GENERAL DYNAMICS
Mission Systems

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 H. Malloy
Systems Engineer
nicolas.malloy@gd-ms.com

Outline

- Purpose
- Problem
- Problem Approach
- Conclusion
- Recommendations
- Benefits
- References

GENERAL DYNAMICS
Mission Systems

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.)

GENERAL DYNAMICS
Mission Systems

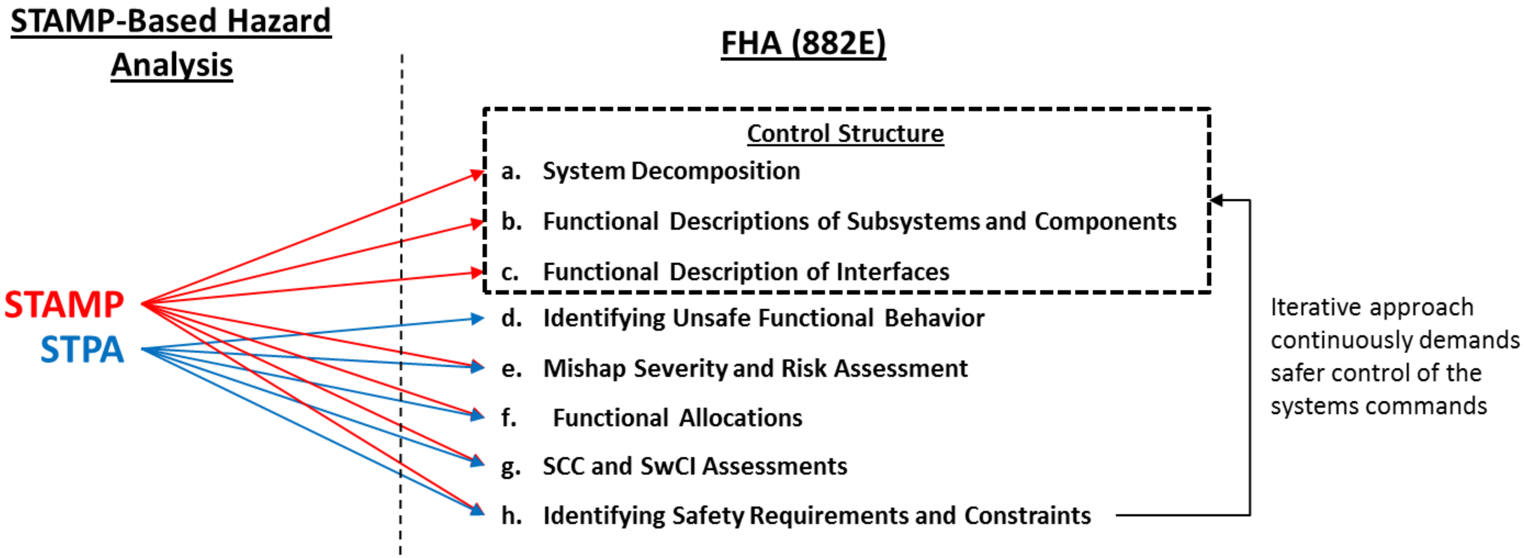
Problem

- 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

GENERAL DYNAMICS
Mission Systems

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

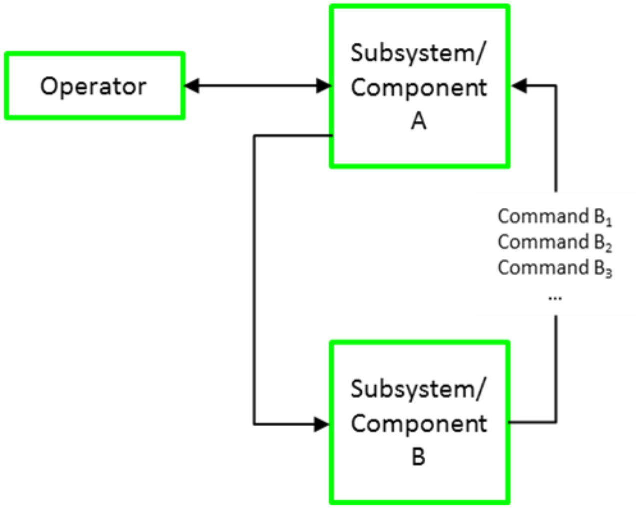


- Develop a Safety Process and Plan to be shared with the safety community
  - Whitepapers can be written as necessary to support the process

GENERAL DYNAMICS
Mission Systems

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.

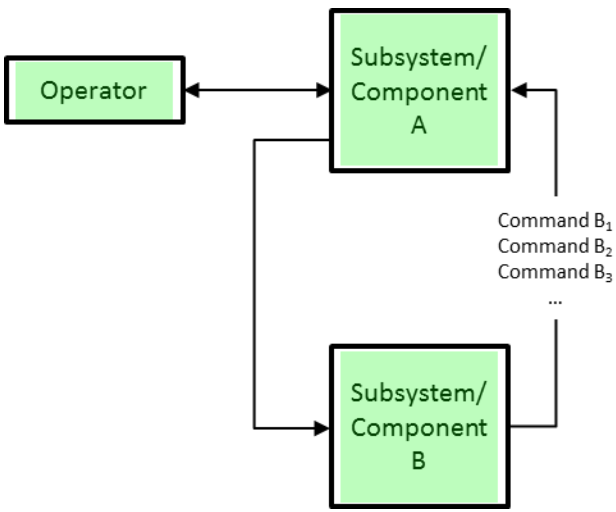


Control Structure for a Generic Man/Machine System

3. DoD. (2012). Department of Defense Standard Practice: *System Safety.* Washington DC.: Department of Defense (DoD).

Functional Descriptions of Subsystems 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.



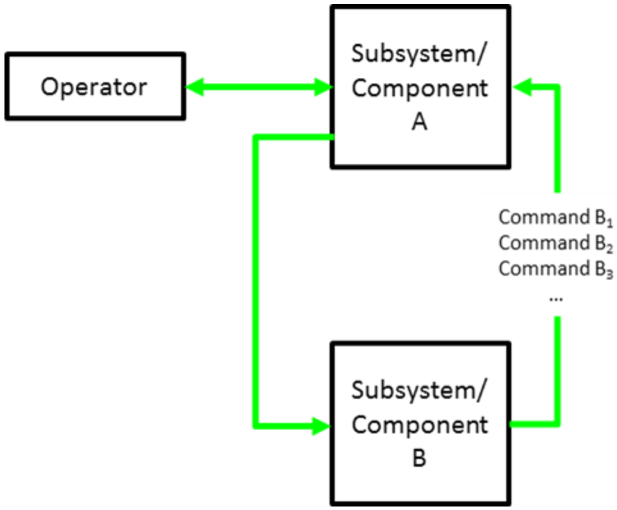
Control Structure for a Generic Man/Machine System

GENERAL DYNAMICS
Mission Systems

3. DoD. (2012). Department of Defense Standard Practice: *System Safety.* Washington DC.: Department of Defense (DoD).

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

3. DoD. (2012). Department of Defense Standard Practice: *System Safety.* Washington DC.: Department of Defense (DoD).

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	<u>STPA step 1</u> identifies the potential for inadequate control of the system leading to a hazardous state. <u>STPA step 2</u> 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.

Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing / Order	Stopped Too Soon / Applied too long

Identifying Unsafe Control Actions[2]

GENERAL DYNAMICS
Mission Systems

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).

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.**

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.

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**

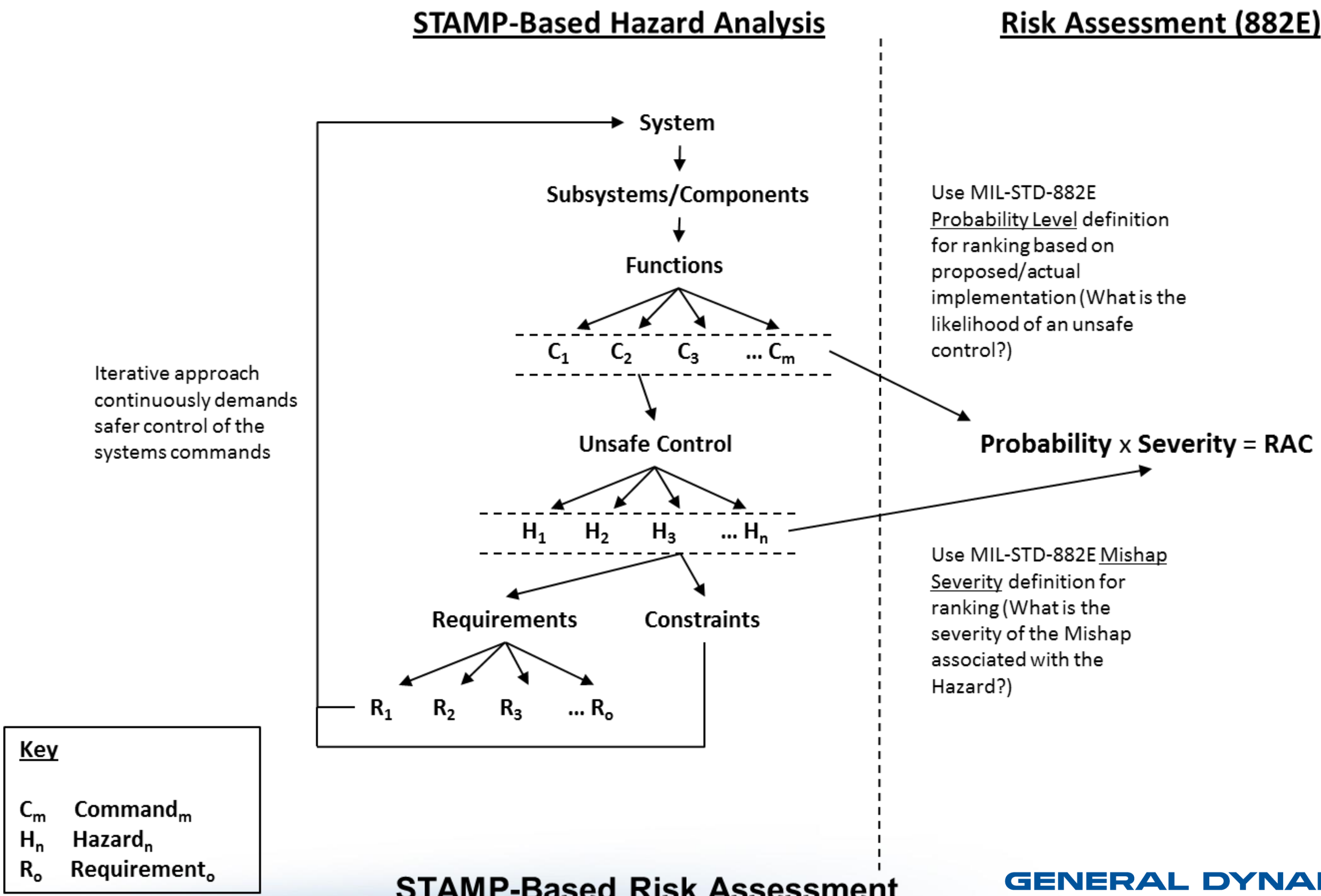
Subsystem/ Component	Function	Command	Unsafe Control	Hazard	Severity	Probability	RAC
• *Electromechanical,* • *Digital,* • *Human, or* • *Social*[2]	A well order set of unique commands	A specific order issued by a Subsystem/ Component	A specific order issued by a Subsystem/Component that contributes/leads 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

GENERAL DYNAMICS
Mission Systems

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).**

Risk Assessment (con't)

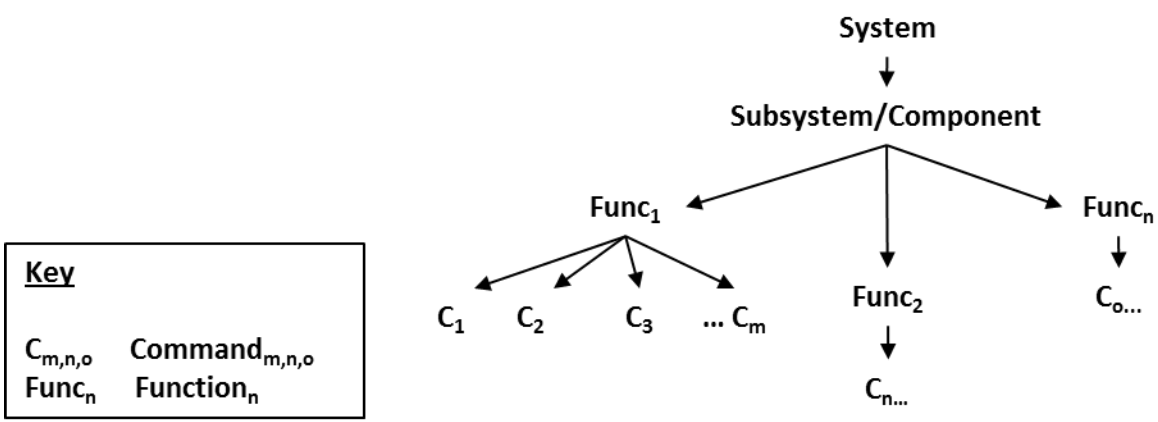


STAMP-Based Risk Assessment

GENERAL DYNAMICS
Mission Systems

Function 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 STAMP and STPA steps 1 and 2 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

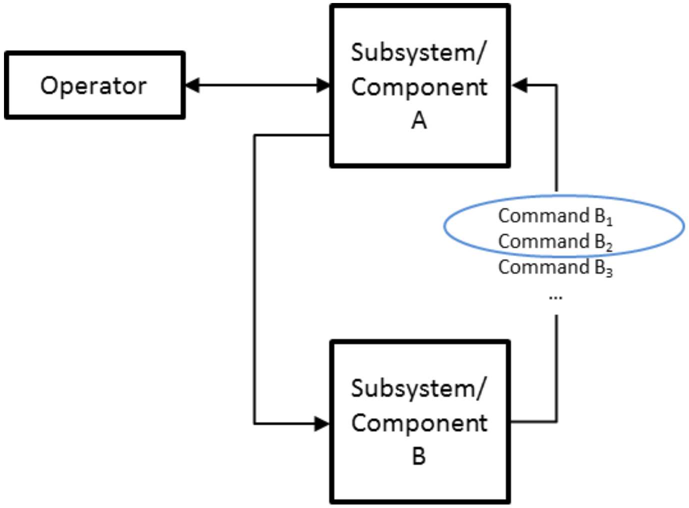


Functional Decomposition

GENERAL DYNAMICS
Mission Systems

3. DoD. (2012). Department of Defense Standard Practice: *System Safety.* Washington DC.: Department of Defense (DoD).

Function Allocations (con't)



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

GENERAL DYNAMICS
Mission Systems

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**

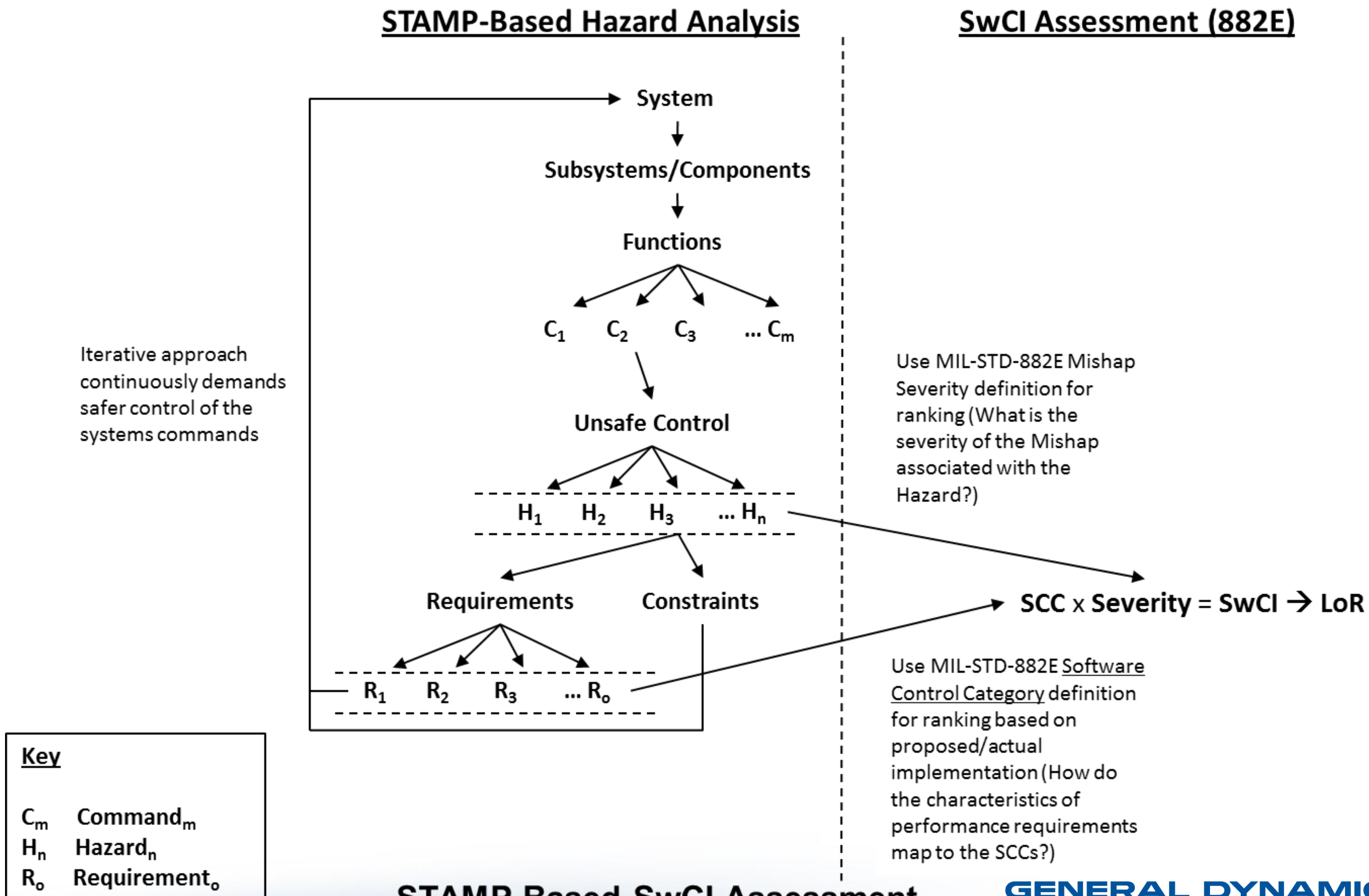
Subsystem/ Component	Function	Command	SCC	Unsafe Control	Hazard	Severity	SwCI	LoR
• *Electromechanical,* • *Digital,* • *Human, or* • *Social*[2]	A well order set of unique commands	A specific order issued by a Subsystem/ Component	The degree of software control (Autonomous, Semi-Autonomous, Redundant 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

GENERAL DYNAMICS
Mission Systems

3. DoD. (2012). Department of Defense Standard Practice: *System Safety.* Washington DC.: Department of Defense (DoD).

Software Criticality Index Assessments (con't)



STAMP-Based SwCI Assessment

GENERAL DYNAMICS
Mission Systems

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]

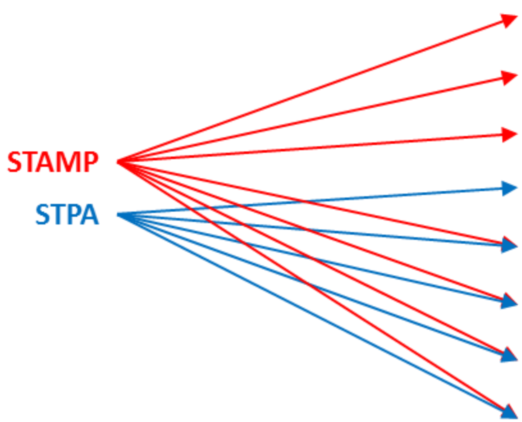
Safety Requirements and Constraints Traceability Matrix

GENERAL DYNAMICS
Mission Systems

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).

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 ✓



a. System Decomposition ✓
b. Functional Descriptions of Subsystems and Components ✓
c. Functional Description of Interfaces ✓
d. Identifying Unsafe Functional Behavior ✓
e. Mishap Severity and Risk Assessment ✓
f. Functional Allocations ✓
g. SCC and SwCI Assessments ✓
h. Identifying Safety Requirements and Constraints ✓

- 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

GENERAL DYNAMICS
Mission Systems

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

GENERAL DYNAMICS
Mission Systems

Benefits

- 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.

GENERAL DYNAMICS
Mission Systems