Hazard Analysis for Rotorcraft

2nd Lt. Blake Abrecht, USAF
Massachusetts Institute of Technology
Engineering Systems Division Master's Student

Mr. Dave Arterburn
Director, Rotorcraft Systems Engineering and Simulation Center
University of Alabama in Huntsville

2nd Lt. David Horney, USAF
2nd Lt. Jon Schneider, USAF
Massachusetts Institute of Technology
Aeronautics and Astronautics Master's Student

Major Brandon Abel, USAF
Massachusetts Institute of Technology
Aeronautics and Astronautics PhD Candidate

Dr. Nancy Leveson
Professor of Aeronautics and Astronautics
Massachusetts Institute of Technology

22 March 2016

Disclaimer

The views expressed in this presentation are those of the authors and do not reflect the official policy or position of the United States Air Force, United States Army, Department of Defense, or the U.S. Government.

Case Study

Solem, Courtney. "Using Fly-By-Wire Technology in Future Models of the UH-60 and other Rotary Wing Aircraft," Oregon NAZA Space Consortium.

Solem, Courtney. "Using Fly-By-Wire Technology in Future Models of the UH-60 and other Rotary Wing Aircraft," Oregon NAZA Space Consortium.

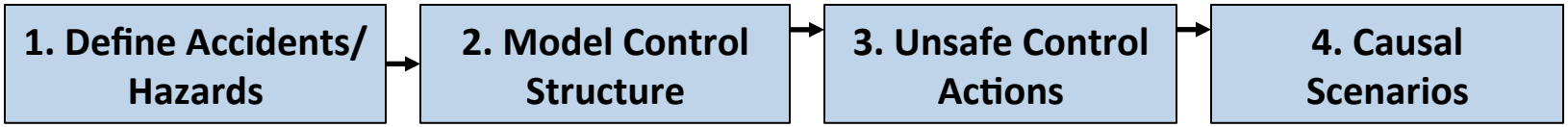
Havir, T. J., Durbin, D. B., and Frederick, L. J., "Human Factors Assessment of the UH-60M Common Avionics Architecture System (CAAS) Crew Station During the Limited User Evaluation (LEUE)," Army Research Laboratory. December 2005.

Apply Systems Theoretic Process Analysis (STPA) to the analysis of the Warning, Caution, and Advisory System of the UH-60M Upgrade

Outline

- UH-60MU WCA Case Study
- Comparison to Traditional Techniques
- MIL-STD-882E Compliance
- Summary

STPA Process



1: Identify and define accidents and hazards

- Accident (loss): "an undesired or unplanned event that results in a loss"
- Hazard: "A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident"

2: Model the control structure for the system

- Control structure at the organizational level
- Functional control structure at the system level

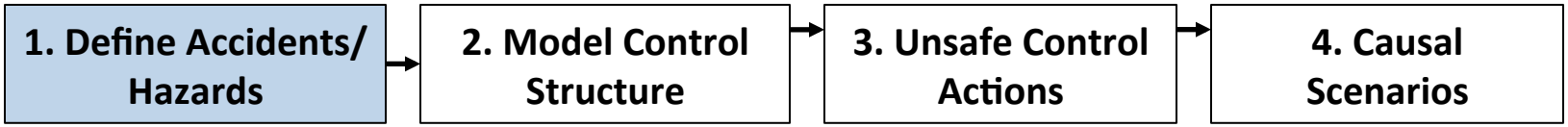
3: Identify unsafe control actions (UCAs)

- UCAs lead to a hazardous system state

4: Identify causal factors and generate scenarios

- Causal scenarios identified for each unsafe control action

UH-60MU WCA Case Study



Defined Accidents

A-1: Loss or major damage to aircraft

A-2: One or more fatalities or significant injuries

Defined Hazards

H-1: Violation of minimum separation requirements (A-1, A-2)

H-2: Lack of aircraft control (A-1, A-2)

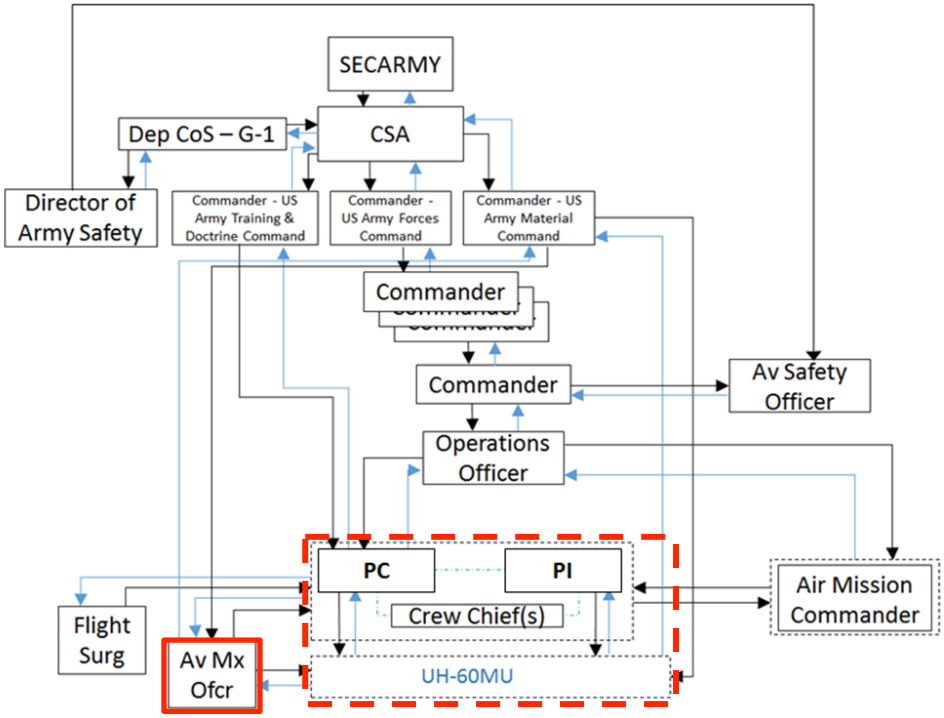
Scope of Case Study

Limited to WCAs and systems associated with the Electrical and Flight Control Subsystems of the UH-60M Upgrade

UH-60MU WCA Case Study

1. Define Accidents/ Hazards → **2. Model Control Structure** → 3. Unsafe Control Actions → 4. Causal Scenarios

Training and Peacetime Organizational Safety Control Structure



- Continuously monitor quality control.
- Ensure adequate training of UH-60MU maintenance personnel.
- Ensure proper and timely UH-60MU inspections.
- Ensure adequate UH-60MU program supervision.
- Provide maintenance personnel with lessons-to-be-learned from all platform accident summaries.

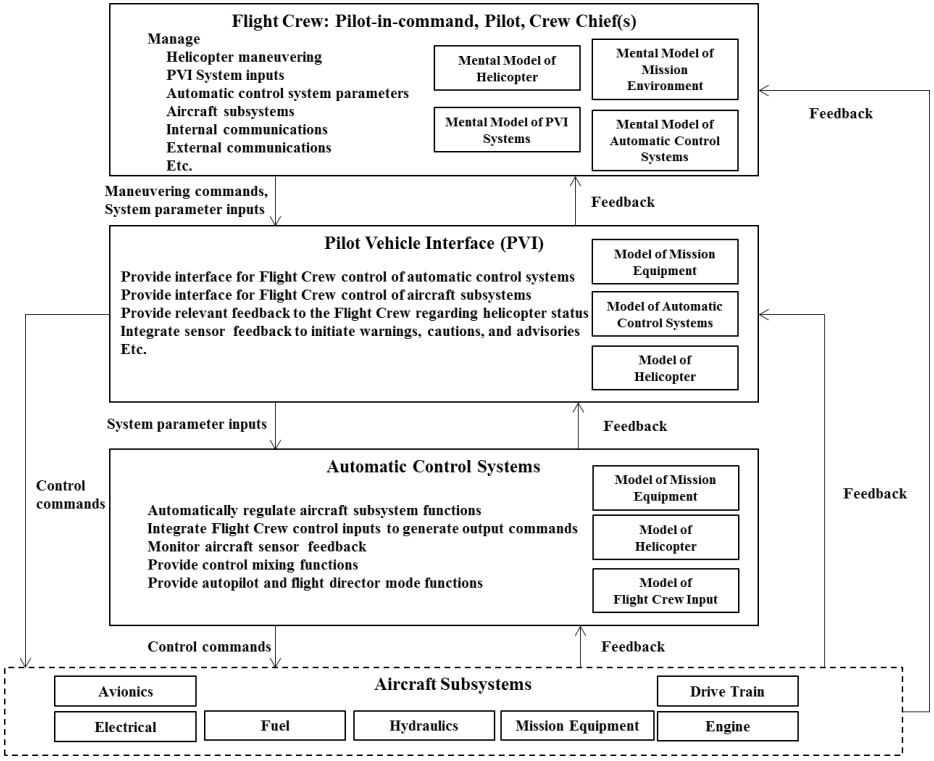
Focus of this analysis

Organizational decisions, regulations, training procedures/requirements, operations orders, etc. can all affect UH-60MU operations

UH-60MU WCA Case Study

1. Define Accidents/ Hazards → **2. Model Control Structure** → 3. Unsafe Control Actions → 4. Causal Scenarios

Functional Control Structure (1): Safety Related Responsibilities/Process Models

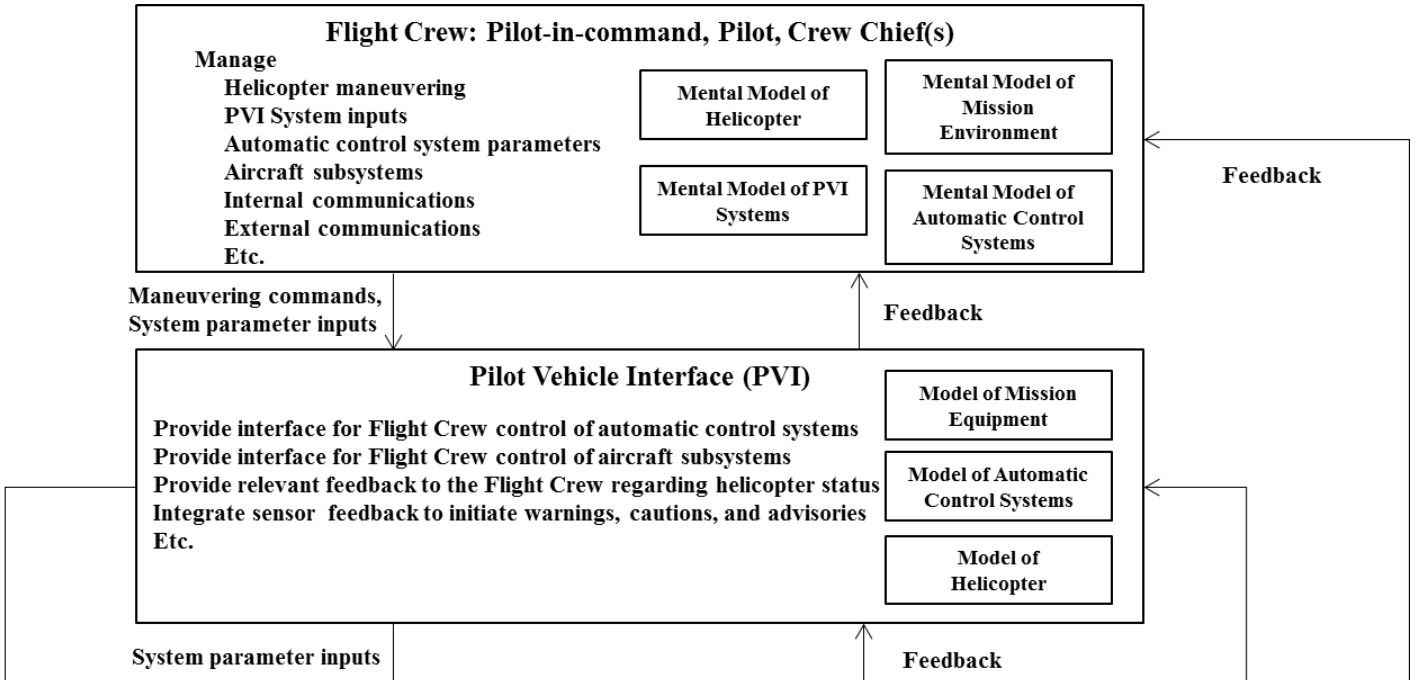


Each controller within the UH-60MU has safety-related responsibilities and process models that inform action generation

UH-60MU WCA Case Study

1. Define Accidents/ Hazards → **2. Model Control Structure** → 3. Unsafe Control Actions → 4. Causal Scenarios

Functional Control Structure (1): Safety Related Responsibilities/Process Models

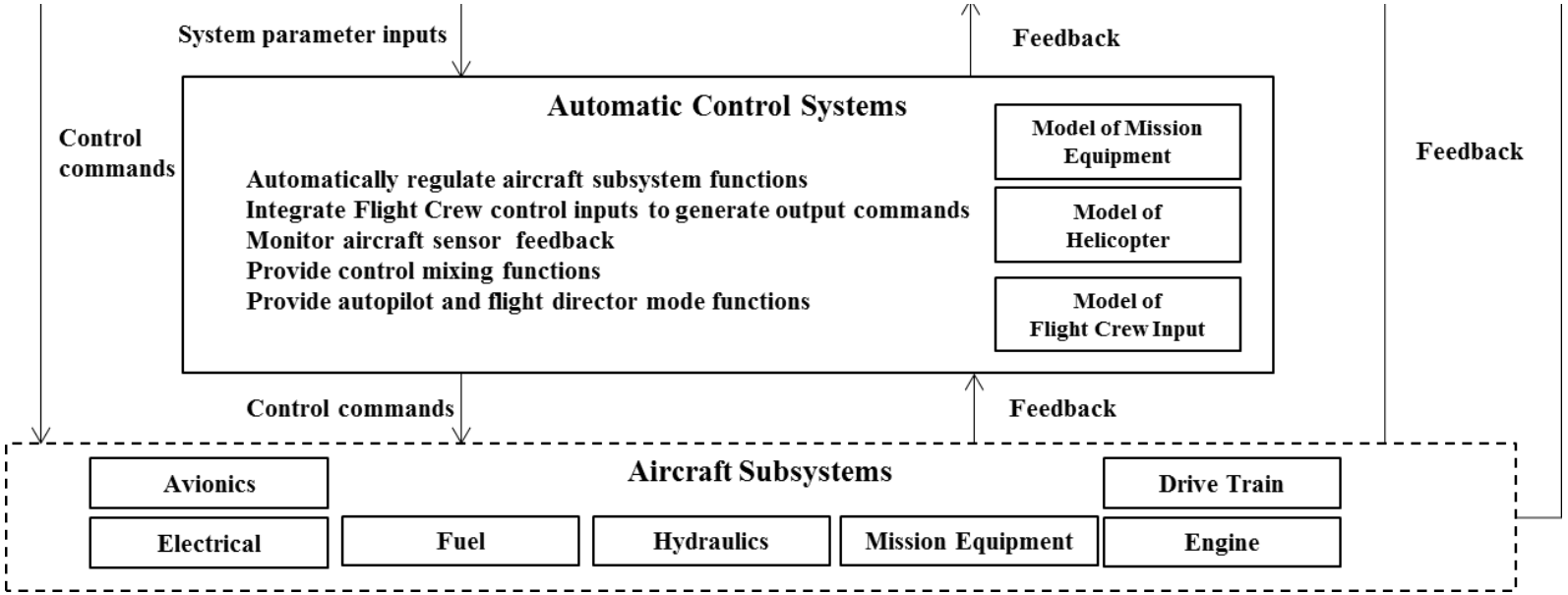


Each controller within the UH-60MU has safety-related responsibilities and process models that inform action generation

UH-60MU WCA Case Study

1. Define Accidents/ Hazards → **2. Model Control Structure** → 3. Unsafe Control Actions → 4. Causal Scenarios

Functional Control Structure (1): Safety Related Responsibilities/Process Models

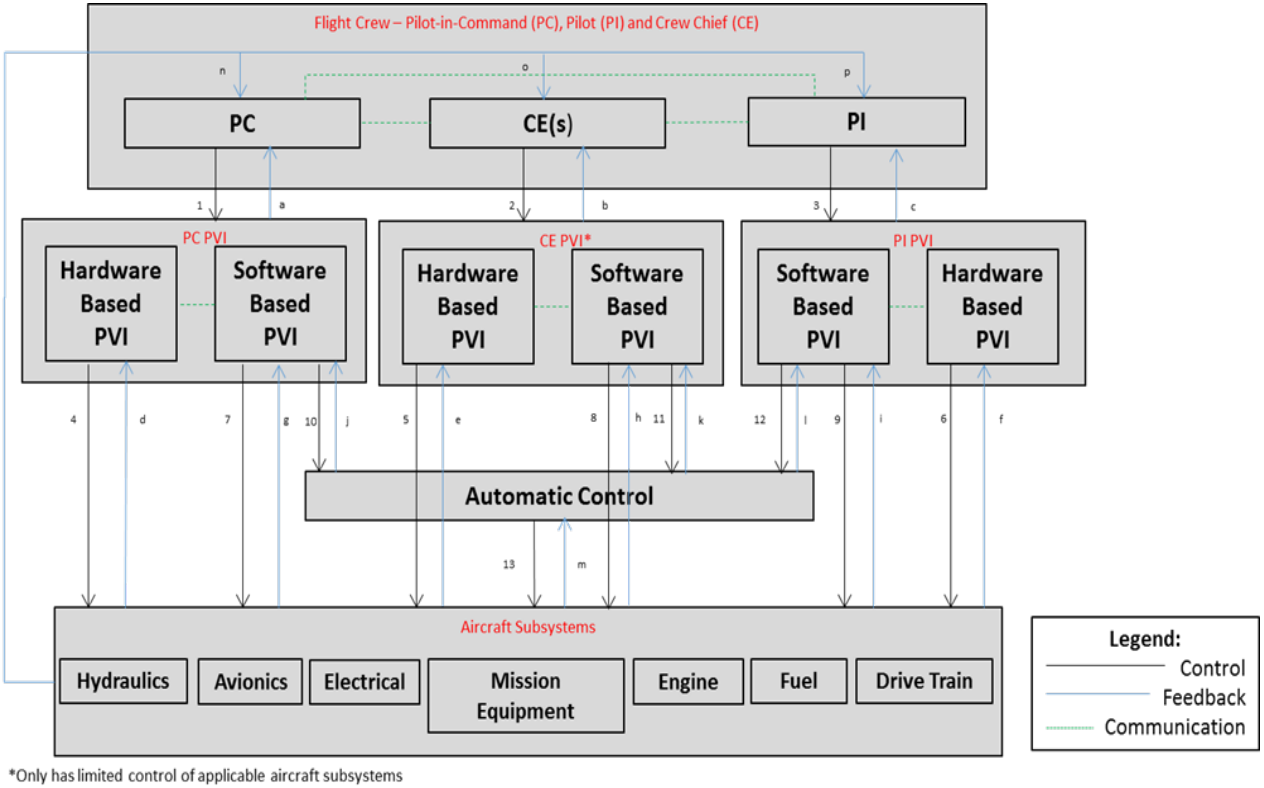


Each controller within the UH-60MU has safety-related responsibilities and process models that inform action generation

UH-60MU WCA Case Study

1. Define Accidents/ Hazards → **2. Model Control Structure** → 3. Unsafe Control Actions → 4. Causal Scenarios

Functional Control Structure (2): Feedback Loops and Functional Relationship

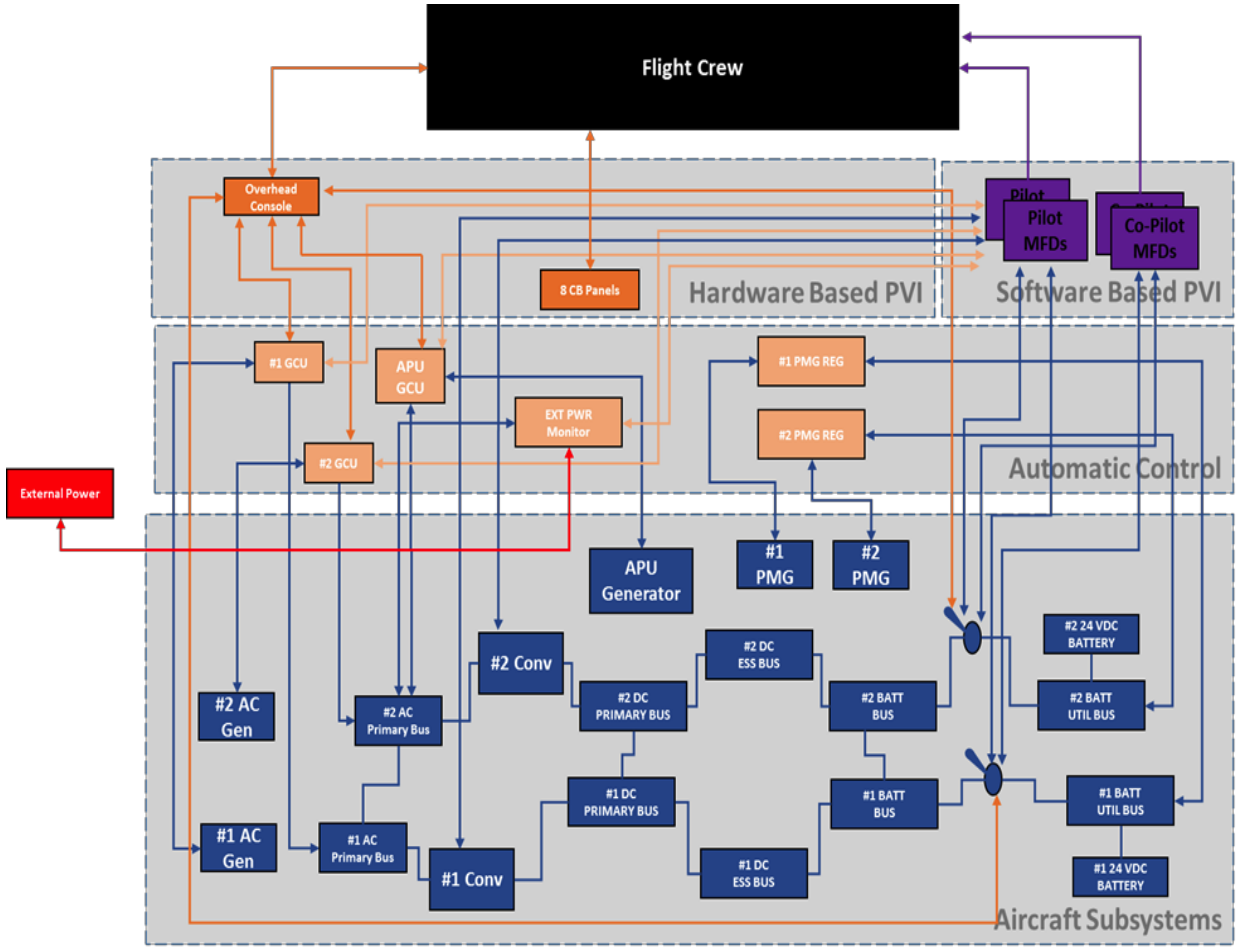


The relevant control actions and feedback within each feedback loop is analyzed to determine unsafe control actions and generate causal scenarios

UH-60MU WCA Case Study

1. Define Accidents/ Hazards → **2. Model Control Structure** → 3. Unsafe Control Actions → 4. Causal Scenarios

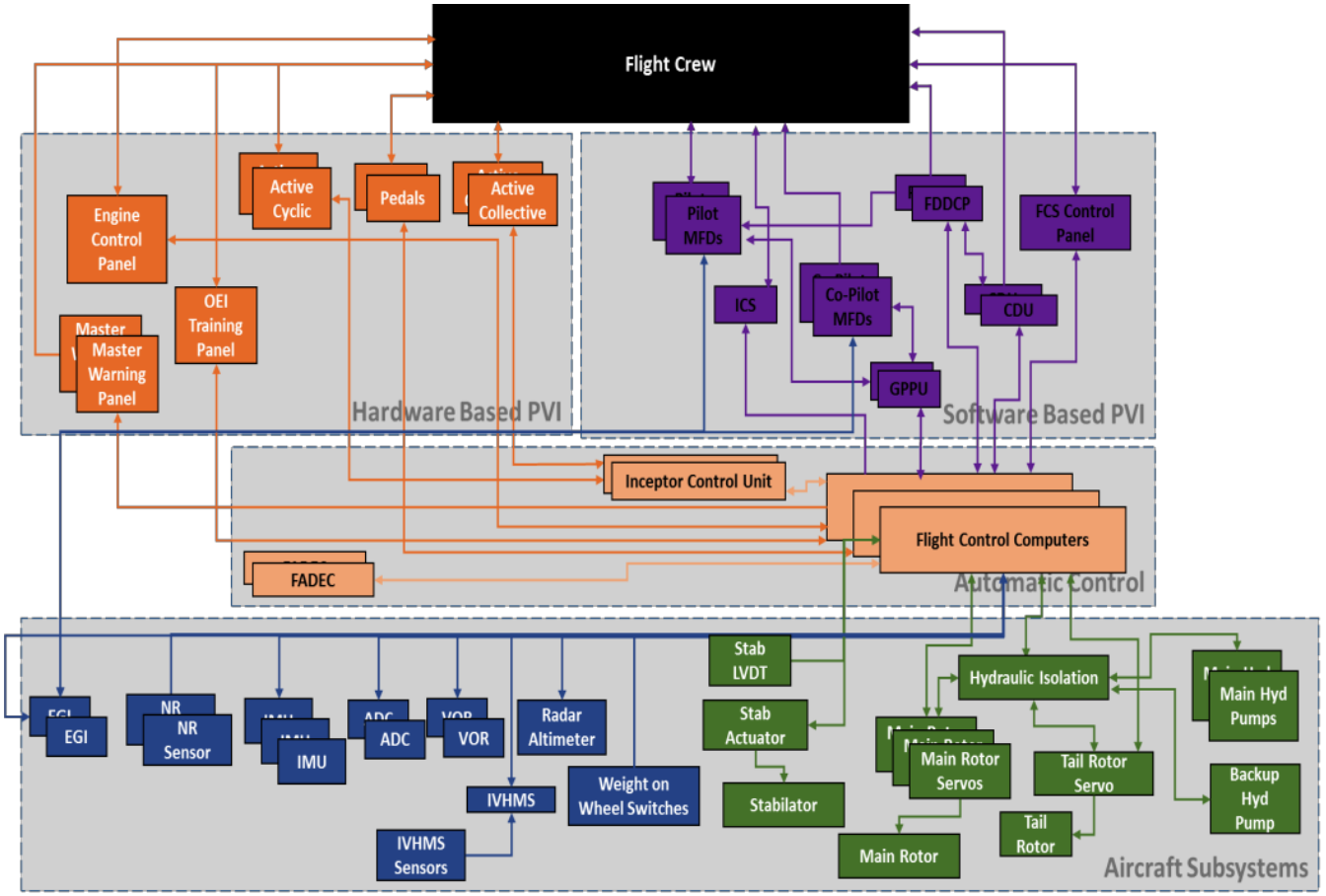
Functional Control Structure (3): Detailed Electrical Subsystem Components



UH-60MU WCA Case Study

1. Define Accidents/ Hazards → **2. Model Control Structure** → 3. Unsafe Control Actions → 4. Causal Scenarios

Functional Control Structure (4): Detailed FCS Components



UH-60MU WCA Case Study

1. Define Accidents/ Hazards → 2. Model Control Structure → **3. Unsafe Control Actions** → 4. Causal Scenarios

Four parts of an unsafe control action:

Source Controller
- Flight Crew
- PVI Components
- Automatic Controllers (FCC)

Type of Control Action
- Does not provide
- Does provide
- Provided in the wrong order/ incorrect timing
- Stopped too soon/applied too long

Control Action
- The action that the controller provides (or does not provide)

Context
- The scenario that makes the control action unsafe

(Example UCA Table)

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 fails to present 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

This technique identified 126 unsafe control actions as part of this case study

UH-60MU WCA Case Study

1. Define Accidents/ Hazards → 2. Model Control Structure → 3. Unsafe Control Actions → **4. Causal Scenarios**

- **Potential causes of unsafe control**
  - Process model flaws
  - Inadequate design requirements
  - Conflicting feedback
  - Inadequate feedback
  - Missing feedback
  - Inappropriate control actions
  - Ineffective control actions
  - Missing control actions
  - Physical component failures
  - Etc.

Causal scenarios allow for more detailed, traceable safety recommendations to be made for safe UH-60MU operation

STPA Unsafe Control Action

The Flight Crew does not provide collective control input necessary for level flight, resulting in controlled flight into terrain

Scenario 1: The Flight Crew has a flawed process model and believes they are providing sufficient control input to maintain level flight. This flawed process model could result from:

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

Outline

- UH-60MU WCA Case Study
- Comparison to Traditional Techniques
  - Hazard Classification example
  - Hazard Tracking Worksheet example
  - Failure based Hazard example
- MIL-STD-882E Compliance
- Summary

UH-60MU SAR Hazard Classification

UH-60MU SAR marginal hazards

- Loss of altitude indication in DVE
- Loss of heading indication in DVE
- Loss of airspeed indication in DVE
- Loss of aircraft health information
- Loss of external communications
- Loss of internal communications

UH-60MU SAR identifies various hazards as marginal that could lead to a catastrophic accident

STPA Unsafe Control Action

The Flight Crew does not provide collective control input necessary for level flight, resulting in controlled flight into terrain

Scenario 1: The Flight Crew has a flawed process model and believes they are providing sufficient control input to maintain level flight. This flawed process model could result from:

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

UH-60MU SAR Hazard Tracking Worksheet

Hazardous Condition: **Loss of Displayed Flight State Information**

Hazard Severity:
Catastropic

Frequency Rationale:
Improbable.

FTA Reference: SSA SER 703654 Rev 2 Appendix

Causal Factors:
1. MFD failure
2. Loss of power
3. FCC hardware/software fault
4. ADC failure
5. EGI failure
6. ESIS failure

Detection/Annunciation:
a. Pilot would notice blank attitude, altitude, airspeed, and heading on MFDs
b. Pilot would notice blank attitude, altitude, airspeed, and heading on ESIS
c. MFD, CDU, and FCC statuses displayed within the System Status on CDUs and MFDs

Existing Controls:
1. Redundant Pilot and Copilot MFD Displays
2. Triple Redundant FCC
3. FCC Level A Software
4. Independent backup ESIS
5. Redundant Pilot and Copilot ADCs
6. Redundant Pilot and Copilot EGIs
7. Redundant heading/attitude sources (EGIs), altitude sources (RALT, ADCs), airspeed sources (ADCs)
8. Electrical System Design, multiple AC & DC buses
9. Failure Detection of MFD1-4, CDU1-2, FCC1-3, EGI1-2, ADC1-2, RALT

- **Causal factors of this hazard condition only include failures**
- **An assumption is made that the Flight Crew will not only recognize this hazard condition, but also that they will respond appropriately.**
- **As a result, existing controls that are considered adequate for mitigation only include redundant systems and Level A software.**

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

UH-60MU SAR Failure based Hazards

UH-60MU SAR residual hazard

- APU Chaffing can lead to failure of the UH-60MU APU and can affect blade deice operations when the loss of a main generator occurs

STPA Unsafe Control Action

UCA: The Flight Crew does not switch 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.

Scenario 1: The Flight Crew does not know that APU generator power is needed to run the Blade Deice System. This flawed process model could result from:

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

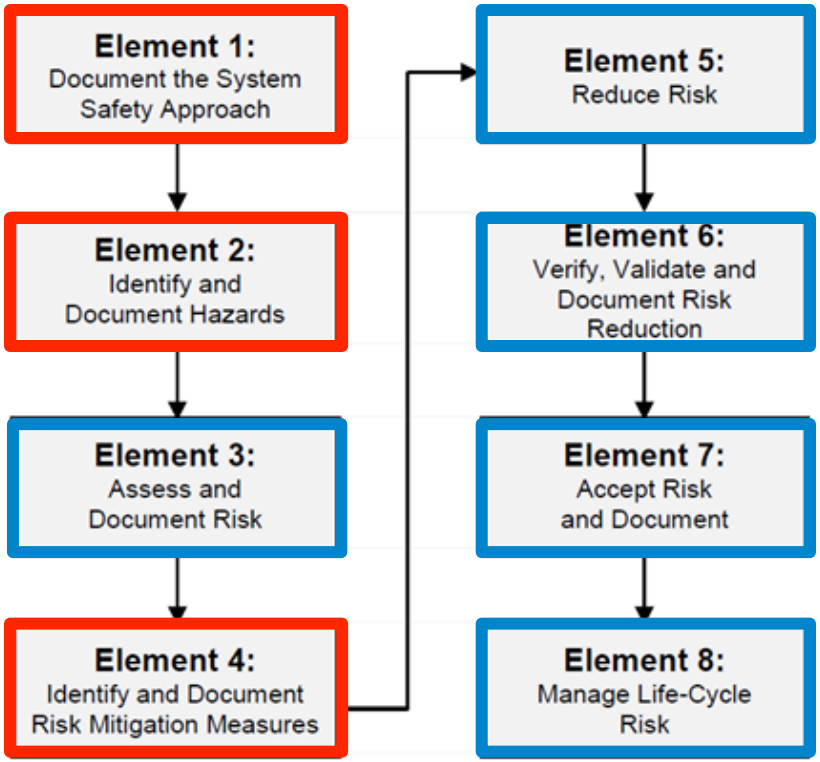
c) The Flight Crew acknowledged the GEN1 or GEN 2 Fail cautions prior to needing the Blade Deice system and failed to start the APU GEN when the additional power was required for the Blade Deice System

STPA identifies non-failure scenarios that can lead to a hazardous system state that are not documented by traditional hazard analysis techniques

Outline

- STPA Background
- UH-60MU WCA Case Study
- Comparison to Traditional Techniques
- MIL-STD-882E Compliance
- Summary

MIL-STD-882E Compliance



MIL-STD-882E System Safety Process

Fully addressed through use of STPA

Partially addressed through use of STPA

MIL-STD-882E Compliance

STPA supports Task Section 100- (System Safety) Management

- **Task 106: Hazard Tracking System**
  - **STPA allows for the generation of normal operations mitigation measures that are "identified and selected with traceability to version specific hardware designs or software releases" (MIL-STD-882E, pp. 38)**

STPA supports Task Section 200- Analysis

- **Task 205: System Hazard Analysis**
  - **"Identify previously unidentified hazards associated with subsystem interfaces and faults; identify hazards associated with the integrated system design, including software and subsystem interfaces; recommend actions necessary to eliminate identified hazards or mitigate their associated risks" (MIL-STD-882E, pp. 54)**

Summary

- STPA shown to be a viable and useful hazard analysis process
- STPA identified additional hazard causes not documented by previous traditional analyses and includes humans as system components.
- STPA's top down approach assists in scoping and reducing the analysis effort
- The hierarchal abstraction of STPA limits the analysis to the most serious hazards and does not require considering all component failures
- STPA can be used at any life cycle stage
  - Provides the most benefits in the early stages of design and contracting (when existing methods are not feasible)
  - Can be included in system specifications and contracting language
  - Using STPA supports both MIL-STD-882E and SAE ARP 5754A standards for military and commercial aircraft, respectively