.* The result of the unsafe control action is *depleting the standby batteries before landing.* There is always a context in which the control action is unsafe. If the control action is always unsafe, then it would not have been included in the system design.

It is important to note that these unsafe control actions do not need to be solely in response to failures. Design issues during normal operation of the equipment can and often do cause unsafe control actions when the crew or system does not respond to control the system in response to input or stimulus that is part of the design as intended. This important distinction allows identification of flaws in the design for both normal operations and in response to failures. To identify unsafe control actions for the electrical system focus, the control loops between the Flight Crew, PVI, automatic control and the aircraft subsystems were analyzed. To identify unsafe control actions for the FCS focus, the control loops between the Flight Crew, the hardware and software-based PVI, automatic control, and the aircraft subsystems were analyzed.

Using this process 126 unsafe control actions associated with the electrical subsystem and FCS were identified. There were 24 unsafe control actions identified between the Flight Crew and the PVI (electrical), 10 unsafe control actions identified between the automatic control and the aircraft subsystems (electrical), 44 unsafe control actions identified between the Flight Crew and the PVI (FCS), 24 unsafe control actions identified between the software-based PVI and the automatic control (FCS), and 24 unsafe control actions identified between the automatic control and the aircraft subsystems (FCS). Table 2 shows one row from an unsafe control action table that identifies unsafe control actions related to the electrical subsystems. It has been found that documenting these control actions in tables is convenient for the analyst. Automated tools can generate all the possible unsafe control actions from the control structure, but human intervention is needed to sort through the generated list to identify which ones are possible and hazardous. By automating the generation of all unsafe control actions, this step in the process can be shown to be complete.

Table 2. Partial UCA table depicting three electrical related unsafe control actions

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect timing/ incorrect order	Stopped too soon/ applied too long
Electrical Cautions ON	**ES UCA32:** EICAS does not display an "electrical" caution when the applicable conditions for an alert exist. *[H-1, H-2]*	**ES UCA33:** EICAS presents an "electrical" caution when the conditions applicable to the caution do not exist. *[H-1, H-2]*	**ES UCA34:** EICAS presents an "electrical" caution too late for the Flight Crew to recover the aircraft to a safe condition. *[H-1, H-2]*	N/A

Identifying Causes of Unsafe Control Actions

In many cases, identifying the unsafe control actions allows design requirements to be generated and provides enough information for engineers to eliminate or mitigate the unsafe control in the system design. If more information is needed or desired to adequately eliminate or mitigate the unsafe control, then more information about its causes, i.e., the scenarios leading up to it, must be obtained. This scenario generation step cannot be automated (at least not yet) and requires human analysis. The same is true for the traditional hazard analysis methods, of course. Because STPA works on a formal model, automation of this step is potentially possible in the future.

Figure 8 shows some generic control loop flaws that can lead to an unsafe control action. For example, a controller might not provide a control action when needed or might provide an unsafe one because of an inadequate control algorithm or an inconsistent, incomplete, or incorrect process model of the controlled process or system state. This flawed process model could, in turn, result from inadequate, incorrect, missing, or delayed feedback from sensors. Sensors may not operate as required due to feedback delays, measurements inaccuracies, or missing sensor information from the controlled process. There is also the possibility that a correct control action causes safety problems due to delayed operation from an actuator or component failures, resulting in an unsafe system state.

Another reason for an accident is that a safe control action is provided, but it is not executed correctly. The hazard causes found by component failure-based hazard analysis techniques are this type of cause, i.e., a failure in the execution of a control command. STPA, however, also allows the analyst to identify causes that do not result from failure but from requirements and design errors, i.e., the component behavior satisfies its requirements but those requirements are incorrect, perhaps because the designer forgot cases or misunderstood how the system components would interact and work together or did not account for human errors.

Causal scenarios were generated for each of the 126 identified unsafe control actions for the electrical systems and FCS WCA systems in the UH-60MU aircraft. It is not possible to discuss each individually within the scope of this paper, however, example electrical and FCS causal scenarios are described in the following sections.

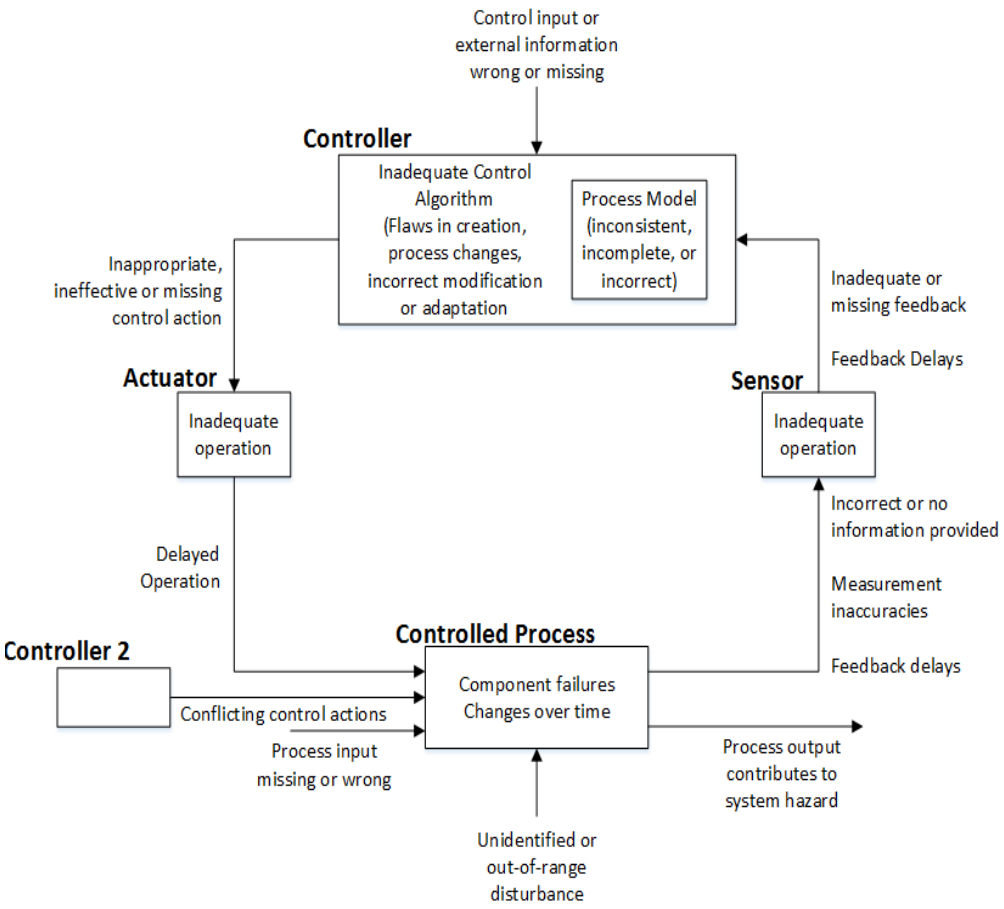

Figure 8. Generic control loop flaws (Ref. 1, p. 93)

Example Electrical System Hazard Causal Scenarios

Consider the following unsafe control action and causal scenarios related to the electrical subsystem: *Flight Crew switches battery power ON and does not reduce the amount of mission equipment (when batteries are the only source of DC power) to allow sufficient time for a safe landing in friendly territory. [H-1, H-2]* There are at least three causal scenarios identified that could lead to this unsafe control action:

- *Scenario 1:* The Flight Crew does not reduce the amount of mission equipment when batteries are the only source of DC power because the Flight Crew is unable to immediately determine what mission equipment can safely be taken offline.

- *Scenario 2:* The Flight Crew is unaware that the batteries are the only source of DC power that is powering the helicopter. This flawed process (mental) model could be the result of:
  a) The Flight Crew does not receive the applicable cautions because of a WCA system failure and thus does not know that there has been total power loss except for the battery power supply.
  b) Applicable cautions associated with power loss are annunciated to the Flight Crew but they are masked by other warnings, cautions, and advisories that are also being presented to the Flight Crew.

- *Scenario 3:* The Flight Crew does not know that there is insufficient time to safely land the helicopter given the power remaining and the amount of power being used by the mission equipment unless the amount of mission equipment is reduced. This flawed process model could result because:
  a) The amount of battery power remaining is not presented to the Flight Crew.
  b) The amount of power time that is remaining given battery power remaining and mission equipment on is not presented to the Flight Crew.
  c) The Flight Crew is unaware of a battery low charge condition due to a failure of the battery low charge caution display.

Scenario 1 represents a situation where the Flight Crew does not provide a control action needed for safe helicopter operations because doing so could result in another potential conflicting safety concern. Scenario 2 and Scenario 3 represent situations where the Flight Crew does not provide a needed control action because of a process model flaw that could result from a component failure, inadequate interpretation of correct and available feedback, and/or missing or inadequate feedback.

With these three causal scenarios generated, it is possible to then mitigate these safety concerns through recommended safety requirements. For instance, four possible safety requirements for Scenario 1 could include:

1. Implement an automated power saving mode that shuts off equipment that is not being used in order to prolong battery life in emergency situations.
2. When battery power is the sole source of power for the helicopter, the Flight Crew must still have access to critical information to make a safe landing under mission conditions.
3. The UH-60MU operator manual should rank order mission equipment in terms of DC power consumption to allow the Flight Crew to determine what mission equipment should be powered off first in the event that mission equipment must be reduced to allow sufficient time for a safe landing.
4. The Flight Crew should receive adequate training and guidance in landing the helicopter when landing under minimum electrical power conditions.

Two possible safety requirements for Scenario 2 may include:

1. The Flight Crew must receive feedback any time battery power is the sole source of DC power being supplied to the helicopter.
2. Further analysis of warning, cautions, and advisories must be conducted to ensure that the hierarchy of displaying WCAs to the Flight Crew does not result in important information being masked in critical emergency situations.

Two possible safety requirements for Scenario 3 may include:

1. The Flight Crew should receive feedback regarding how much battery power remains and the percentage of battery charge that remains while batteries are being used as the sole means of electrical power for the helicopter.
2. The Flight Crew should receive feedback regarding how long the batteries will provide power to the helicopter before being depleted given the amount of equipment that is receiving power.

These three causal scenarios and the associated potential recommended requirements highlight an important point. The possibility of an emergency landing due to loss of main sources of power and mission equipment running solely on battery power was identified in the UH-60MU, as well as older versions of the Blackhawk. There are emergency procedures in the manuals that direct the Flight Crew to land the aircraft as soon as possible and disconnect unnecessary electrical equipment. The manuals, however do not address what equipment should be turned off or their relative power consumption to provide the crew with a realistic process for increasing the time that critical equipment might remain available. STPA allows for not only the identification of unsafe control actions and the causal scenarios that can lead to a hazardous system state, but it also allows for a meaningful consideration of the role of the Flight Crew (human factors) in emergency scenarios. By considering the Flight Crew as an integral component of the system and by

recommending safety requirements and constraints that allow for the Flight Crew to receive appropriate information and feedback necessary for safe helicopter operation, unsafe scenarios such as the three previously described can be adequately mitigated through design or by providing more detailed information in flight manuals and training.

Example FCS Causal Scenarios

Consider the following unsafe control action and associated causal scenarios related to the FCS: *One or more of the FCCs command collective input to the hydraulic servos too long, resulting in an undesirable rotor RPM condition. [H-1, H-2]* There are at least five causal scenarios identified that could lead to this unsafe control action:

- *Scenario 1:* The FCCs are unaware that the desired state has been achieved and continue to supply collective input. The FCCs could have this flawed process model because:
  a) The FCCs are not receiving accurate position feedback from the main rotor servos.
  b) The FCCs are not receiving input from the ICUs to stop supplying swashplate input.

- *Scenario 2:* The FCCs do not send the appropriate response to the aircraft for particular control inputs. This could happen if:
  a) The control logic does not follow intuitive guidelines that have been implemented in earlier aircraft, perhaps because requirements to do so were not included in the software requirements specification.
  b) The hardware on which the FCCs are implemented has failed or is operating in a degraded state.

- *Scenario 3:* The FCCs do not provide feedback to the pilots to stop commanding collective increase when needed because the FADEC is supplying incorrect cues to the FCCs regarding engine conditions.

- *Scenario 4:* The FCCs do not provide feedback to the pilots to stop commanding collective increase when needed because the FCCs are receiving inaccurate NR sensor information from the main rotor.

- *Scenario 5:* The FCCs provide incorrect tactile cueing to the ICUs to properly place the collective to prevent low rotor RPM conditions.

Each of these scenarios could be expanded if necessary to design appropriate mitigation. For example, in Scenario 4, the reasons that the FCCs could receive inaccurate NR sensor information from the main rotor could be identified. Scenario 1 represents a situation where the FCCs continue to provide a control action for too long due to a flawed process model. Scenario 2 represents a component failure or software requirements error that could result in an unsafe control action. Scenarios 3 through 5 represent situations where missing or incorrect feedback results in a hazardous system state. Given only the information in the scenario, mitigation measures could be identified. For example, three safety requirements could be identified related to Scenario 1:

1. The FCCs must perform median testing to determine if feedback received from the main rotor servos is inaccurate.
2. The PR SVO FAULT caution must be presented to the Flight Crew if the FCCs lose communication with a main rotor servo.
3. The EICAS must alert the Flight Crew if the FCCs do not get input from the ICU every x seconds.

If these are mitigation measures are considered to be inadequate, e.g., median testing is not a good enough indicator or simply alerting the crew is not safe enough, then further scenario development could determine the hardware failures that could lead to these requirements and determine if there are ways to control or mitigate them.

Comparison of the STPA UH-60MU results to the Traditional Safety Analysis Results

The five causal scenarios related to the example FCS unsafe control action do not have a direct correlation to any single hazard identified in the previous hazard analyses for the UH-60MU performed using traditional hazard analysis techniques. While there are indirect correlations with failure conditions that were identified previously in the aircraft level FHA, STPA causal scenarios go further in the identification of the causes and mitigation of this unsafe control action.

Reference 6 (the UH-60MU FHA) discusses failure scenarios that allow for an indirect comparison. One failure condition is "loss of auxiliary flight state information [steering cues]" (p. 33). Reference 6 states that such a failure condition would result in the Flight Crew having an increased workload and that the Flight Crew would need to control the aircraft based on visual cues. The hazard severity is classified as critical because the loss of auxiliary flight state information could impact the Flight Crew's ability to properly control the aircraft. One of the causal factors for this hazardous condition is that the Flight Crew does not detect the loss of auxiliary flight state information. As such, traditional hazard analysis techniques place a huge emphasis on the Flight Crew responding correctly when hardware systems fail or the software does the wrong thing. The only alternative is to eliminate all failures. Unfortunately, counting on perfect human behavior is unrealistic and leads to most accidents being blamed on the human operators. STPA instead focuses on the interactions through control and feedback, including the Flight Crew responding to feedback from the system and having the ability to process the feedback and apply the appropriate control/response. These interactions are critical to identifying design flaws where the Flight Crew and systems interaction can lead to process model flaws that contribute to unsafe control actions which then create hazardous conditions for the aircraft and crew. In essence, STPA provides more detailed causal analysis that can be used to provide design features that do

not rely on the crew behaving perfectly in every emergency situation or provide them with help to do that job.

STPA considers a wide range of contributing factors, assessing what can lead to unsafe control actions and hazardous system states. Identifying these contributing factors allows the analyst to recommend much larger number of safety mitigation techniques to constrain the system behavior and mitigate or prevent hazardous system states. More important, STPA can be performed during concept development and before design decisions are made. Therefore, the analysis can guide the design, which allows improving the safety of the design from the beginning and also allows for tracking safety requirements early in the design phases to provide architecture and capability for design improvements during the lifecycle. STPA also considers crew impact and workload much earlier in the design process to insure the aircraft design and crew procedures properly address crew interaction issues as the design evolves.

Reference 6 describes the analysis of the UH-60MU at the aircraft level using FHA as defined in SAE ARP 4761. Reference 7 contains a final Safety Assessment Report (SAR) for the UH-60MU containing the FHA, a Preliminary System Safety Assessment (PSSA), and a System Safety Assessment (SSA). The SAR is described as outlining the results of "a systematic examination of the design and operation of the…aircraft" as well as "a comprehensive evaluation of the safety risks being assumed prior to Combined Team Testing" (Ref. 7, p. 1). These results are compared with the results of STPA on equivalent parts of the helicopter.

One clear difference is that the FHA hazards are limited to "failures" and classified according to the criteria shown in Figure 9. STPA, in contrast, starts from accidents (losses) and prioritizes the accidents (not the hazards) into severity levels. Unlike the typical PHA, STPA does not look at all hazards (usually defined as failures in an FHA) and spend time classifying them. STPA also does not consider probability or likelihood. There is not enough information about the causes at this point in time to determine their likelihood, if that can ever be determined. In addition, assigning probabilities to human decision making and software makes no technical sense and can detract from investigating the most important safety concerns. The usual response to this dilemma using traditional methods is to dismiss humans from the analysis process early and to assign relative reliability levels to the software and assume these reliability levels will be achieved in the software development process.

Probability per Flight Hour				
	Not Specified	1.0E-5	1.0E-7	1.0E-9
Severity Level	**IV**	**III**	**II**	**I**
	Negligible	Marginal	Critical	Catastrophic
	Class D or E mishap damage (less than $20,000). Impact on occupants other than the crew: Less than minor injury or occupational illness (no lost workdays). Impact of the Crew: Less than minor injury or occupational illness (no lost workdays); Slight increase in work load which involve crew actions well within crew capabilities such as routine flight plan changes. Impact on the Mission: Degraded or lack of, mission success. During combat, aircraft and crew could be in jeopardy of loss.	Class C mishap damage (greater than or equal to $20,000 but less than $200,000); Significant reductions in safety margins or functional capabilities. Impact on occupants other than the crew: Minor injury or minor occupational illness (no permanent effect). Impact of the Crew: Minor injury or minor occupational illness (no permanent effect); Physical discomfort or a significant increase in workload or in conditions impairing crew efficiency. Impact on the Mission: Immediate or almost immediate mission abort. Injury or loss of life possible though unlikely unless the aircraft is involved in combat, in which case aircraft may not be able to return to base safely.	Class B mishap damage (greater than or equal to $200,000 but less than $1,000,000); Large reduction in functional capabilities or safety margins. Critical failure conditions can include events that are manageable by the crew by use of proper procedures, which, if not implemented correctly or in a timely manner, may result in a Catastrophic event. Impact on occupants other than the crew: Severe injury or severe occupational illness (permanent partial disability), Impact of the Crew: Severe injury or severe occupational illness (permanent partial disability), Physical distress or excessive workload impairs ability to perform tasks accurately or completely.	Class A mishap damage (greater than or equal to $1,000,000). Impact on occupants other than the crew: Death or permanent total disability. Impact of the Crew: Death or permanent total disability or incapacitation.
Development Assurance Level	**D**	**C**	**B**	**A**

Figure 9. SAR Hazard severity and probability levels (Ref. 7, pp. 13)

STPA selects the accidents to be considered based on severity only. Those with negligible impact would never be considered at all and thus valuable resources would not be spent on them. Once the accidents to be considered are identified and prioritized, then a decision can be made about which ones will be analyzed using STPA and how many resources would be expended for each. Note that the two defined accidents for the UH-60MU STPA analysis (*A-1: Loss of Aircraft; A-2: One or more fatalities or permanent disability)* fall into the category of critical and catastrophic events in Ref. 7 as shown in Figure 9. The causes of only these two accidents were included in the STPA analysis. If other accidents were important to the stakeholders, they could be added to the analysis.

FHA omits humans from the analysis except for assuming that they will mitigate the effects of some failures and thus those failures can be classified as having no safety effect. Too often, aircraft designs assume the Flight Crew will behave perfectly and then blame accidents on imperfect Flight Crew behavior. STPA, in contrast, includes Flight Crew errors in the hazard analysis and uses the information obtained to design the aircraft to reduce those errors. Furthermore, the hazards (failures) identified using traditional techniques can be incomplete. In contrast, the generation of unsafe control actions in STPA follows a rigorous process and, if automated, can be shown to be complete.

In addition, the UH-60MU SAR does not distinguish between the system-level hazards and the causes of those hazards at the component level, as does STPA. Thus, the hazards in the SAR include what STPA categorizes as hazards, unsafe control actions, and causal scenarios (the latter two being identified through the STPA process). Comparing the catastrophic, critical, and marginal hazards (failures) noted in the SAR with the STPA results, the STPA analysis identified all that were associated with the electrical and FCS subsystems in the unsafe control actions or in the causal scenarios that could lead to the unsafe control actions. The STPA process traces these control actions or causes to the specific system-level hazard and thus accident so no information is lost by this hierarchical decomposition, but rather the information is organized in a fashion that allows omissions to be identified. In addition, STPA found many more "hazards" and causes related to the electrical and FCS subsystems, than were identified in the SAR.

Another important comparison is in the classification level of the hazards. Consider the hazards identified as marginal in Ref. 6. These hazards include: *Loss of a single engine, Engine surges during hover taxi, loss of altitude indication in a degraded visual environment, loss of heading indication in a degraded visual environment, loss of airspeed indication in a degraded visual environment, loss of aircraft health information, loss of external communications, loss of internal communication, and stored cargo becoming free during all phases of flight* (pp. 65-66).

One of these hazards classified as marginal is loss of communication. Under most conditions, this classification may be correct, however there may be conditions under which such failures may be more critical. Consider the 1994 loss of a Blackhawk and the lives of all on board due to friendly fire. The investigation report (Ref. 8) cited loss of communication as an important cause of this accident. In this case, the classification as marginal was incorrect.

In addition, combinations of these supposedly marginal failures could lead to serious accidents. For example, consider a situation where there is a degraded visual environment as well as a loss of altitude indication, heading indication, airspeed indication, aircraft health indication, and/or internal communication. Individually, each loss may or may not result in an accident. When multiple losses occur simultaneously, however, the potential for an accident can be raised significantly. Combinations of failures leading to hazards (and thus accidents) are identified by STPA. A specific example is related to the unsafe control action (UCA): *The Flight Crew does not provide collective control input necessary for level flight, resulting in controlled flight into terrain. [H1]*. This UCA could occur if the Flight Crew believes that they are providing sufficient control input to maintain level flight but they are in fact heading in an unsafe trajectory. The Flight Crew could have this flawed process model because:

a) The altitude indicator and attitude indicator are malfunctioning during IFR flight and the pilots are unable to maintain level flight.
b) The Flight Crew believes the aircraft is trimmed in level flight when it is not.
c) The Flight Crew has excessive workload due to other tasks and cannot control the aircraft.
d) The Flight Crew has degraded visual conditions and cannot perceive slow rates of descent that result in a continuous descent.
e) *The Flight Crew does not perceive rising terrain and trims the aircraft for level flight that results in controlled flight into terrain.*

In this scenario, loss of feedback to the Flight Crew is critical and could contribute to a catastrophic hazard (accident). But the SAR classifies the loss of pertinent information to the Flight Crew as marginal due to the probability of occurrence and the severity level of each of the individual failures. STPA, in contrast, identifies this loss of feedback as a more significant hazard due to the complex interaction of system components and the utmost importance of controllers (the Flight Crew) having an accurate process model during flight operations.

The UH-60MU SAR identifies residual hazards and single point failures that can lead to identified hazards.

These are important to analyze further in comparison to the STPA results to understand the difference between the two methods. Ref. 6 discusses a number of single point hardware failures that can lead to the Flight Crew being unable to control the aircraft (pp. 80-86), such as piston nuts breaking and LVDT rod failures. While it is important to design the aircraft to prevent these single point hardware failures, STPA goes a step further. Not only does STPA identify hardware failures as a contributing factor that could lead to the loss of aircraft control, but the analysis also identifies software functions and non-failures that can lead to a lack of aircraft control.

Consider the following unsafe control action: *The Flight Crew does not deflect pedals sufficiently to counter torque from the main rotor, resulting in the Flight Crew losing control of the aircraft and coming into contact with an obstacle in the environment or the terrain [H-1, H-2]*. One of the causal scenarios that could lead to this unsafe control action could be that *the Flight Crew is unaware that the pedals have not been deflected sufficiently to counter the torque from the main rotor.* The Flight Crew could have this flawed process model because:

a) The flight instruments are malfunctioning and providing incorrect or insufficient feedback to the crew about the aircraft state during degraded visual conditions.
b) The flight instruments are operating as intended, but providing insufficient feedback to the crew to apply the proper pedal inputs to control heading of the aircraft to avoid obstacles during degraded visual conditions.
c) The Flight Crew has an incorrect mental model of how the FCS will execute their control inputs to control the aircraft and how the engine will respond to the environmental conditions.
d) The Flight Crew is confused about the current mode of the aircraft automation (in general called mode confusion) and is unaware of the actual control laws that are governing the aircraft at this time.
e) There is incorrect or insufficient control feedback.

Although failures and malfunctions are considered as causal factors for this unsafe control action, the mental (process) model of Flight Crewmembers is also considered and has equivalent importance to that of hardware or component failures. The Flight Crew must receive, process, and act upon numerous sources of feedback in order to interact with the various vehicle and mission systems required for safe operation of the helicopter. The interaction of control mode displays, pedal position, reference settings for various modes, and other visual and proprioceptive feedback can lead to Flight Crew mode confusion, resulting in an unsafe control action, especially if external visual feedback is degraded. By considering not only the feedback that is presented but also how the feedback is presented and how this flow of information fits into the larger system perspective, safety requirements can be generated that not only dictate structural integrity of hardware components, but also system and software design that considers the human in the loop and the role that the Flight Crew plays during operations.

Another example identified in Ref. 6 as a residual hazard is APU chaffing that can result in the helicopter's APU not starting (p. 67). This is important because the APU is used when the loss of one generator occurs during blade deice operations. This residual hazard is considered open in the SAR and no recommendations for mitigation are provided.

While APU chaffing can prevent the blade deice function from operating, there is another scenario found using STPA that could prevent the blade deice function when the APU has not failed. Consider the following unsafe control action: *The Flight Crew does not switch the APU generator power ON when either GEN 1 or GEN 2 are not supplying power to the helicopter and the blade deice system is required to prevent icing. [H-2]* One causal scenario that could lead to this unsafe control action is that *the Flight Crew does not know that APU generator power is needed to run the Blade Deice System and prevent icing.* The Flight Crew could have this incorrect process model because:

a) The ICE DETECTED, MR DEICE FAULT/FAIL, or TR DEICE FAIL cautions are not given to the Flight Crew when insufficient power is available for the Blade Deice System.
b) The Flight Crew does not know that two generators are not providing power to the Blade Deice System.
c) The Flight Crew acknowledged the GEN1 or GEN 2 Fail cautions prior to needing the Blade Deice system but did not start the APU GEN when the additional power was required for the Blade Deice System.

As this causal scenario highlights, there are additional factors besides APU chaffing that could hinder the Blade Deice System from functioning, however, only APU chaffing is documented and referenced in the UH-60MU SAR. In contrast, STPA identifies and documents non-failure factors that could contribute to this hazardous system state. The identification of these additional safety conditions allows the software designers to place more criticality on the hardware and software that is required to generate and display these specific cautions to the Flight Crew.

Addressing the quality of information available to the Flight Crew dramatically expands the specific design features to reduce hazards in the WCA environment. Because traditional techniques focus on failure and on probabilities, the design features considered often involve adding redundancy to reduce the probability of the failure. However, redundancy is not always the best solution and can be very expensive. In general, the UH-60MU FHA (Ref. 6), from which the functional safety requirements were derived for the platform, describe the effect of the failure condition on the aircraft/crew as "describing the effects of the subsystem failure conditions identified as they relate to the crew, aircraft, sub-system, environment, property or

personnel…and includes various physiological and mechanical effects based upon the operational mission" (pp. 16). STPA requirements include failure modes and the interaction of the crew to those scenarios, but also include requirements associated with normal functions that could cause unsafe control actions. By including crew interaction in the early definition of safety requirements, the safety analyst and design team can trace these requirements through the design of the subsystems and address complex interactions across the various subsystems to ensure safe operation under both normal and failure conditions. These human factor requirements do not need to wait for crew station evaluations and the development of simulators to identify crew interaction problems.

Only a few comparative examples have been discussed, however there are many more similar examples that highlight the distinction between STPA and the hazard analysis techniques used in the UH-60MU Safety Assessment Report. Due to differing levels of focus between the traditional hazard analyses and this STPA analysis, a one-to-one comparison of all results is not possible. In general, however, traditional hazard analysis methods focus on failure modes and reducing the probability of hazard occurrences to levels lower than probabilistic design requirements. In contrast, STPA focuses on identifying necessary safety constraints (requirements) on the system and component behavior and ensuring that system controllers have adequate information and feedback to operate the aircraft safely.

MIL-STD-882E Compliance

STPA was designed to be compliant with MIL-STD-882 (all versions) and has been approved previously for use in a defense system safety program plan. STPA provides support for the process described in the standard if no specific tasks are mandated and it also supports many of the important tasks that can be required. Figure 10 shows the general process required if no specific tasks are called out in the contract. STPA directly or indirectly assists in meeting the requirements of all eight elements.

In terms of documenting the system safety approach (Element 1), STPA not only looks at the technical product (the aircraft or weapon) but also can include an overall organizational analysis of the system within which the product fits. That is, it can be used to "describe how the program is integrating risk management into the…Integrated Product and Process Development process and the overall program management structure" (Ref. 9, p. 10) and also analyze this program for its adequacy.

By using a systematic approach to identifying and documenting hazards and risk mitigation measures, STPA is also able to directly meet the requirements for Element 2 and Element 4. While traditional safety analyses address the contribution of failures to creating hazardous states, STPA supports both the identification of failures and non-failures (e.g., system design flaws) as well as addressing the human behavior in response to both failure modes and normal function that can lead to hazardous states.

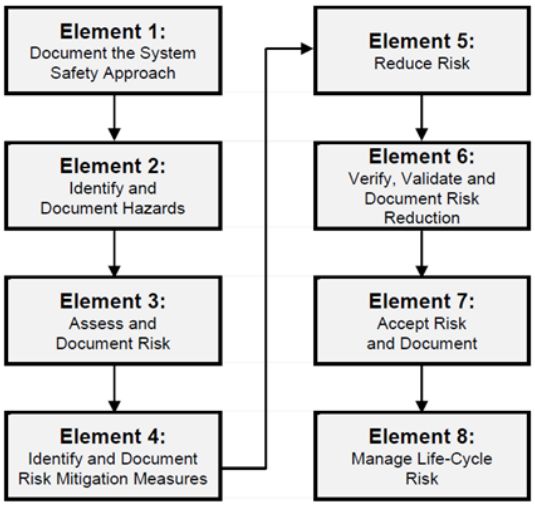

Figure 10. MIL-STD-882E System Safety Process (Ref. 9, p.9)

While STPA allows the analyst to assess and document risk (Element 3), the process purposely does not include assigning severity levels or probabilities of occurrence and therefore only indirectly supports Element 3. However, because STPA is an iterative, top-down hazard analysis that generates traceable results and that can be performed at any stage in the system's development lifecycle, the results that are obtained using this method contribute to programs reducing system risk (Element 5); verifying, validating, and documenting risk reduction (Element 6); and managing the system life-cycle risk (Element 8). In addition to the eight element process, MIL-STD-882E contains various tasks that must be completed if assigned to a program. Below are a few examples of how STPA can support these various tasks.

STPA clearly supports Task Section 100 (System Safety Management). While the management tasks described in this section are focused on traditional hazard analysis techniques, STPA can be integrated and complement these management approaches if not replace them all together. STPA has the added benefit of addressing safety issues associated with the interaction of human operators that can and should be traced to design requirements that mitigate the unsafe control actions throughout the design, including those that are not caused by component failures.

For instance, Task 106 (Hazard Tracking System) is supported by STPA through creating failure mode and normal operations mitigation measures that are "identified and selected with traceability to version specific hardware designs or software releases" (Ref. 9, p. 38). The inclusion of these safety requirements early in the design further supports programmatic monitoring of risk throughout the lifecycle.

STPA also clearly supports the various analysis elements called out in Task Section 200 (Analysis). As an example, Task 205 (System Hazard Analysis) states:

> Perform and document a System Hazard Analysis (SHA) to verify system compliance with requirements to eliminate hazards or reduce the associated risks; to identify previously unidentified hazards associated with the subsystem interfaces and faults; identify hazards associated with the integrated system design, including software and subsystem interfaces; and to recommend actions necessary to eliminate identified hazards or mitigate their associated risks. (Ref. 9, pp. 54)

In fact, STPA is the only existing hazard analysis technique that does satisfy all the specified requirements for a System Hazard Analysis including identifying hazards associated with integrated system design and not just component failures.

CONCLUSIONS

1. The demonstration of STPA on the UH-60MU WCA system showed it to be a viable and useful hazard analysis process that identified all of the hazardous conditions related to the electrical system and FCS documented in traditional safety assessment reports. Furthermore, STPA identified additional hazard causes that were not documented by previous traditional analyses. As such, STPA can be relied upon in the future to increase helicopter safety and strengthen the hazard analysis process for Army aviation.

2. The WCA system is intended to aid the Flight Crew in responding to failure and emergency situations. As such, even if this system operates properly and as intended with no component failures, there can still be design flaws that lead to hazardous system states. Such flaws are manifested when intended and correct feedback is presented to the Flight Crew through WCA mechanisms but that feedback does not have the desired result of aiding the Flight Crew in preventing an accident. An example is the masking of a caution due to priority ranking and the manner in which two cautions are presented to the Flight Crew during operations. These nuances are not incorporated into traditional hazard analysis techniques, but are a focus of STPA.

3. STPA's top down approach assists in scoping and reducing the analysis effort. Given the very large number of system interactions in the UH-60MU and the fact that the WCA system is directly or indirectly connected with every other system component and responsible for presenting critical safety information and feedback to the helicopter's Flight Crew, analyzing every possible failure is impossible. By using the hierarchical abstraction inherent in STPA, i.e., starting with the few system hazards and then analyzing them by identifying unsafe control actions (component hazards leading to the system hazards) and their causal scenarios, the analysis effort is limited to the most serious hazards and does not require considering all component failures. By first modeling the functional control structure and addressing the control and feedback mechanisms between the Flight Crew and the various subsystems, the safety analyst can better create and refine system and component safety requirements that may involve complex system interactions early in the design process. They can then be traced throughout hardware and software development, with mitigations included as a function of design and not by adding costly redundancy or relying on human procedures to mitigate hazards when design changes become unaffordable late in the program.

4. While STPA can be used at any life cycle stage, including after the design is complete, as shown in the UH-60MU WCA analysis in this paper, it provides the most benefits by applying it early in the design effort and using the results to guide design decisions and design safety into the aircraft from the beginning. STPA also is a deliberate and effective approach for communicating safety requirements in the early stages of design and contracting.

5. The description of the organizational control structures shown in Figures 2 and 3 and the aircraft functional control structure shown in Figure 4 represent generic control structures that can be used for most military helicopters. As such, a generic STPA analysis of unsafe control actions can be conducted and driven into system specifications and contracting language to set the conditions for further analysis at the system level. By including an aircraft level STPA on a functional control structure similar to Figure 4 or 5 as part of the documentation provided by the government to the contractor, the government can drive the safety process from the beginning of design and set expectations for the traceability of specific hazardous conditions throughout the design process, including those that involve complex subsystem and human interaction.

6. Identification of system safety requirements using STPA supports both MIL-STD-882E and SAE ARP 5754A standards for military and commercial aircraft, respectively.

7. STPA is compliant with the requirements for system hazard analysis as set forth by MIL-STD-882E and the SAE ARP 4754A standard used for commercial aircraft.

Blake Abrecht babrecht@mit.edu
Dave Arterburn arterbd@uah.edu
David Horney dchorney@mit.edu
Jon Schneider jjschnei@mit.edu
Brandon Abel abelb@mit.edu
Nancy Leveson leveson@mit.edu

ACKNOWLEDGMENTS

The authors would like to thank the Futures Team of the Utility Helicopter Project Office (UHPO) and engineers and program managers from Sikorsky Aircraft Corporation (SAC) for their support in conducting this work. Travis Sinclair (UHPO), Igor Cherepinsky (SAC), Thomas Page (SAC), Al Oliver (SAC) and Jesse Lesperance (SAC) were extremely helpful in providing access to documents needed to conduct this study and in answering questions that supported the completion of this work.

REFERENCES

[1]Leveson, N. *Engineering a Safer World*, MIT Press, Cambridge, MA, 2012.

[2]Thomas, J. "Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis," MIT Ph.D. Dissertation. June, 2013.

[3]Leveson, N., Wilkinson, C., Fleming, C., Thomas, J., and Tracy, I., "A Comparison of STPA and the ARP 4761 Safety Assessment Process," MIT PSAS Technical Report, Rev.1. October, 2014.

[4]Sikorsky Aircraft Corporation, "A-144 1265: Sikorsky UH-60M BLACK HAWK Helicopter," March, 2014.

[5]Department of the Army, "Army Aviation Accident Prevention Program Rapid Action Revision (RAR)", DA PAM 385-90. 24 February, 2010.

[6]Sikorsky Aircraft Corporation, "Functional Hazard Assessment for the UH-60M Upgrade Aircraft," Document Number SER-703359. 21 September, 2005.

[7]Sikorsky Aircraft Corporation, "Safety Assessment Report for the UH-60M Upgrade Aircraft," Document Number SER-703655. 03 January, 2012.

[8]Andrus, J. G., "Aircraft Accident Investigation Board Report: U.S. Army UH-60 Black Hawk Helicopters 87-26000 and 88-26060," Department of Defense, July 13, 1994.

[9]Department of Defense Standard Practice, "System Safety," MIL-STD-882E. 11 May, 2012.