Integrating STAMP-Based Hazard Analysis with MIL-STD-882E Functional Hazard Analysis

A Consistent and Coordinated Process Approach to MIL-STD-882E Functional Hazard Analysis

Nicolas Malloy

Systems Engineer

L3 KEO

Outline

- Purpose
- Problem
- Problem Approach
- Brief High-Level Example
- Conclusion
- Recommendations
- Benefits
- References

Purpose

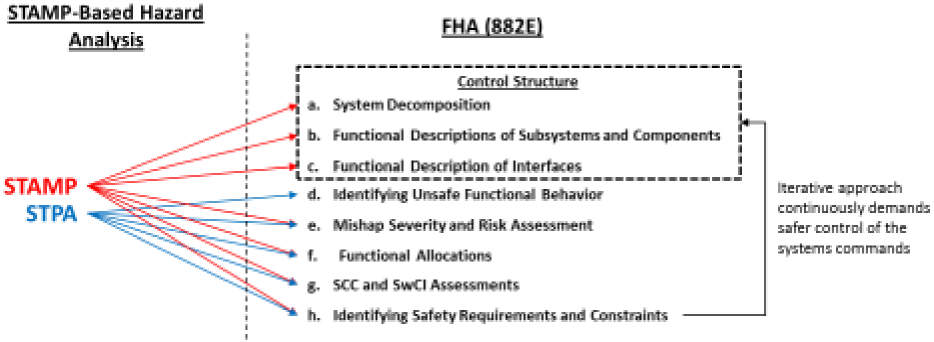
- Promote the integration of STAMP-Based Hazard Analysis with MIL-STD-882E Functional Hazard Analysis
  - Document a process which organizations can follow to conduct well-crafted safety hazard analysis
  - Improve the safety process through the use of a continuous process improvement plan
  - Break through “business as usual” paradigms
  - System safety must be an organic component of the system design process (hardware, software, etc.)

Problem

- MIL-STD-882E provides high-level descriptions of tasks required to achieve standard compliance
  - Very helpful for some tasks
  - Others leave the practitioner needing more instruction
- Example: Functional Hazard Analysis
  - List of eight tasking elements
    - There are high-level descriptions but little instructions or references provided
      - Some tasking elements are straight forward while others are not
      - Can lead to analysis approach based on assumption
    - Tasking elements build upon each other – Effectiveness and quality of hazard identification and mitigation controls become susceptible to serious degradation if initial tasks are flawed
  - A consistent and coordinated process is needed

Problem Approach

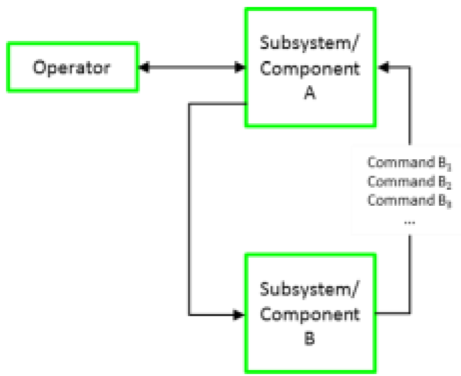
- Integrate STAMP-Based Hazard Analysis with MIL-STD-882E Functional Hazard Analysis
  - Map STAMP and STPA → MIL-STD-882E Functional Hazard Analysis Tasking Elements
  - Document rationale



- Develop a Safety Process and Plan to be shared with the safety community
  - Whitepapers can be written as necessary to support the process

System Decomposition

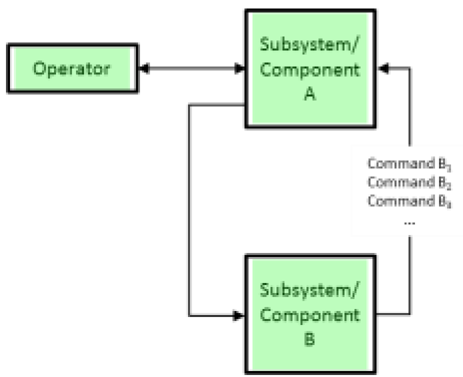
Tasking Element	MIL-STD-882E FHA Tasking Element Description	Allocation	Rationale
a.	*Decomposition of the system and its related subsystems to the major component level.*[3]	STAMP	Decomposing the system and its related subsystems to the major component level feeds directly into STAMP with the construction of the Control Structure. Also includes early safety Requirements and Constraints development and preliminary identification Hazards and Mishaps.



Control Structure for a Generic Man/Machine System

Functional Descriptions of Subsystem and Components

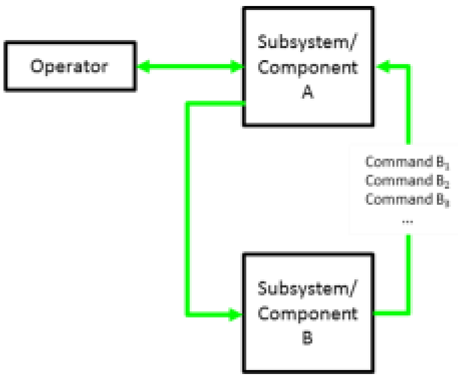
Tasking Element	MIL-STD-882E FHA Tasking Element Description	Allocation	Rationale
b.	*A functional description of each subsystem and component identified.*[3]	STAMP	Documenting the behavioral characteristics of the system using functional descriptions contributes to STAMP with the continued construction of the Control Structure. Also includes early safety Requirements and Constraints development and preliminary identification of Hazards and Mishaps continues to occur.



Control Structure for a Generic Man/Machine System

Functional Descriptions of Interfaces

Tasking Element	MIL-STD-882E FHA Tasking Element Description	Allocation	Rationale
c.	*A functional description of interfaces between subsystems and components. Interfaces should be assessed in terms of connectivity and functional inputs and outputs.*[3]	STAMP	Documenting the behavioral characteristics of system interfaces contributes to STAMP and the continued construction of the Control Structure. Also includes early safety Requirements and Constraints development and preliminary identification of Hazards and Mishaps continues to occur.



Control Structure for a Generic Man/Machine System

Identifying Unsafe Functional Behavior

Tasking Element	MIL-STD-882E FHA Tasking Element Description	Allocation	Rationale
d.	*Hazards associated with loss of function, degraded function, or malfunction, or functioning out of time or out of sequence for the subsystems, components, and interfaces. The list of hazards should consider the next effect in a possible mishap sequence and the final mishap outcome.*[3]	STPA	STPA step 1 identifies the potential for inadequate control of the system leading to a hazardous state. STPA step 2 considers multiple controllers of the same components and seeks to identify conflicts and potential coordination problems. This aids in identifying next effects and top level events.

STPA step 2 supports the identification of HOW unsafe control actions can occur

- **Example: Security**
  - **Integrated approach to Safety and Security with STPA-Sec[4]**
    - **Physical, Cyber, Parts Tampering, etc.**

Identifying Unsafe Control Actions[2]

Risk Assessment

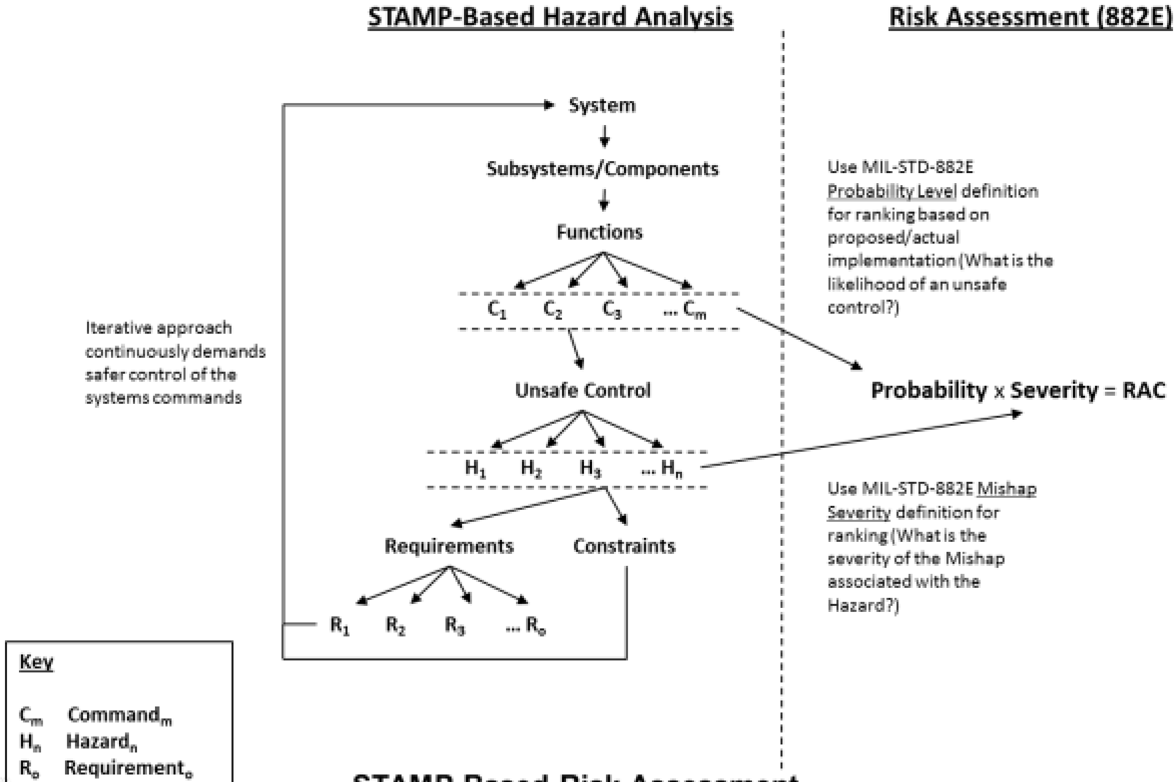
Tasking Element	MIL-STD-882E FHA Tasking Element Description	Allocation	Rationale
e.	*An assessment of the risk associated with each identified failure of a function, subsystem, or component. Estimate severity, probability, and Risk Assessment Code (RAC) using the process described in Section 4 of 882E.*[3]	STAMP STPA	STAMP together with STPA *identifies the system-level Hazards associated with each function (and unsafe control action) so the classification as to severity comes from the classification of the system level hazards and their associated mishaps.*[1] STPA *can be used to make risk acceptance decisions and to plan mitigations for open safety risks that need to be changed before a system is deployed and field tested.*[2]

Probability x **Severity** = **RAC**

Subsystem/ Component	Function	Command	Unsafe Control	Hazard	Severity	Probability	RAC
• *Electromechanical,* • *Digital,* • *Human, or* • *Social*[2]	A well order set of unique commands	A specific order issued by a Subsystem/ Component	A specific order issued by a Subsystem/Component that contributes/leads to a hazard	A real or potential condition that could lead to a mishap	An event or series of events that result in a loss	A quantitative or qualitative assessment used to express the likelihood of an events occurrence	An assessment comprised of mishap probability and severity

Risk Assessment Traceability Matrix

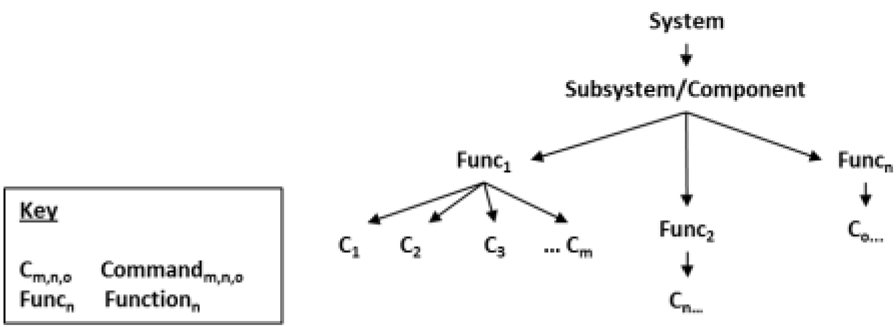
Risk Assessment (cont.)



STAMP-Based Risk Assessment

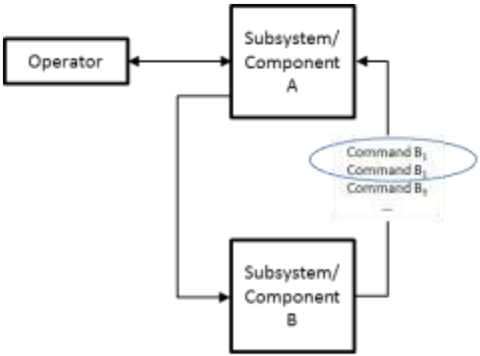
Functional Allocations

Tasking Element	MIL-STD-882E FHA Tasking Element Description	Allocation	Rationale
f.	*An assessment of whether the functions identified are to be implemented in the design hardware, software, or human control interfaces. This assessment should map the functions to their implementing hardware or software components. Functions allocated to software should be mapped to the lowest level of technical design or configuration item prior to coding (e.g., implementing modules or use cases).*[3]	STAMP STPA	Determining how system functionality and components are to be implemented is based on the safety Requirements and Constraints that are developed while the safety practitioner works through <u>STAMP</u> and <u>STPA steps 1 and 2</u> iteratively. "Like" Commands can also be Functionally Grouped. This can be used to establish traceability between the Functions, Commands, Hazards, Safety Requirements, and Constraints. Example: RTM



Functional Decomposition

Functional Allocations (cont.)



Function	Command	Control Interface Implementation	Software Only		
			CSCI	CSC	CSU
$Func_1$	Command B_1	• Hardware, • Software, or • Human			
	Command B_2				
$Func_2$	Command B_3				
	Command B_4				
	Command B_5				
	Command B_6				
$Func_n$	Command B_7				

Functional Hazard Traceability Matrix

Key

$Func_n$	$Function_n$
CSCI	Computer Software Configuration Item
CSC	Computer Software Component
CSU	Computer Software Unit

Software Criticality Index Assessments

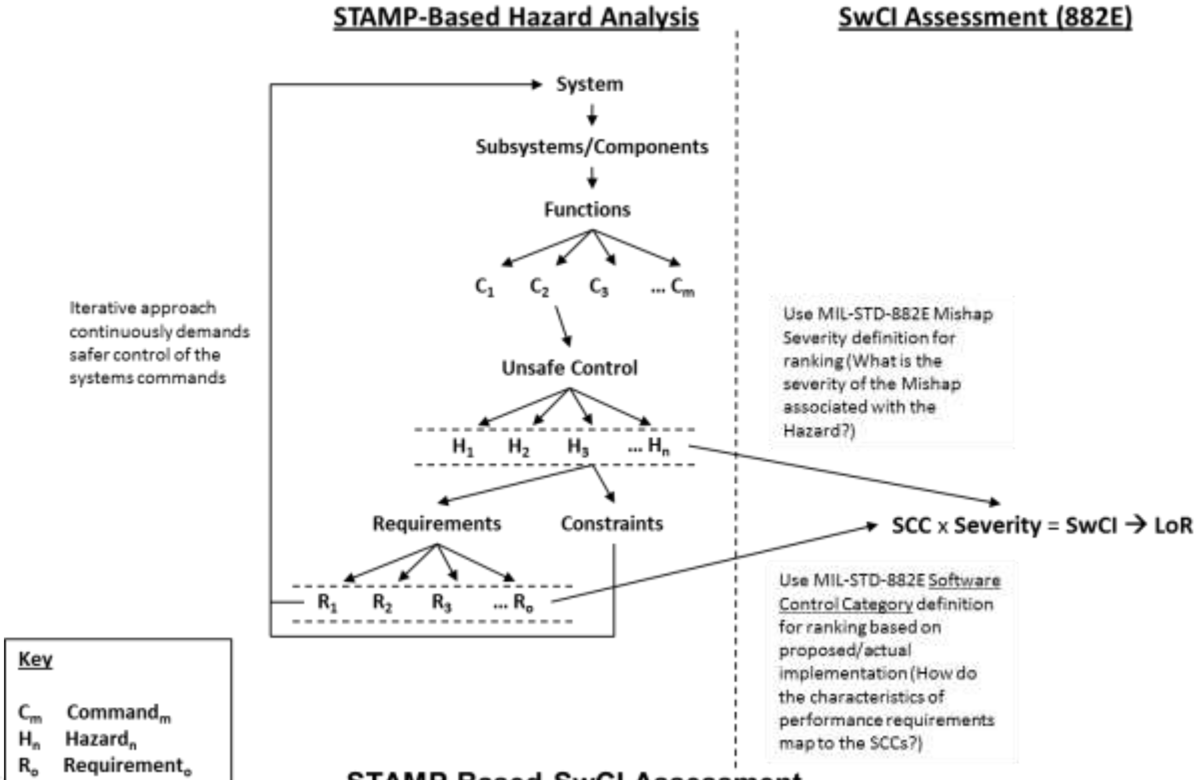
Tasking Element	MIL-STD-882E FHA Tasking Element Description	Allocation	Rationale
g.	*An assessment of Software Control Category (SCC) for each Safety-significant Software Function (SSSF). Assign a Software Criticality Index (SwCI) for each SSSF mapped to the software design architecture.*[3]	STAMP STPA	SCC and SwCI are unique to MIL-STD-882E but the determination for how software functionality is to be implemented is in part based upon the technology needed to support the safety Requirements and Constraints that are developed while the safety practitioner works through STAMP and STPA steps 1 and 2 iteratively.

SCC x Severity = SwCI → LoR

Subsystem/ Component	Function	Command	SCC	Unsafe Control	Hazard	Severity	SwCI	LoR
• *Electromechanical,* • *Digital,* • *Human, or* • *Social*[2]	A well order set of unique commands	A specific order issued by a Subsystem/ Component	The degree of software control (Autonomous, Semi-Autonomous, Redundant Fault Tolerant, Influential, or Not Involved)	A specific order issued by a Subsystem/ Component that contributes/ leads to a hazard	A real or potential condition that could lead to a mishap	An event or series of events that result in a loss	An event or series of events that result in a loss	*Depth and breadth of software analysis and verification activities necessary to provide a sufficient level of confidence*[3]

SwCI Assessment Traceability Matrix

Software Criticality Index Assessments (cont.)



STAMP-Based SwCI Assessment

Identifying Safety Requirements and Constraints

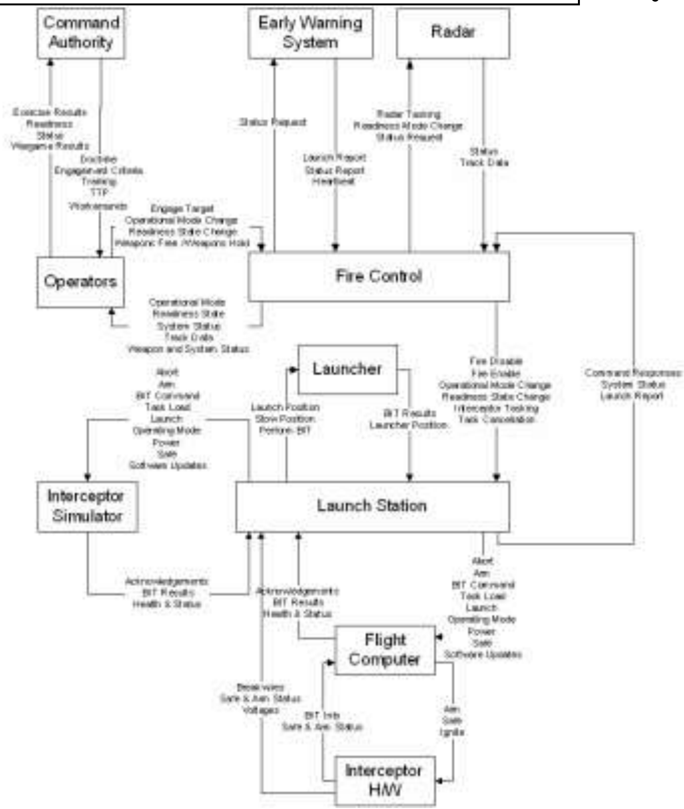
Tasking Element	MIL-STD-882E FHA Tasking Element Description	Allocation	Rationale
h.	*A list of requirements and constraints (to be included in the specifications) that, when successfully implemented, will eliminate the hazard, or reduce the risk. These requirements could be in the form of fault tolerance, detection, isolation, annunciation, or recovery.*[3]	STAMP STPA	STAMP begins with the preliminary identification of safety requirements and constraints. Analysis of the system and component hazards identified during STPA steps 1 and 2 aids in the iterative development of the safety Requirements and Constraints necessary to address the unsafe controls leading to hazards.

Subsystem/ Component	Function	Command	Unsafe Control	Hazard	Mishap	Safety Requirement	Constraint	Requirement Type
• *Electromechanical,* • *Digital,* • *Human, or* • *Social*[2]	A well order set of unique commands	A specific order issued by a Subsystem/ Component	A specific order issued by a Subsystem/Component that contributes/leads to a hazard	A real or potential condition that could lead to a mishap	An event or series of events that result in a loss	*Derived from the mission or reason for the systems existence*[2]	*Represents acceptable ways the system can achieve mission goals*[2]	• *Fault tolerance,* • *Detection,* • *Isolation,* • *Annunciation, or recovery.*[3]

Safety Requirements and Constraints Traceability Matrix

Identifying Inadequate Control – STAMP and STPA (Example)

Ballistic Missile Intercept System Control Structure [1]



- STAMP – Modeling Process based on the premise that loss is caused by inadequate control [1]
  - Requirements and Constraints
  - Control Structure
  - Process Model

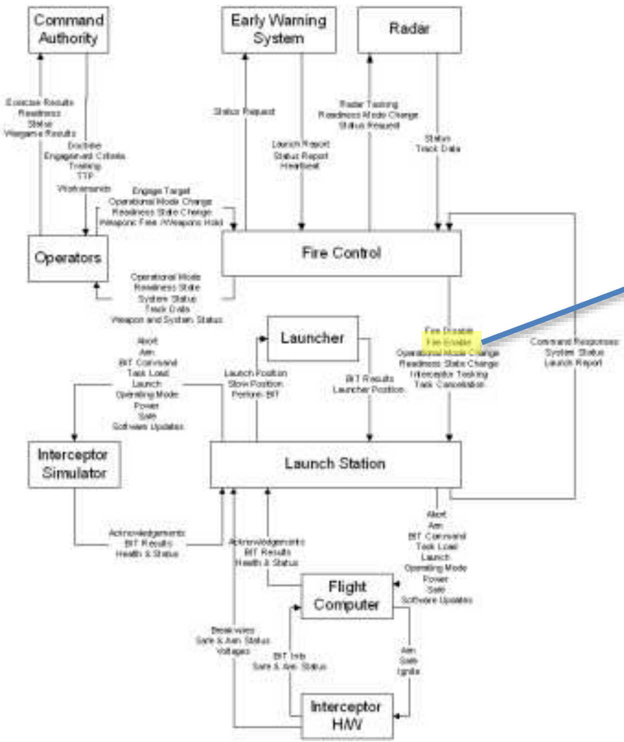
STPA – How do we find inadequate control in a system? [1]

- Identify loss and causal scenarios
- Construct the control structure
- STPA Step 1: Identify inadequate control actions
- STPA Step 2: Identify causal factors and control flaws

Identifying Inadequate Control – STAMP and STPA (Example)

1st

Ballistic Missile Intercept System Control Structure [1]



Loss – Inadvertent launch results in a lost asset and possible injury/death.

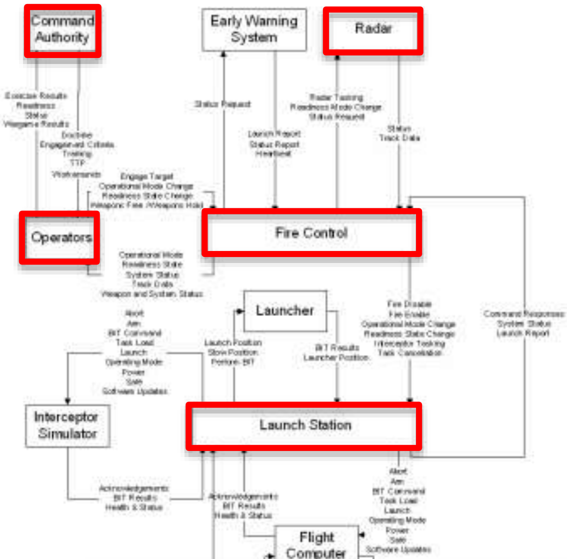
STPA Step 1 – Identify the potential for inadequate control of the system that could lead to a casual scenario. [1]

Inadequate Control Actions [1]				
Command	**Not Providing Leads to Causal Scenario**	**Providing Incorrectly Leads to Causal Scenario**	**Wrong Timing or Order Leads to Causal Scenario**	**Stopped Too Soon or Applied Too Long Leads to Causal Scenario**
Fire Enable	Not Hazardous	Will accept interceptor tasking and can progress to a launch sequence	Early: Can inadvertently progress to an inadvertent launch Out of Sequence: Disable comes before the enable	Not Applicable

Identifying Inadequate Control – STAMP and STPA (Example)

1st

Ballistic Missile Intercept System Control Structure [1]



STPA Step 2 – Determine how each potentially inadequate control action identified in step 1 could occur. [1]

Q: Why might Fire Control issue the *Fire Enable* command incorrectly?

A: Security Flaw

1. Cyber Attack against the Radar Subsystem has injected erroneous *Track Data* that shows a hostile target
2. Operator training says, Operator shall issue *Engage Target* if *Track Data* shows hostile target and *Engagement Criteria* provided by Command Authority complies
3. Operator accepts hostile target and issues *Engage Target* which results in Fire Control generating the *Fire Enable* command
4. When the *Fire Enable* command is provided to the launch station incorrectly, the launch station will transition to a state where it accepts *interceptor tasking* and can progress through a launch sequence

ontrol

What design changes (adaptations) could be applied to mitigate this inadequate control?

Designing Adaptation – Resilience Engineering Design Principles

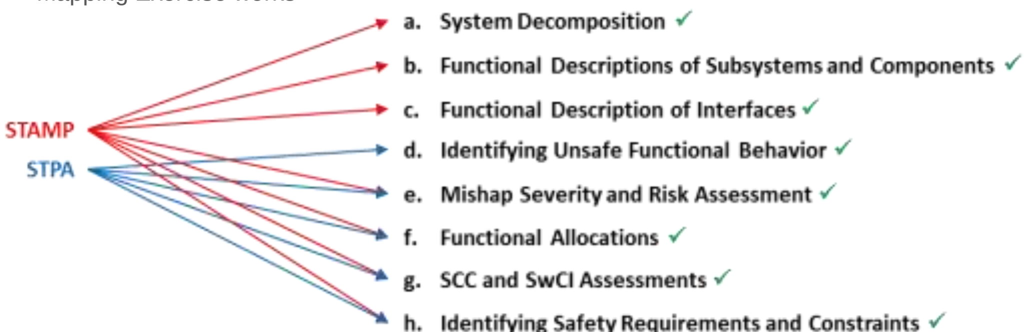
2nd

Design Principle	Heuristic: "rule of thumb" for systems engineering [4, 5, 6, 7]
Functional Redundancy	Design alternative methods to perform particular functions that do not rely on the same physical components
Physical Redundancy	Include redundant hardware
Reorganization	Design an ability for the system to restructure itself in response to an external change
Absorption	Include adequate margin to withstand threats
Human-in-the-Loop	Include humans interaction where rapid cognition is needed
Loose Coupling	Limit the ability of failures to propagate from one component to the next in a system of many components
Complexity Avoidance	Avoid complexity added by poor human design practice
Localized Capacity	Design functionality through various nodes of the system so that if a single node is damaged or destroyed, the remaining nodes will continue to function
Drift correction	Monitor and correct if the system is drifting towards boundaries of capability
Neutral state	Prevent further damage from occurring when hit with an unknown perturbation until the problem can be diagnosed
Reparability	Design the ability to repair system elements
Inter-node Interaction	Design communication, cooperating, and collaborating between system elements
Reduce Hidden Interactions	Potentially harmful interactions between nodes of the system should be reduced
Layered Defense	Use two or more independent principles that address a single element of system vulnerability

- **Example** heuristic considerations for Ballistic Missile Intercept System requirements and constraints
  - **Absorption** ensures protection against cyber threats by compartmentalizing sensitive parts of the system by allowing intrusion detection more time to neutralize the attack
  - **Functional Redundancy** provides data validity checking to ensure the correctness of mission critical functionality
  - **Neutral State** ensures that positive system control is maintained upon detection of cyber threats
  - **Layer Defense = Absorption + Functional Redundancy + Neutral State**

Conclusion

- STAMP-Based Hazard Analysis provides the needed conceptual rigidity and contextual flexibility to perform accurate and complete Functional Hazard Analysis consistently
  - Mapping Exercise works ✓



- Certain tasking elements call out Probabilistic Risk Assessment (PRA) and various software (functional control) specific assessments that are based on software implementation and unique to MIL-STD-882E
  - These are not part of STAMP-Based Hazard Analysis process but can be used to influence design decisions

Recommendations

Use this mapping as the basis for generating a process document that serves to instantiate STAMP-Based Hazard Analysis as a means for performing MIL-STD-882E Functional Hazard Analysis

Other considerations:

- Generate tools to manage the analysis approach
- Use modeling tools to create and maintain the control structure(s)
- Investigate an integrated approach using modeling and analysis management tools in the same environment

Benefits

- STAMP and STPA embody Resilient Systems Engineering Processes
- Consistent approach that documents MIL-STD-882E has been met
- Safety is approached in a consistent and coordinated manner
- All personnel involved in the design of safety significant components (hardware, software, or human) must meet safety requirements
- Modeling approach allows for the design team to continually improve the safety of the system prior to pursuing implementation
- Iterative approach can drive down cost and schedule long term

References

1. Leveson, N. (2016). STPA Compliance with Army Safety Standards and Comparison with SAE ARP 4761. Cambridge, Massachusetts: The MIT Press.
2. Leveson, N. (2011). Engineering a Safer World: Systems Thinking Applied to Safety. Cambridge, Massachusetts: The MIT Press.
3. DoD. (2012). Department of Defense Standard Practice: System Safety. Washington DC.: Department of Defense (DoD).
4. Young, W., & Leveson, N. (2014). Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory. Communications of the ACM, 1-5.
5. Resilience Engineering. (2016, March 25)., Guide to the Systems Engineering Body of Knowledge (SEBoK), version 1.6, R.D. Adcock (EIC), Hoboken, NJ:
6. Jackson, S. & Ferris, T., (2013), Resilience principles for engineered systems, Systems Engineering, 2012, 15, 3, 333-346, Wiley Subscription Services, Inc., A Wiley Company.
7. International Council on Systems Engineering (INCOSE). A World in Motion - Systems Engineering Vision 2025, June 2014

Thank you

Questions ?

nicolasmalloy@gmail.com
https://www.linkedin.com/in/nicolasmalloy/