A New Approach to Hazard Analysis for Naval Systems

2nd Lt. Blake Abrecht, USAF
MIT, Engineering Systems Division

22 March 2016

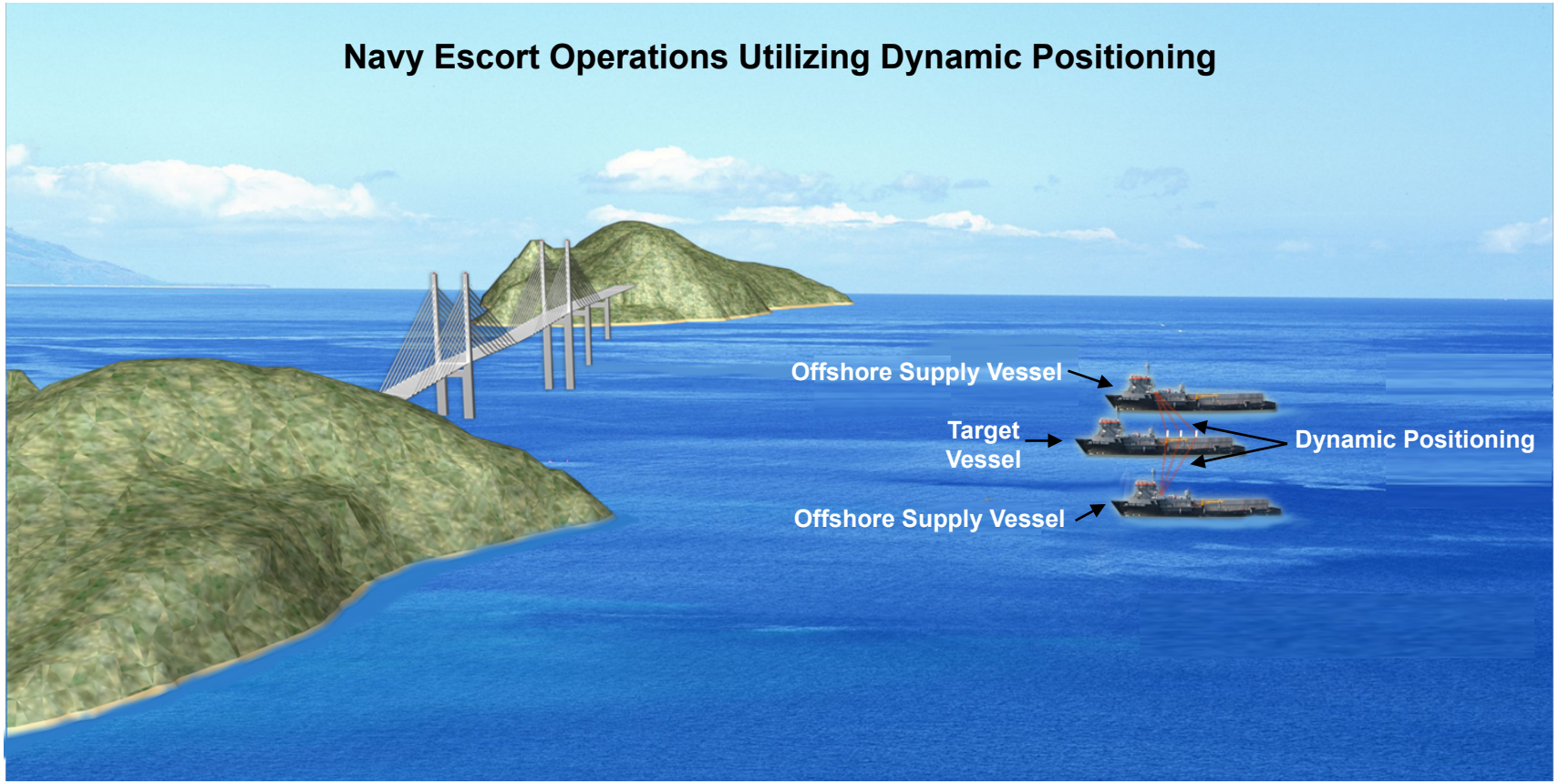




Disclaimer

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

Case Study



Systems Theoretic Process Analysis (STPA) is a new technique that identifies hazards for Offshore Supply Vessel (OSV) Dynamic Positioning Systems more effectively than traditional analysis methods.



Outline

- Executive Summary
- Dynamic Positioning System Case Study
- Comparison of STPA Results to FTA/FMEA
- MIL-STD-882E Compliance
- Summary

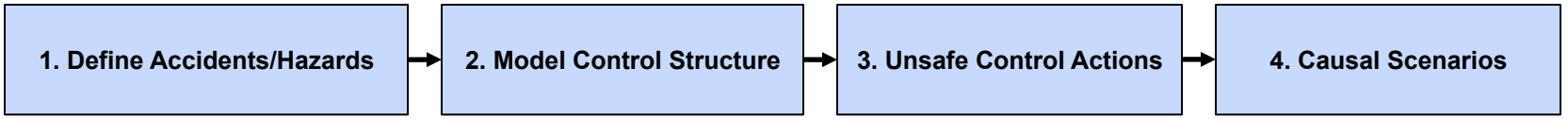


Executive Summary

- STPA applied to the OSV dynamic positioning system identified…
  - 46 unsafe control actions
  - 37 system-level safety constraints
  - 171 additional recommended safety requirements
- STPA identified all system component failures found via Fault Tree Analysis (FTA) & Failure Modes and Effect Analysis (FMEA) and also identified numerous additional safety concerns not found through FTA & FMEA
- Results generated by STPA better satisfy the requirements for systems hazard analysis set forth by MIL-STD-882E than traditional hazard analysis techniques



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

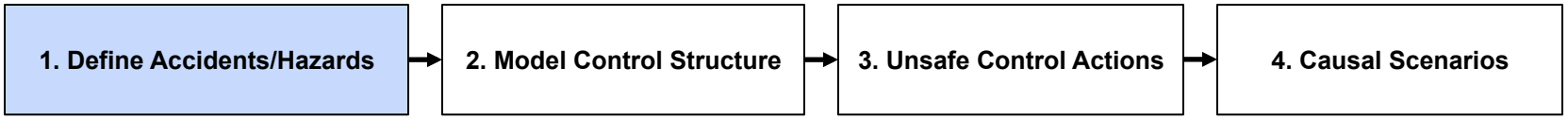
3: Identify unsafe control actions (UCAs)

- UCAs lead to a hazardous system state

4: Identify causal factors and create scenarios

- Causal scenarios identified for each unsafe control action

OSV Dynamic Positioning Case Study



Defined Accidents

A-1: Multi-vessel collision (OSV-OSV, OSV-Target Vessel)
A-2: OSV collision with external structure (static, dynamic)
A-3: OSV running aground (shore or ocean floor)

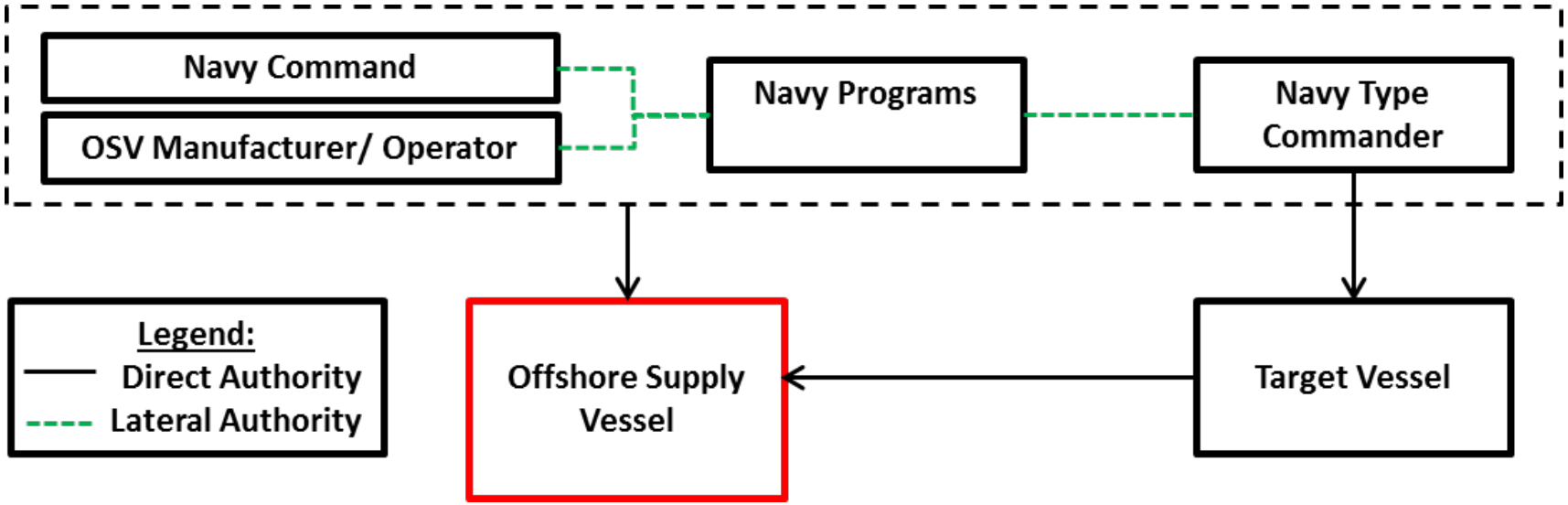
Defined Hazards

H-1: Loss of minimum separation (A-1, A-2, A-3)
H-2: Loss of OSV Control (A-1, A-2, A-3)

OSV Dynamic Positioning Case Study

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

Organizational Control Structure



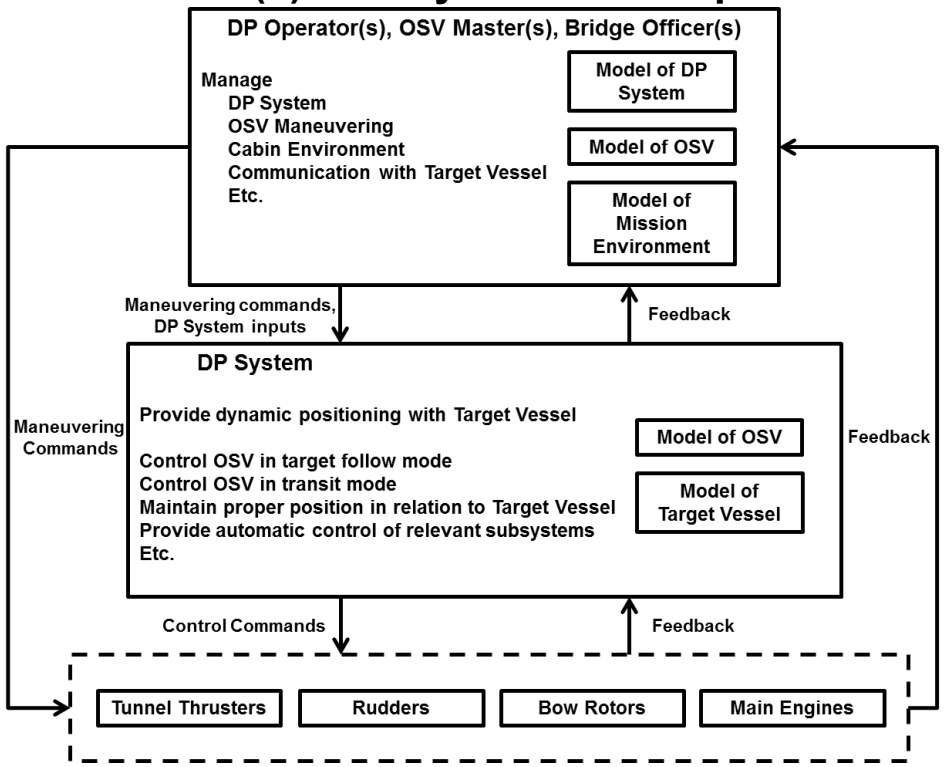
Focus of this analysis

Organizational decisions, regulations, training procedures/requirements, operations orders, etc. can all affect Offshore Supply Vessel operations

OSV Dynamic Positioning 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

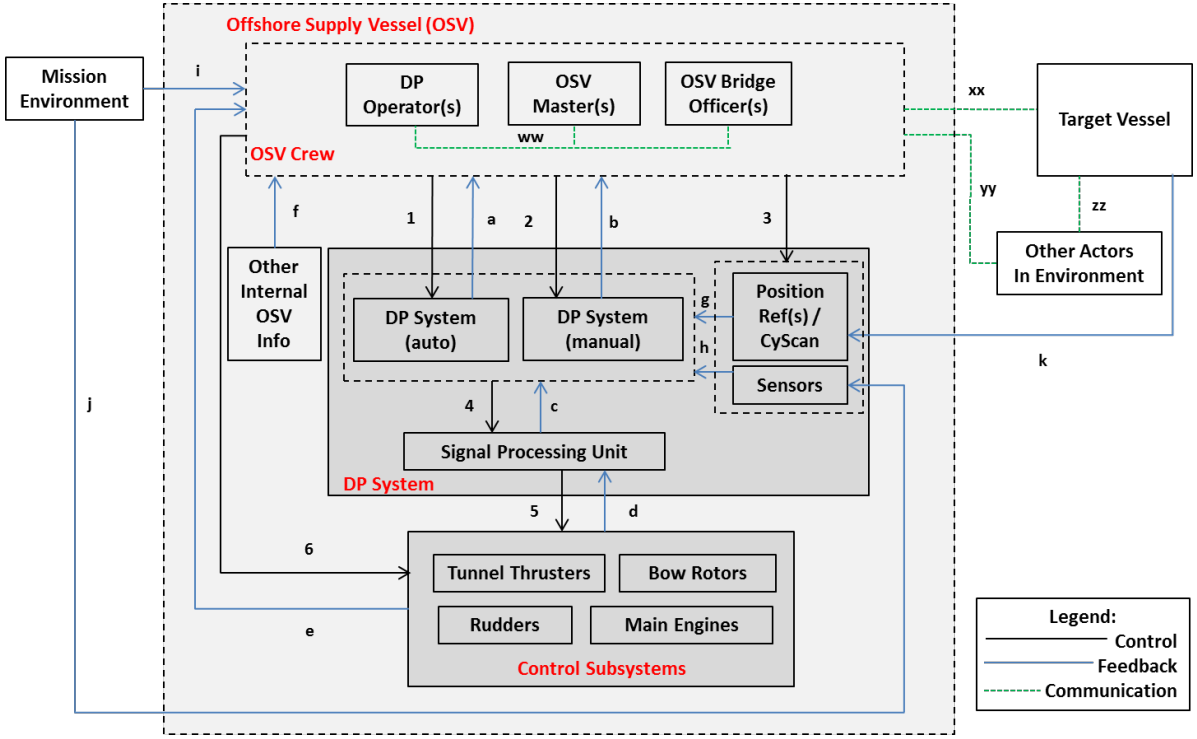


Process (mental) models are updated using feedback from the controlled process and are used to inform action generation

OSV Dynamic Positioning 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

OSV Dynamic Positioning 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
- OSV Crew
- DP System
- SPU

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/order	Stopped too soon/applied too long
Provide directional command (DP Auto; target follow mode)	UCA16: DP System (auto) does not provide a directional command during automatic operations when a maneuver is required. [H-1, H-2]	UCA18: DP System (auto) gives an unsafe directional command to maneuver towards the target vessel, terrain, an external structure, or another vessel during automatic operations. [H-1, H-2]	UCA21: DP System (auto) gives a maneuvering command to the OSV x seconds too late to perform the maneuver successfully. [H-1, H-2]	UCA22: DP System (auto) stops providing a directional command to the OSV before the desired maneuver is accomplished. [H-1]

DP System (auto)	does not provide	a directional command	during automatic operations when a maneuver is required
Source Controller	Type of Control Action	Control Action	Context

This technique identified 46 unsafe control actions as part of this case study

OSV Dynamic Positioning 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.

Unsafe Control Action- UCA13: OSV Crew does not update a system parameter when a changing situation requires a system parameter to be updated. [H-1, H-2]

Scenario 13: During operations, many user configurable parameters will not change; however, some user configurable parameters will require change as dynamic situations progress. As such, changes in user configurable parameters are mainly limited to DP system threshold (alarm) values. As the lateral separation distance between the OSV and the target vessel changes, the OSV Crew must change the DP system thresholds values as the relative positions of the two vessels changes. If the lateral separation between the OSV and the target vessel is changing often and the OSV Crew is experiencing a high-workload, high stress environment, the OSV Crew may forget to change the DP system threshold values.

Possible requirements for Scenario 13:

1. DP System threshold values must be compared to other available information to verify that the threshold value is appropriate for a given operation. If the threshold value is too close for a given operation, the OSV Crew should receive feedback and be required to change the threshold value.
2. The OSV Crew must receive feedback to actively verify the DP system threshold yellow/red alarm values if no change is made to the parameter value when lateral separation distances change by x feet.
3. The OSV Crew should receive trend analysis information regarding the OSV's position relative to the target vessel to help them better understand the future state of the OSV.

† Abrecht, B., Leveson, N., "Systems Theoretic Process Analysis (STPA) of an Offshore Supply Vessel Dynamic Positioning System," pp. 21.

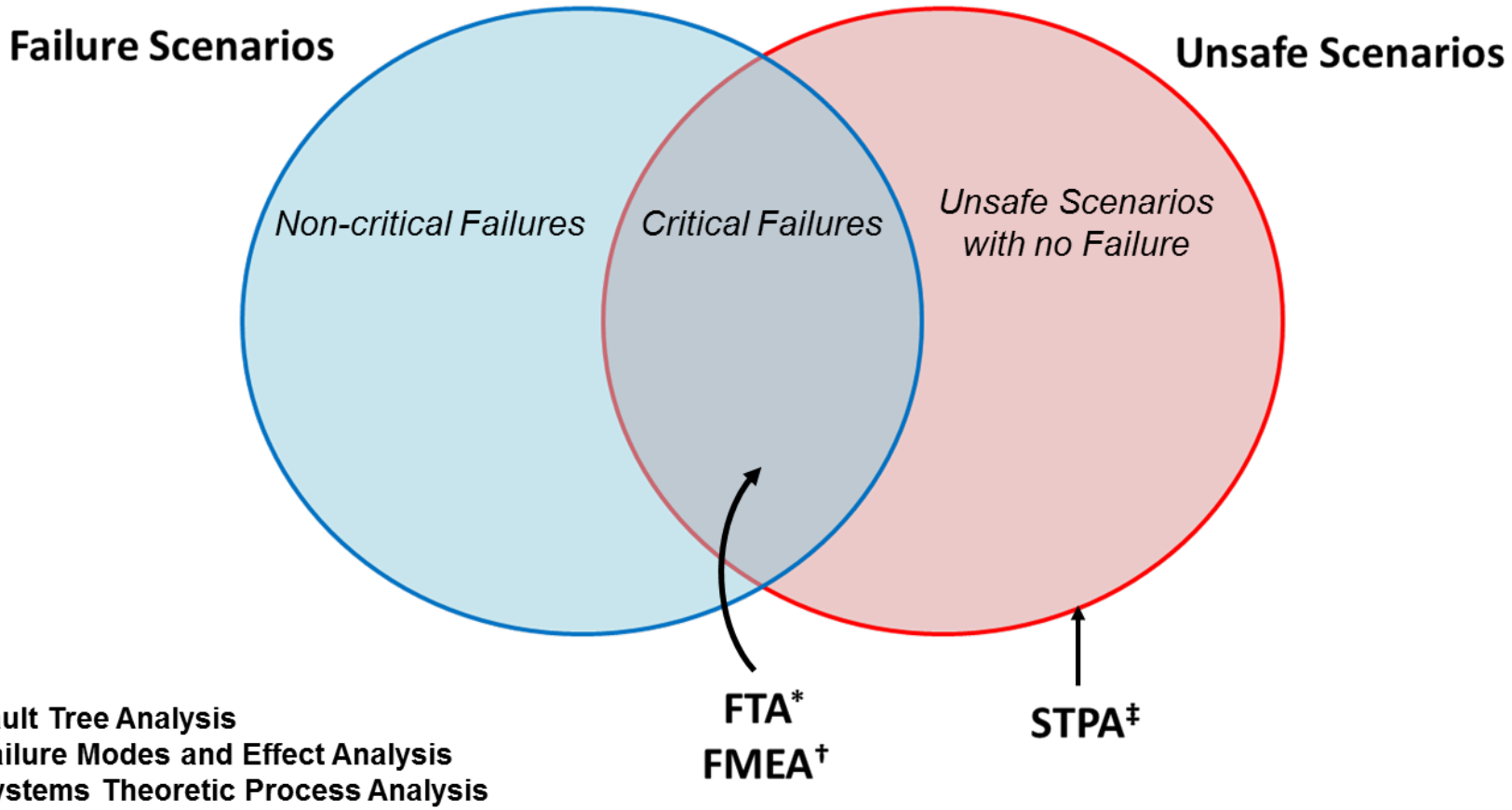
Causal scenarios allow for more detailed, traceable safety recommendations to be made for safe Offshore Supply Vessel operation



Outline

- Executive Summary
- Dynamic Positioning System Case Study
- Comparison of STPA Results to FTA/FMEA
  - Non-Failure Example (FTA)
  - Process Model Flaw Example (FTA)
  - DP Proving Trial Example (FMEA)
- MIL-STD-882E Compliance
- Summary

Focus of Hazard Analysis Techniques



STPA identifies safety issues that are outside the FTA/FMEA problem space.

FTA is Failure-Centric

Unsafe Control Action 13 with Causal Scenario

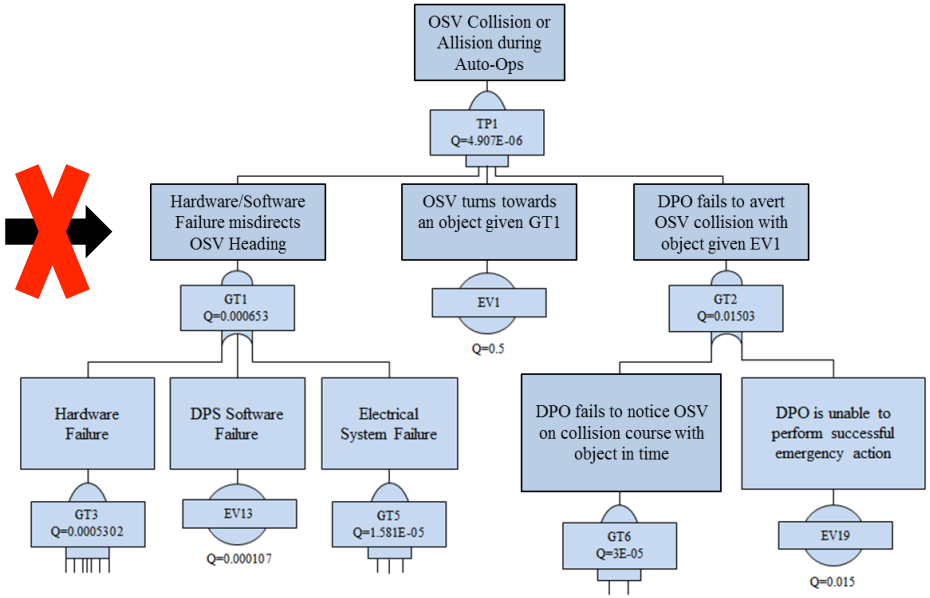
UCA 13: OSV Crew does not update a system parameter when a changing situation requires a system parameter to be updated.

Scenario: OSV Crew does not update the DP system threshold values when lateral separation between the OSV and target vessel changes due to a high-workload, high-stress environment.

Possible Requirements:

1. The OSV Crew must receive feedback to actively verify yellow/red alarm values if no parameter change is made when lateral separation changes by x feet.

Provided Safety Documentation (Fault Tree)



STPA identifies unsafe scenarios where no failure occurs

Process Model Flaws Not Part of FTA

Unsafe Control Action 3 with Causal Scenario

UCA 3: OSV Crew activates DP System (auto) during an unsafe sea state

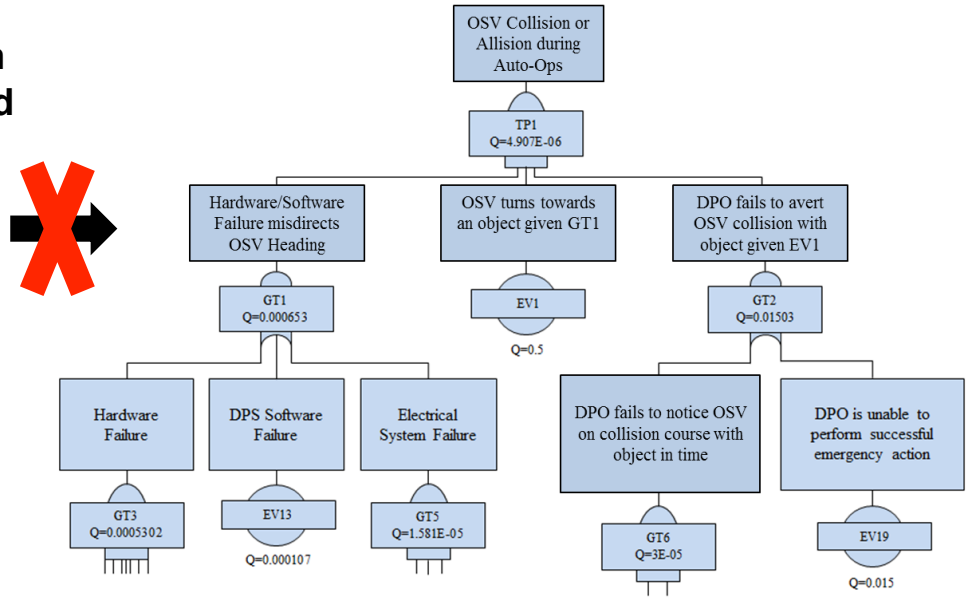
Scenario: The OSV Crew activates the DP System in an unsafe sea state because they have a flawed process model due to…

a) Missing/inaccurate feedback
b) Incorrect assessment of conditions
c) Abrupt change in environment

Possible Requirements:

1. The Crew must be notified if the sea state is unsafe for auto ops. If possible, integrate sea state classification sensors onto OSV.
2. If possible, the DP system should prevent activation of automatic mode when sea state exceeds a predetermined limit.

Provided Safety Documentation (Fault Tree)



STPA identifies unsafe scenarios where the human operator (or non-human controller) has a process model flaw.

STPA Analysis Compared to Proving Trials

Proving Trials Safety Documentation

EQUIPMENT SUB-SYSTEM 1	
Test No 8	DP Control System – SPU Outstation Network Faults
Objective: To verify acceptable SPU power failure modes.	
Method: With the vessel in Auto DP and all thrusters and propellers selected, c position reference systems selected and all control computers online:	
1. Fail Net A for SPU 1 by disconnecting. Observe results and restore.	
2. Fail Net B for SPU 1 by disconnecting. Observe results and restore.	
3. To simulate a failure of SPU 1, open both primary and secondary 24 vdc CB's.	
4. Fail Net A for SPU 2 by disconnecting. Observe results and restore.	
5. Fail Net B for SPU 2 by disconnecting. Observe results and restore.	
6. To simulate a failure of SPU 2, open both primary and secondary 24 vdc CB's.	
7. Fail Net A for SPU 3 by disconnecting. Observe results and restore.	
8. Fail Net B for SPU 3 by disconnecting. Observe results and restore.	
9. To simulate a failure of SPU 3, open both primary and secondary 24 vdc CB's.	
Results expected:	
1. Alarm for loss of Net A.	
2. Alarm for loss of Net B.	
3. Loss of communication with SPU1. No loss of position or heading.	
4. Alarm for loss of Net A.	
5. Alarm for loss of Net B.	
6. Loss of communication with SPU1. No	
Alarm for loss of Net A.	

Unsafe Control Action 46 with Causal Scenario

UCA 46: SPU stops implementing a directional command to the OSV control subsystems before the maneuver is complete.

Scenario: The SPU fails mid-maneuver. The DP System's thruster allocation logic (TAL) attempts to make adjustments to use the remaining thrusters for maneuvering. However, because the loss of a single SPU prevents the DP System from utilizing all subsystems connected to that SPU, the TAL may be unable to successfully maneuver.

Possible Requirements:

1. Each SPU should be capable of controlling all control subsystems on the OSV so that if a single SPU fails, the backup SPUs are fully redundant.

- Proving trials representative of DP System's original use (station keeping)
- OSV was essentially stationary during proving trials test conditions
- OSV conditions during escort operations are very different
- Expected results in proving trials may not represent SPU failure during operations

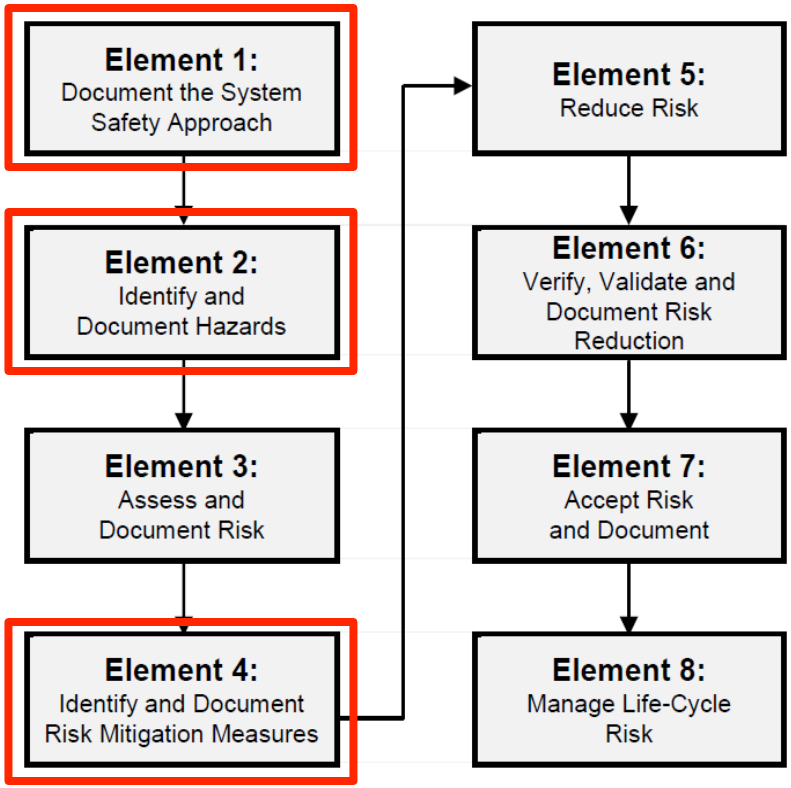
DP proving trials do not always represent DPS use during escort operations. STPA shows that SPU redundancy is inadequate.



Outline

- Executive Summary
- Dynamic Positioning System Case Study
- Comparison of STPA Results to FTA/FMEA
- MIL-STD-882E Compliance
- Summary

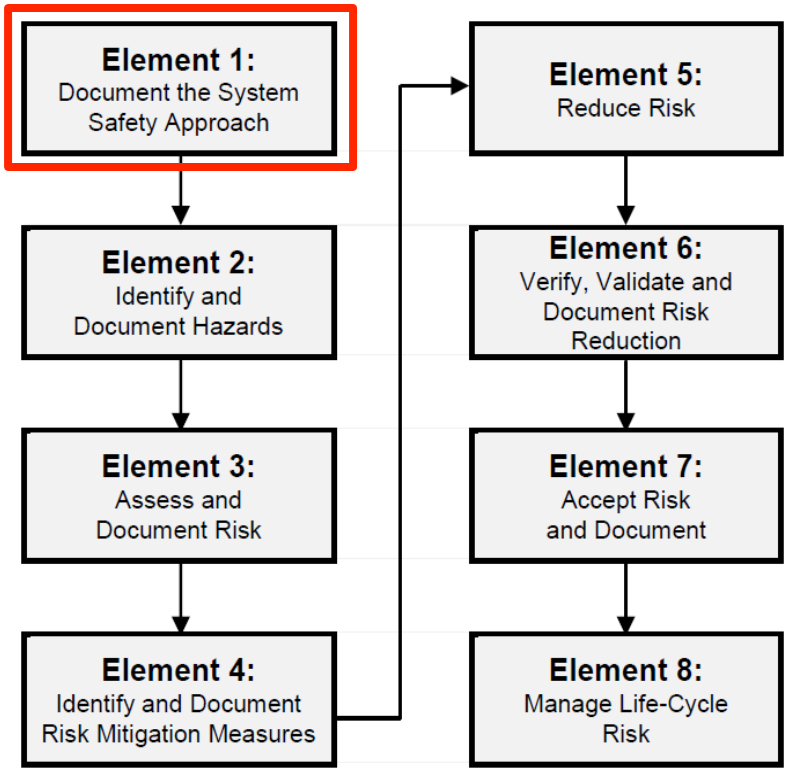
MIL-STD-882E Compliance



Eight Elements of MIL-STD-882E System Safety Process

Elements fully addressed through use of STPA

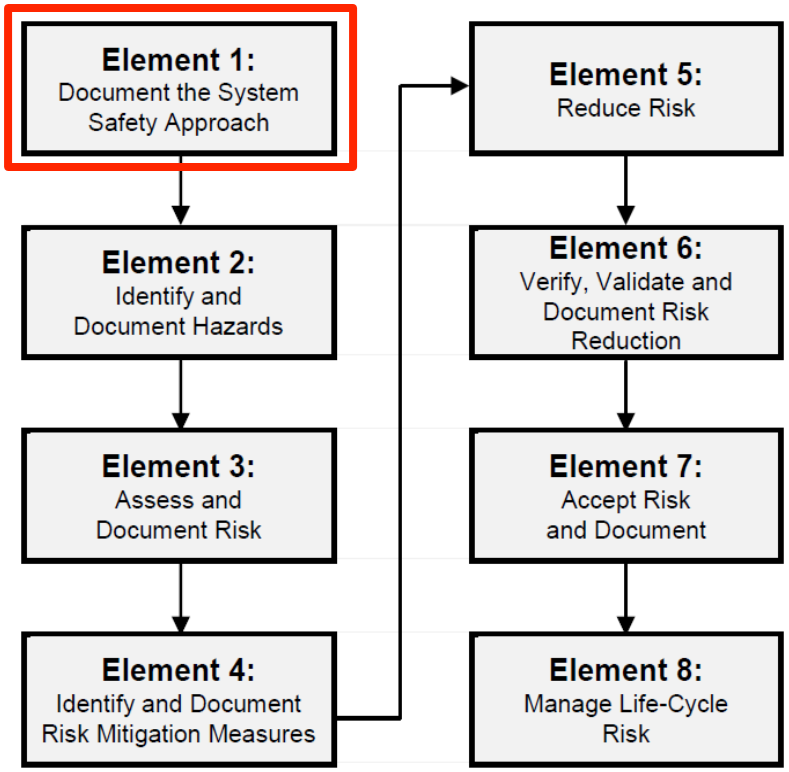
MIL-STD-882E Compliance



Eight Elements of MIL-STD-882E System Safety Process

The safety approach must "describe the risk management effort and how the program is integrating risk management into the SE process, the Integrated Product and Process Development process, and the overall program management structure." MIL-STD-882E Pg. 10.

MIL-STD-882E Compliance

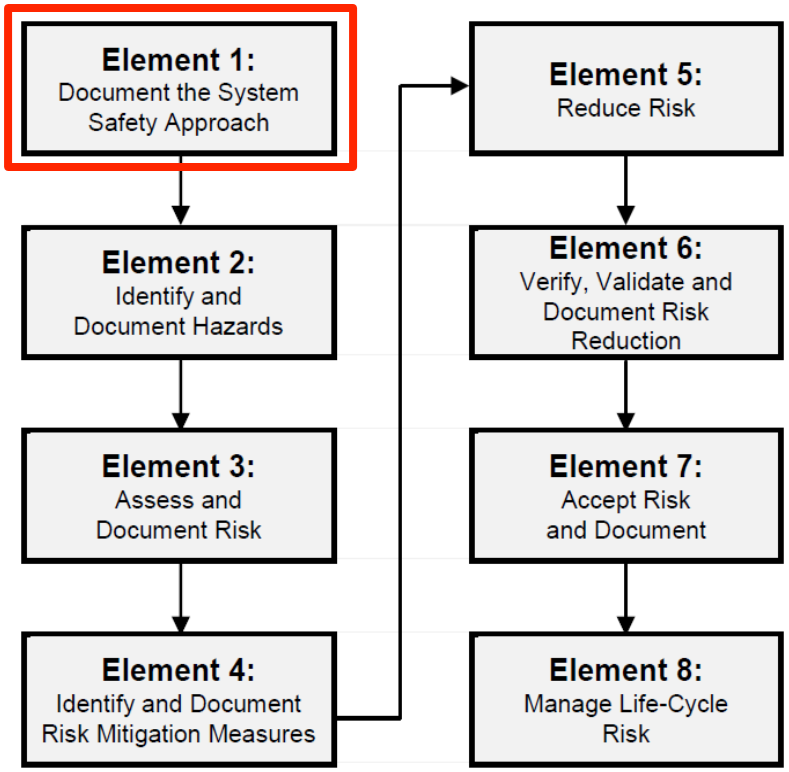


Eight Elements of MIL-STD-882E System Safety Process

The safety approach must "**describe the risk management effort** and how the program is integrating risk management into the SE process, the Integrated Product and Process Development process, and the overall program management structure." MIL-STD-882E Pg. 10.

- **STPA provides useful guidance to the analyst to ensure a uniform process is used to identify traceable unsafe control actions, safety constraints, and recommendations**

MIL-STD-882E Compliance

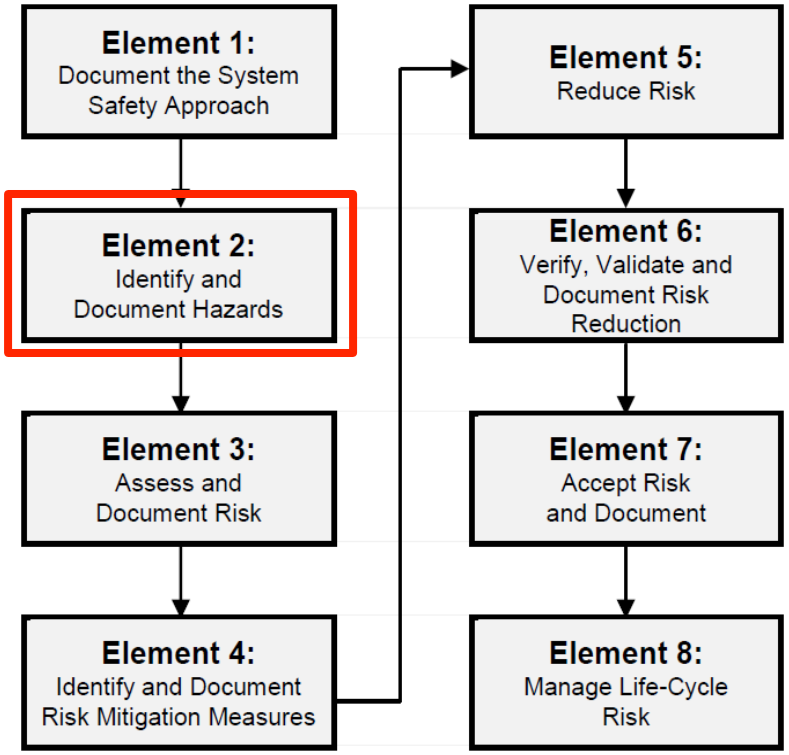


Eight Elements of MIL-STD-882E System Safety Process

The safety approach must "describe the risk management effort and **how the program is integrating risk management into** the SE process, the Integrated Product and Process Development process, and **the overall program management structure**." MIL-STD-882E Pg. 10.

- **STPA used not only on technical design, but on organizational design and analysis as well**

MIL-STD-882E Compliance

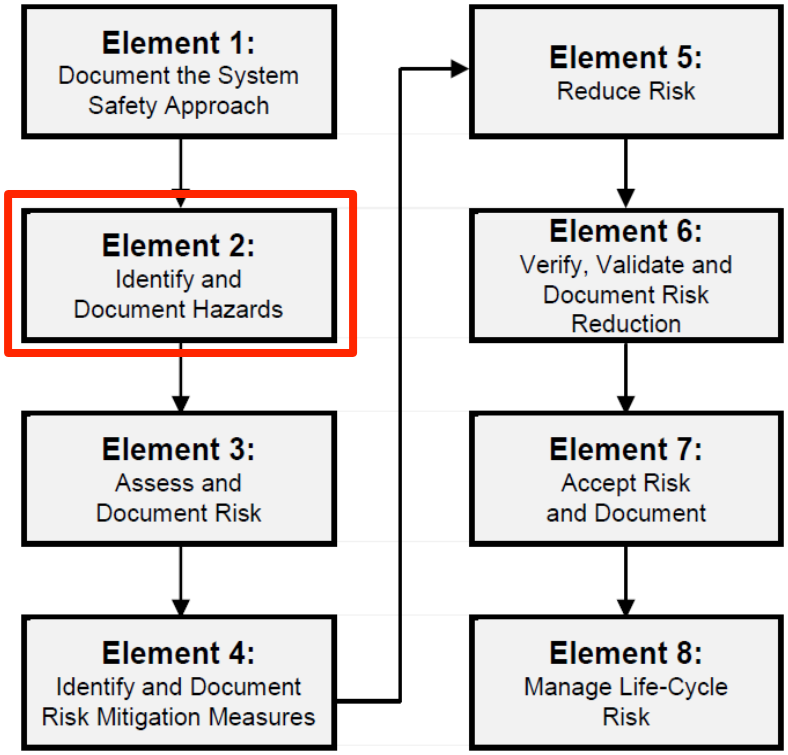


Eight Elements of MIL-STD-882E System Safety Process

"Hazards are identified through a systematic analysis process that includes system hardware and software, system interfaces (to include human interfaces), and the intended use or application and operational environment."

MIL-STD-882E Pg. 12.

MIL-STD-882E Compliance



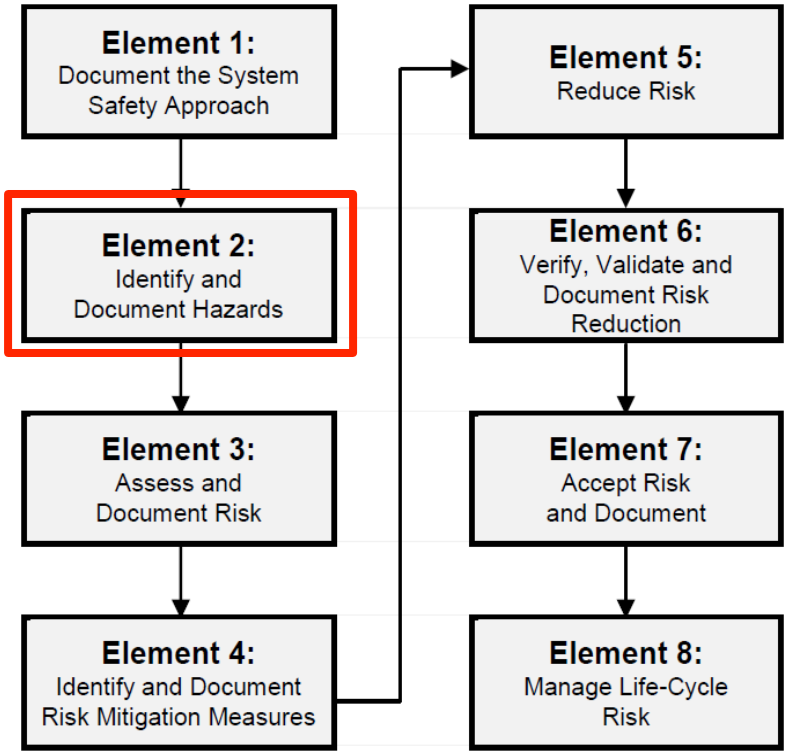
Eight Elements of MIL-STD-882E System Safety Process

"Hazards are identified through a **systematic analysis process that includes system hardware and software, system interfaces (to include human interfaces)**, and the intended use or application and operational environment."

MIL-STD-882E Pg. 12.

- **Structured process addresses the functional relationships between human controllers, software, and hardware components**

MIL-STD-882E Compliance



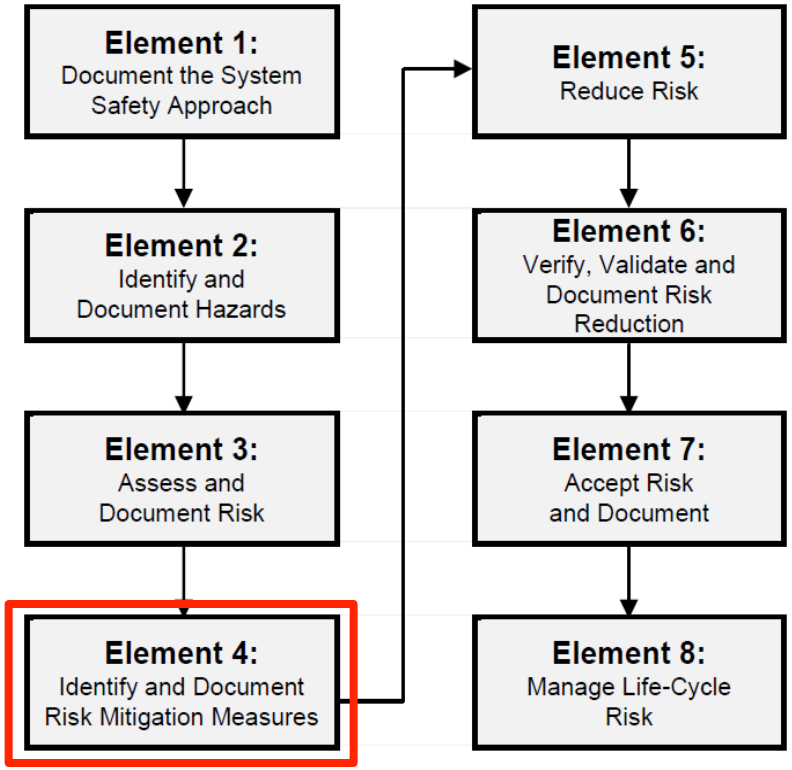
Eight Elements of MIL-STD-882E System Safety Process

"Hazards are identified through a **systematic analysis process that includes** system hardware and software, system interfaces (to include human interfaces), and **the intended use or application and operational environment**."

MIL-STD-882E Pg. 12.

- **DP proving trial analysis of SPU failure compared to STPA analysis of the same failure**

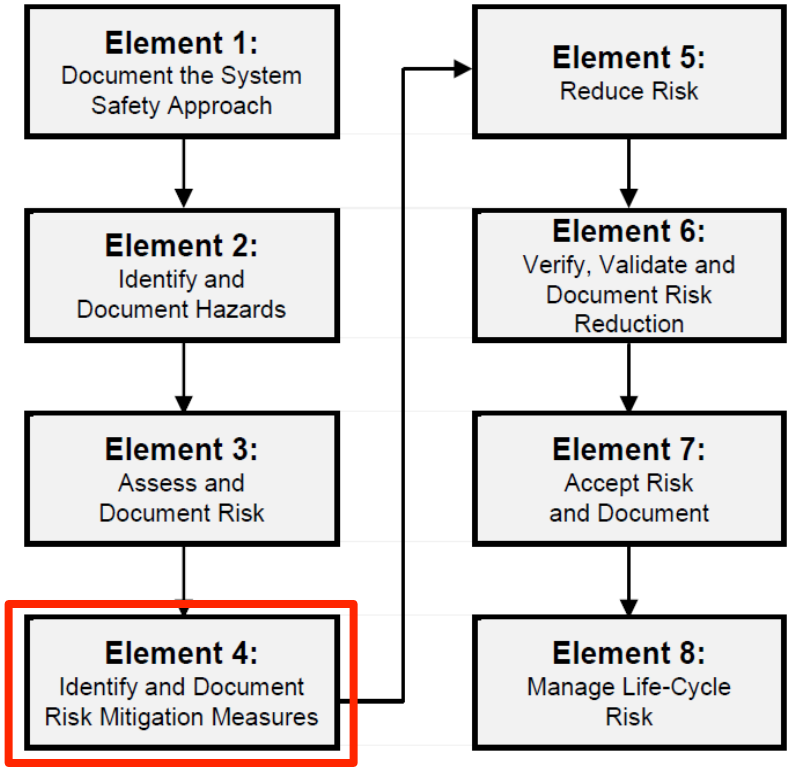
MIL-STD-882E Compliance



Eight Elements of MIL-STD-882E System Safety Process

"Mitigation approaches can include elimination of the hazard through design selection, reduction of risk through design alteration, incorporation of engineering features or devices, the provision of warning devices, and/or the incorporation of signage, procedures, training, and PPE." **MIL-STD-882E Pg. 12.**

MIL-STD-882E Compliance



Eight Elements of MIL-STD-882E System Safety Process

"Mitigation approaches can include elimination of the hazard through **design selection**, reduction of risk through **design alteration**, **incorporation of engineering features or devices**, the **provision of warning devices**, and/or the incorporation of signage, **procedures, training**, and PPE." MIL-STD-882E Pg. 12.

- **The 171 safety recommendations generated from this analysis include mitigation approaches in each of these categories**

MIL-STD-882E Compliance

Task 205: System Hazard Analysis

"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…; and to recommend actions necessary to eliminate identified hazards or mitigate their associated risks." MIL-STD-882E Pg. 54.

- **By addressing unsafe scenarios along with failure scenarios, STPA is able to more adequately meet the requirements set forth in Task 205**
- **By assigning importance to software and human operators as well as electromechanical components, recommendations for risk mitigation and/or elimination are more appropriate than those generated by FTA/FMEA**

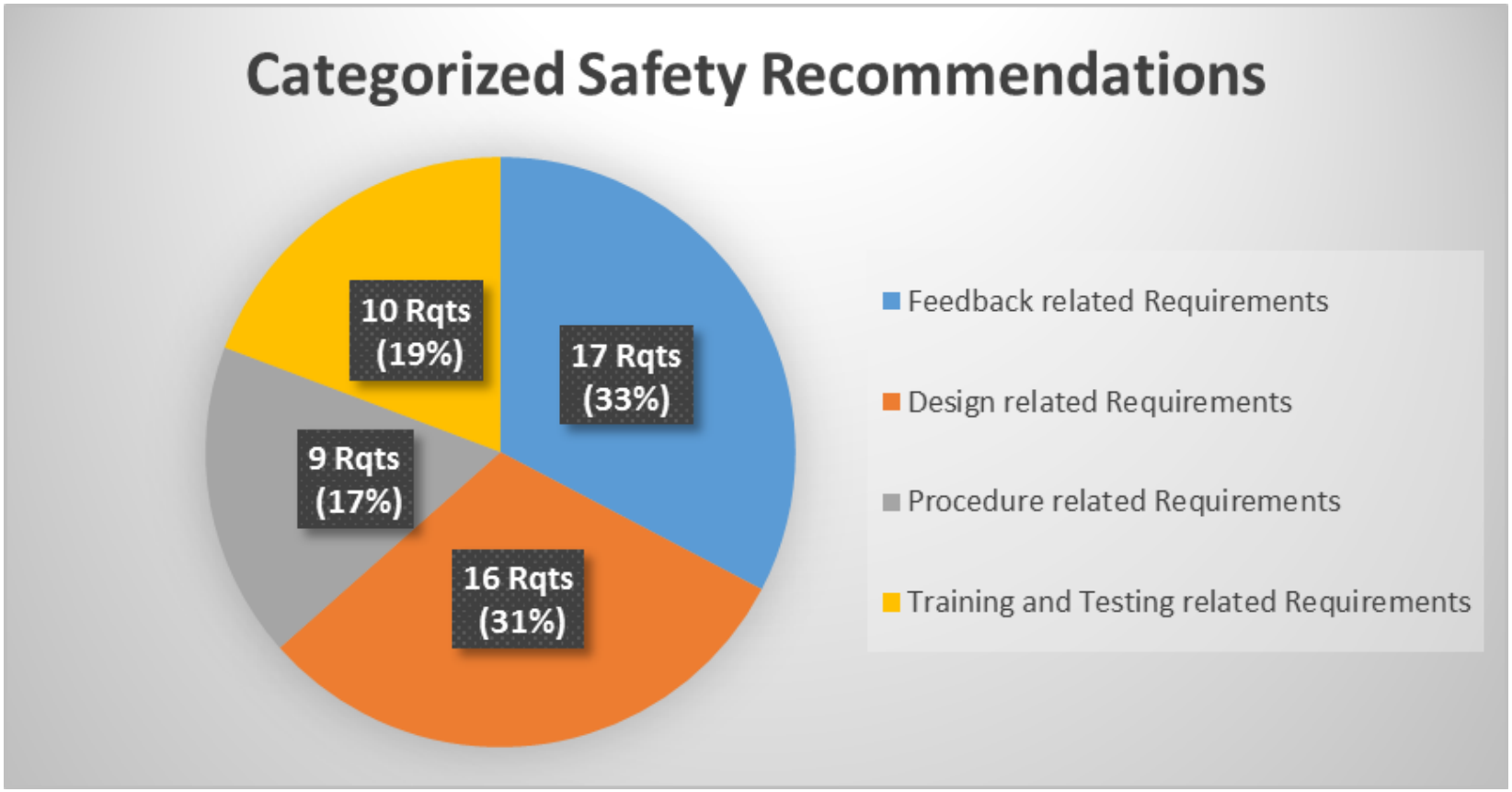


Outline

- Executive Summary
- STPA Background
- Dynamic Positioning System Case Study
- Comparison of STPA Results to FTA/FMEA
- MIL-STD-882E Compliance
- Summary

Summarized Results

- **The 171 recommended safety requirements were combined and rewritten and then categorized into four types of requirements.**





Summary

- STPA identified all system component failures found via Fault Tree Analysis (FTA) & Failure Modes and Effect Analysis (FMEA) and also identified numerous additional safety concerns not found through FTA & FMEA
- Recommended safety requirements fell into four categories…
  - 17 Feedback related Requirements
  - 16 Design related Requirements
  - 9 Procedure related Requirements
  - 10 Training and Testing related Requirements
- Results generated by STPA better satisfy the requirements for systems hazard analysis set forth by MIL-STD-882E than traditional hazard analysis techniques
- Because STPA can be used at any point during a system's developmental lifecycle, even very early in the concept development stage, STPA can be used as a tool to help design safety into other current and future Naval Systems