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
nmalloy@uab.edu
Advanced Safety and Engineering Management Masters of Engineering Program (Student)
University of Alabama at Birmingham School of Engineering

Table of Contents

Abstract 1
1 Introduction 2
2 Purpose 2
3 Background 2
4 Method 3
4.1 What is STAMP and STPA? 4
4.2 Improving MIL-STD-882E FHA through the Integration of STAMP and STPA 6
4.2.1 System Decomposition 8
4.2.2 Functional Descriptions of Subsystems and Components 11
4.2.3 Functional Descriptions of Interfaces 12
4.2.4 Identifying Unsafe Functional Behavior 13
4.2.5 Mishap Severity and Risk Assessment 14
4.2.6 Function Allocations 15
4.2.7 Software Control Category and Software Criticality Index Assessments 18
4.2.8 Identifying Safety Requirements and Constraints 20
5 Conclusion 21
6 References 23

Table of Tables

Table 1 Mapping STAMP and STPA to MIL-STD-882E 6
Table 2 Identifying Unsafe Control Actions 13
Table 3 Risk Assessment Traceability Matrix 15
Table 4 Software Safety Criticality Matrix [4] 18
Table 5 SwCI Assessment Traceability Matrix 19
Table 6 Hierarchy of Controls[6] 20
Table 7 Safety Requirements and Constraints Traceability Matrix 21

Table of Figures

Figure 1 Mapping STAMP-Based Hazard Analysis to MIL-STD-882E FHA 4
Figure 2 Control Structure for a Generic Man/Machine System 5
Figure 3 Generic Decomposition Diagram 9
Figure 4 CSCI, CSC, and CSU Decomposition 10
Figure 5 Control Structure for a Generic Man/Machine System (System Decomposition) 11

Figure 6 Control Structure for a Generic Man/Machine System (Functional Descriptions of Subsystems and Components)..... 12
Figure 7 Control Structure for a Generic Man/Machine System (Functional Descriptions of Interfaces) . 13
Figure 8 STAMP-Based Risk Assessment..... 14
Figure 9 Risk Assessment Matrix [4] 15
Figure 10 Functional Decomposition 16
Figure 11 Generic Control Structure 17
Figure 12 Functional Hazard Traceability Matrix..... 17
Figure 13 STAMP-Based SwCI Assessment 19

Abstract

This research demonstrates the integration of STAMP-Based Hazard Analysis with MIL-STD-882E Functional Hazard Analysis (FHA) and the advantages of using an iterative analysis approach that continually shapes the safety mechanisms of a system throughout the design process. To do this, a mapping exercise was performed which first broke the MIL-STD-882E FHA tasks into their respective elements followed by an allocation of the STAMP processes and STPA steps. As this was being performed rationale was documented that further reinforced the allocations. This information can be used as guidance for performing STAMP-Based Hazard Analysis on an actual system.

There are many benefits to be realized from taking a model based approach to system design. This is particularly evident in system safety engineering and more specifically hazard analysis. Model based hazard analysis allows for rapid hazard identification and mitigation development through safety requirements and constraints in a real-time environment. Such an approach enables safety practitioners to assess their systems through hypothetical conditions and then observe their potentially adverse behavioral responses. The systems theory derived tops down approach is a new way to perform hazard analysis that can compensate for the inadequacies associated with using dated approaches like Fault and Event Tree Analysis to assess today's complex systems.

1 Introduction

Safety culture needs to be less driven to assess and implement per standard procedures. Instead it should begin influencing organizations to execute through well-crafted safety processes. To make way for such a philosophy safety practitioners must step out of their comfort zones. At times comfort can be felt when a plan appears to be coming together. More specifically (from an engineering perspective) comfort, can be felt when a design implementation is performing as intended. This is when complacency can creep its way into the best intentioned of teams. Such behavior is often associated with happy talk and it is a recipe for disaster. An organizations goal should be to *never underestimate the magnitude of the forces that reinforce complacency or help to maintain the status quo*[1].

Safety practitioners must seek avenues to provide better assessments that are continually improvable. Such mindsets promote due diligence and encourage creating the safest systems possible. Of course, no system can be guaranteed completely safe but if the focus is improvement centric then the design, development, and implementation will exemplify the highest levels of rigor. Such an attitude combats the threat of complacency.

Avoiding complacency begins with exploring new ways of thinking. This is accomplished by breaking through business as usual paradigms. One such example of this is re-thinking MIL-STD-882E Functional Hazard Analysis (FHA) which uses traditional approaches and treats the problem as a component failure. *This approach is based upon the idea that a chain of continuous failure events will eventually lead to a loss. Such rationalization has built the foundation for most safety and reliability engineering analysis. This is characterized by Fault tree and event tree analysis which provide little guidance to the analyst. Both the model of the system being used by the analyst and the analysis itself are only in the analyst's head. Therefore, analyst expertise in using these techniques is crucial, and the quality of the fault or the event varies greatly. These traditional methods only consider anticipated unsafe conditions and fall short in identifying unexpected causal factors.* [2]

2 Purpose

This paper intends to demonstrate an approach for integrating a new hazard analysis process and approach with MIL-STD-882E FHA. System-Theoretic Accident Model and Processes (STAMP)-Based Hazard Analysis can be used to improve upon traditional hazard analysis techniques. This new way of thinking was developed to account for the complexity of today's socio-technical systems. STAMP and Systems-Theoretic Process Analysis (STPA) are consistent approaches that utilize stepwise methodology which can be used to analyze the safety significance of any system. They are particularly effective for developing system models, performing safety analysis, and implementing safety through design. All of this is linked directly to STAMP and STPAs collective effectiveness in identifying and understanding system hazards.

The MIL-STD-882E FHA is a foundational analysis that sets the stage for its safety programs instantiation of the standard. It is the cornerstone in a safety programs ability to identify, manage, and control its systems hazards. As such, its correctness proves to determine its completeness throughout the life cycle of the design process. STAMP-Based Hazard Analysis can be used to generate an improved MIL-STD-882E compliant FHA.

3 Background

MIL-STD-882E effectively provides high-level descriptions of tasks required to achieve standard compliance but certain tasks would greatly benefit from consistent instructions to support analysis execution. An example of this is the FHA. The FHA provides a point directed list of eight tasking elements

that are to be performed to demonstrate that the analysis has been satisfied. Some of these sub-tasks are straight forward while others are not.

For instance, system decomposition must be performed at the beginning of the analysis. Because decomposition is commonly a part of the systems engineering process this task (for the most part) is an easily satisfied objective. In other words, safety practitioners should not be banging their heads against a wall to figure it out. Similarly, the next two elements are intuitive and build upon the information gained during the decomposition. This is achieved by documenting detailed descriptions for each of the functional components and defining their associated interfaces. Despite its straight forwardness, decomposition can go south quickly. This is in fact the basis of argument for providing safety practitioners with a recommended approach like the one proposed in this paper.

The remaining analysis becomes less simplistic with a set of steps in the process that are increasing prone to subjective interpretation. The safety practitioner proceeds with identifying hazards by analyzing the functional components and their associated interfaces. Determining permutations of adverse behavior that introduce hazards will allow the safety practitioner to capture unsafe conditions. But there is no guidance describing how this should be achieved.

An experienced safety practitioner will note that this activity resembles a technique known as, What-if-Analysis. What-If-Analysis focuses on the inter-relational communications that occur between functional components. What-If-Analysis can be a powerful technique, in that it varies the timing (sequencing) of disturbances applied to functional components through targeted sensitivity testing which allows the safety practitioner to better understand the systems response to adverse conditions. What-If-Analysis is not as effective if the practitioner has performed an inadequate decomposition.

Example illustrations of recommended approaches would be helpful to validate the efforts leading up to this point. Unfortunately, What-If-Analysis is not listed as part of the task instruction so applying this approach is based purely upon assumption. This facilitates the struggle, confusion, and over reaching on behalf of the safety practitioner to meet the task description. If the decomposition is in fact flawed the effectiveness and quality of hazard identification and mitigation controls becomes susceptible to serious degradation. A decreasingly safe system ensues.

The MIL-STD-882E FHA activities can be broken into three parts. The first is hazard identification which begins with the before mentioned system decomposition and interface analysis. Next, management of the hazards identified must occur to ensure that they are being handled accordingly. This activity starts with the establishment of a Hazard Tracking Database (HTD). Lastly, in parallel the safety practitioners establish hazard mitigations which are characterized by controls and reflected in safety requirements and constraints that decrease the calculated risk. Their instantiation will reflect the systems safe performance.

Because the FHA tasking element descriptions lack specific instruction safety practitioners may unknowingly perform inadequate safety analyses. Indeterminate guidance allows them to approach system safety analysis in an inconsistent fashion. This means that if individual safety practitioners were each handed the same system design and instructed to perform a MIL-STD-882E FHA they would all likely take different approaches. This of course begs the question, “which approach is correct?”

4 Method

A new consistent approach in hazard identification adapted for complex systems is needed. To achieve standardization in the process and approach of generating an MIL-STD-882E FHA it is necessary to

explore alternative techniques. STAMP-Based Hazard Analysis provides the needed conceptual rigidity and contextual flexibility to perform accurate and complete hazard analysis consistently. It is comprised of the STAMP process and STPA approach and has shown to be successful in performing hazard analysis on systems in a variety of fields. Examples of a few of these are nuclear power, healthcare, automobiles, spacecraft, defense systems, and aviation. A previous research study that is particularly relevant to this paper was conducted by Nancy Leveson. In her paper, she discusses STAMP and STPAs compliance with MIL-STD-882E which includes FHA. Integrating STAMP-Based Hazard Analysis with MIL-STD-882E FHA is achieved through a simple mapping exercise as illustrated by Figure 1. This exercise traces the processes and approaches of STAMP and STPA to the eight tasking elements.

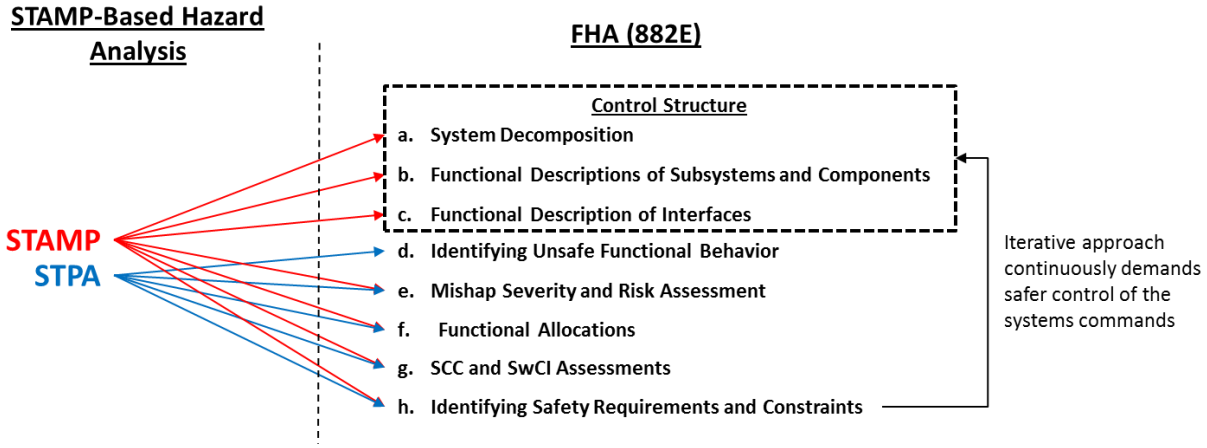


Figure 1 Mapping STAMP-Based Hazard Analysis to MIL-STD-882E FHA

4.1 What is STAMP and STPA?

STAMP changes the emphasis in system safety from preventing failures to enforcing behavioral safety constraints. Component failure accidents are still included, but the conception of causality is extended to include component interaction accidents. Safety is reformulated as a control problem rather than a reliability problem. This change leads to much more powerful and effective ways to engineer safer systems, including the complex sociotechnical systems of most concern today. The three main concepts in this model are safety constraints, hierarchical control structures and process models.[2]

STPA depends upon the establishment of these concepts prior to its own execution and can be used at any stage of the system life cycle. It has the same general goals as any hazard analysis technique: accumulating information about how the behavioral safety constraints, which are derived from the system hazards, can be violated. Depending on when it is used, it provides the information and documentation necessary to ensure the safety constraints are enforced in the system design, development, manufacturing, and operations, including the natural changes in these processes that will occur over time.

STPA uses a functional control diagram and safety requirements, system hazards, and the safety constraints and safety requirements for the component. When STPA is applied to an existing design, this information is available when the analysis process begins. When STPA is used for safety-guided design, only the system-level requirements and constraints may be available at the beginning of the process. In the latter case, these requirements and constraints are refined and traced to individual system components as the iterative design and analysis process proceeds.

Figure 2 depicts a control structure for a generic man/machine system that consists of a Human Operator and two subsystems/components. Their associated interfaces are identified and further information is provided to indicate some of the commands passing through them.

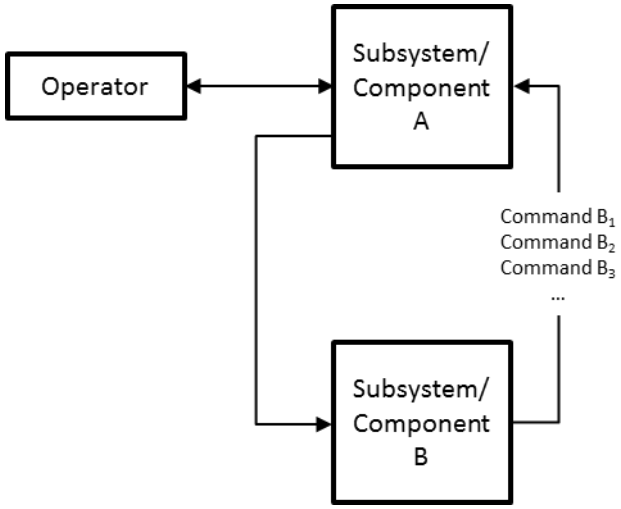


Figure 2 Control Structure for a Generic Man/Machine System

STPA has two main steps:

1. *Identify the potential for inadequate control of the system that could lead to a hazardous state. Hazardous states result from inadequate control or enforcement of the safety constraints, which can occur because:*
    a. *A control action required for safety is not provided or not followed.*
    b. *An unsafe control action is provided.*
    c. *A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequence.*
    d. *A control action required for safety is stopped too soon or applied too long.*
2. *Determine how each potentially hazardous control action identified in step 1 could occur.*
    a. *For each unsafe control action, examine the parts of the control loop to see if they could cause it. Design controls and mitigation measures if they do not already exist or evaluate existing measures if the analysis is being performed on an existing design. For multiple controllers of the same component or safety constraint, identify conflicts and potential coordination problems.*
    b. *Consider how the designed controls could degrade over time and build in protection, including*
        i. *Management of change procedures to ensure safety constraints are enforced in planned changes.*
        ii. *Performance audits where assumptions underlying the hazards analysis are the preconditions for the operational audits and controls so that unplanned changes that violate the safety constraints can be detected.*
        iii. *Accident and incident analysis to trace anomalies to the hazards and to the system design.*

While the analysis can be performed in one step, dividing the process into discrete steps reduces the analytical burden on the safety engineers and provides a structured process for hazard analysis. The information from the first step (identifying the unsafe control actions) is required to perform the second step (identifying the causes of the unsafe control actions).[2]

4.2 Improving MIL-STD-882E FHA through the Integration of STAMP and STPA

The primary purpose FHA serves is identification and classification of system functions and safety consequences of a functional failure or malfunction. In other words, what are the inherent hazards in the design? This is what STAMP and STPA were designed for. By analyzing the control structure inadequate control actions and their associated hazards are revealed. This allows the safety practitioner to draw correlations between areas of safety significance and non-safety-significance within the system. In doing so further focus can be applied to identifying the consequences of the hazards. Furthermore, in practice as a system begins to take shape the design team can generate safety requirements and constraints to improve its overall safety.

Table 1 captures the analysis results of the mapping exercise depicted by Figure 1. The intention is to show how STAMP and STPA can be integrated to support and in fact improve the FHA tasking elements framework provided in MIL-STD-882E. Note that there are certain aspects of FHA that call out Probabilistic Risk Assessment (PRA) and various software specific assessments that are based on software implementation unique to MIL-STD-882E. Instructions regarding these are contained in Section 4 of the standard and should be referenced to meet their full intent. Details are provided in the table acknowledging the uniqueness's which are accompanied by explanations to support the integration of STAMP and STPA.

Table 1 Terminology

Tasking Element – The alpha designator corresponds to the alpha designator provided in MIL-STD-882E.
MIL-STD-882E FHA Tasking Element Description – The description corresponds to the alpha designator tasking description provided in MIL-STD-882E.
Allocation – The allocation corresponds with the corresponding MIL-STD-882E FHA Tasking Element Description ability to be accomplished by STAMP or STPA.
Rationale – The rationale provides justification pertaining to the corresponding MIL-STD-882E FHA Tasking Element Description and Allocation.

Table 1 Mapping STAMP and STPA to MIL-STD-882E

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.*[4]	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.

Tasking Element	MIL-STD-882E FHA Tasking Element Description	Allocation	Rationale
b.	*A functional description of each subsystem and component identified.*[4]	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 continue to occur.
c.	*A functional description of interfaces between subsystems and components. Interfaces should be assessed in terms of connectivity and functional inputs and outputs.*[4]	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 continue to occur.
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.*[4]	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.
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.*[4]	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]

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 MIL-STD-882E 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).*[4]	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
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.*[4]	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.
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.*[4]	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.

4.2.1 System Decomposition

STAMP is used as a mechanism by the safety practitioner to understand the decomposition of the system and its related subsystems to the major component level. This lays the framework for the creation of the control structure to be used for STPA. The system must be analyzed functionally from the perspective of both "what the system is documented to do functionally", and "what you think the system can do functionally". The former is an assessment of documented functionality from the functional specifications and the latter is assessed by analyzing the functionality of the physical components of the system. The analysis of the physical attributes of the system is likely to provide insight to "hidden" or undocumented functionality. This is especially true for systems heavily using COTS components.

To ensure that a system is adequately understood safety practitioners should perform three separate yet related decompositions:

- Hardware Level Decomposition
- System Level Decomposition
- Software Level Decomposition (if needed)

In the context of developing a FHA the physical system can viewed as any system consisting of hardware components which in some way interface with the total system. One must consider from a physical design perspective whilst analyzing system functionally that the system itself is likely comprised of multiple subsystems. Figure 3, depicts a generic decomposition system architecture diagram.

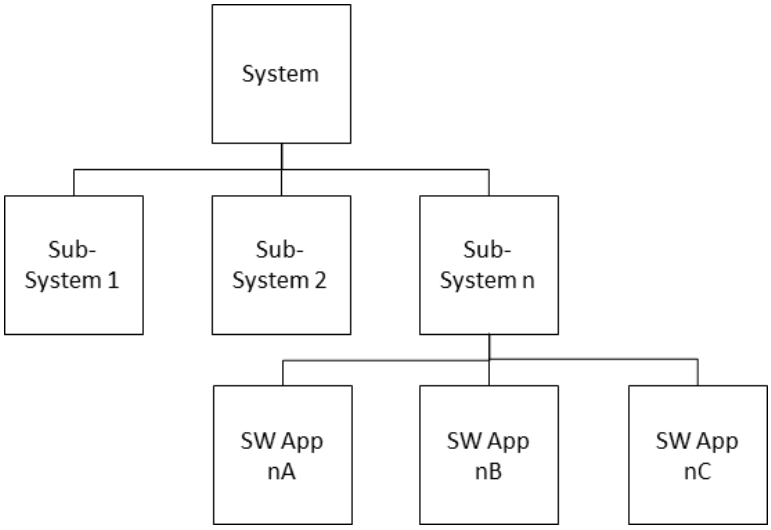


Figure 3 Generic Decomposition Diagram

Establishing physical aspects (physical boundaries) will allow for increased granularity of the system architecture at the functional level. This is the beginning of establishing the delineation between separate physical components and the systems expected behavior (discrete events over time). Software applications are to be grouped and/or categorized so that they correspond with their related upper level physical components. Such lower level detail can be captured once all the physical boundaries of the upper level components have been determined.

Organization of the system architecture involves an approach through which the system design is decomposed and grouped by behavioral functions. These functions (which are conceptualized by the system architecture) represent the structure of the hardware and its software (if present) accompanied by its expected behavior. Categorizing the system by behavioral characteristics allows its basic functionality to be understood more intuitively. Furthermore, if any of the sub-groupings of functions are overly complex on their own continued decomposition can be considered.

Be aware that this is a first step towards the development of control structures. Later, as the FHA progresses an examination of different hazards will occur. Only certain subsets (functional groupings or elements) of the overall structure may be relevant. Therefore, only these will require detailed consideration. When building the structure of a basic control loop it should be noted that the function serves the role of the Controlled Process which receives Controlled Variables, Process Inputs, and

experiences Disturbances. These will represent inadequate control actions exercised during the first part of the STPA. Likewise, the Controlled Process will generate and transmit Measured Variables and Process Outputs. These will later become the unsafe conditions which have been created because of the inadequate control actions having been applied.

If software exists in a system, it should also be decomposed. Commonly software functions are referred to as Computer System Configuration Items (CSCI) and are viewed as single entities comprised of a group of software. Software grouped in a manner such that it is defined as a CSCI consists of two or more Computer Software Components (CSCs). CSCs may be further decomposed into other CSCs and Computer Software Units (CSUs). A CSU is an element specified in the design of a CSC. Figure 4 depicts the three levels of decomposition that can be applied to a software function.

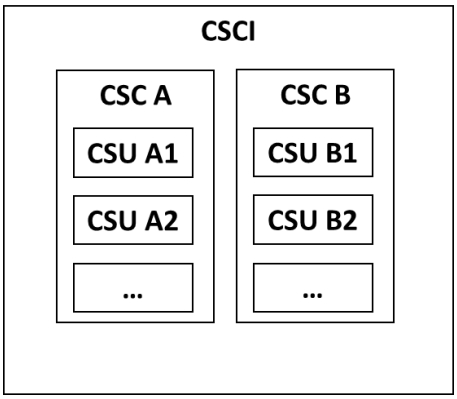


Figure 4 CSCI, CSC, and CSU Decomposition

A software-level functional decomposition is generated in a hierarchical manner that takes into consideration the nesting characteristics of Figure 4. A different perspective in understanding the interactive relationship between CSCs (SW App) and CSUs can be established by developing diagrams like the one depicted in Figure 3.

Such a diagram aids in showing the hierarchical relationship through associated interfaces. These interfaces can provide further insight into the flow of messaging information that is being passed to and from applications throughout the systems software architecture.

Once all necessary information regarding the systems makeup has been determined the construction of the STAMP control structure can begin. Figure 5 depicts a control structure for a generic man/machine system with pronounced green boarders that are intended to place emphasis on its functional components.

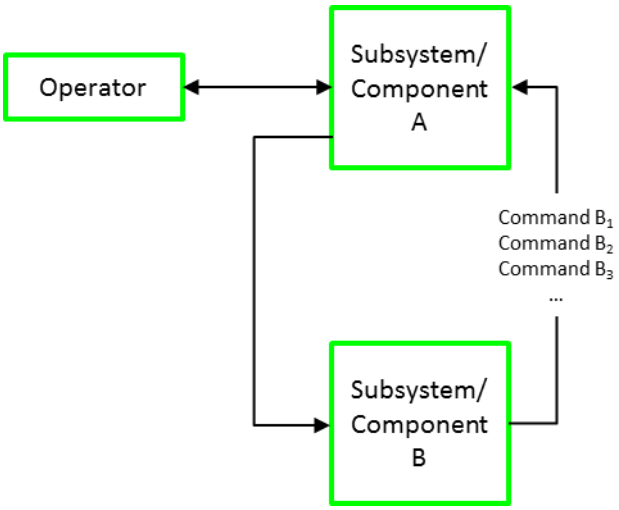


Figure 5 Control Structure for a Generic Man/Machine System (System Decomposition)

4.2.2 Functional Descriptions of Subsystems and Components

The safety practitioner uses the STAMP based processes as a mechanism for determining the functional description of each subsystem and component identified. The functional design description should be completed in parallel with the functional decomposition of the system. It makes sense to do it this way because if the functions are to be defined correctly a proper descriptive understanding of their behavior must be first well documented.

As suggested by the Joint Services - Software Safety Authorities (JS-SSA) Implementation Guide when capturing functional descriptions, there are three things that should be considered:

- *First, the identification of what the element can or should do functionally. Creating a detailed list can be helpful in developing incorrect process models at a later point.*
- *Second, a comparison of the functionality identified with the documented functionality of the functional specification followed by a reconciliation of the two lists.*
- *Last, identification of any functionality that is identified in hardware literature or the performance specification to determine if there are "hidden" or unintended functions residing in the system.*

As the practitioner works through this exercise a table can be used to capture the physical boundaries, functional decomposition (behavior), associated software decomposition, and corresponding functional descriptions. Figure 6 depicts a control structure for a generic man/machine system with pronounced green shading that is intended to place emphasis on its functional description of the system components.

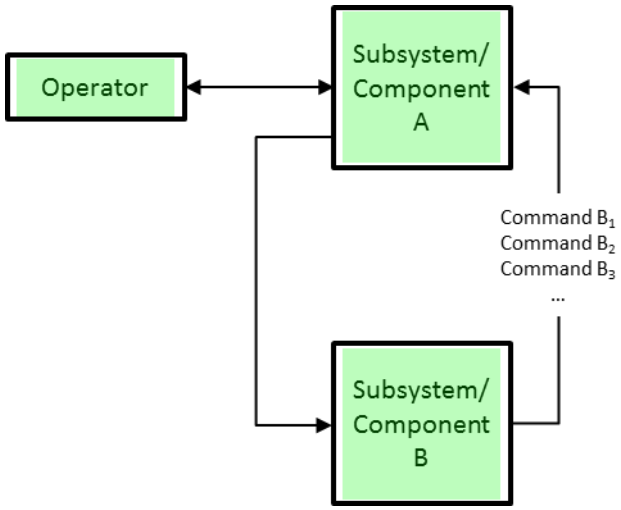


Figure 6 Control Structure for a Generic Man/Machine System (Functional Descriptions of Subsystems and Components)

This is a convenient artifact that can be used for other applications in the future which serve in meeting the expected outputs of various Level of Rigor (LoR) tasking. One such example of reuse is as contribution to the development of a Requirements Traceability Matrix (RTM). Additional details regarding the contents and guidance for creating a RTM can be found in the Joint Software System Safety Engineering Handbook (JSSSEH).

4.2.3 Functional Descriptions of Interfaces

The STAMP based processes can be used as a mechanism for documenting the functional description of interfaces between subsystems and components. Interfaces should be assessed in terms of connectivity and functional inputs and outputs. Interfaces amount to being the medium through which subsystems and components communicate. In some cases, these lines of communication are one directional while under different circumstances they may be bi directional. Identifying the interfaces that exist within the control structure is the final step required to prepare it for STPA step 1.

Figure 7 depicts a control structure for a generic man/machine system with pronounced green shading that is intended to place emphasis on its functional description of the system interfaces.

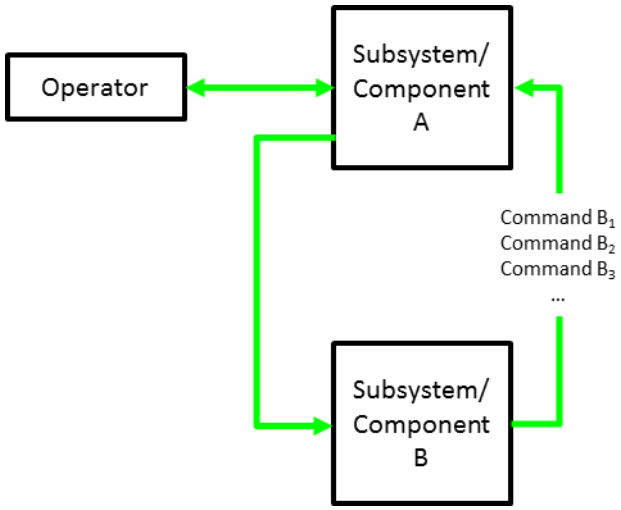


Figure 7 Control Structure for a Generic Man/Machine System (Functional Descriptions of Interfaces)

4.2.4 Identifying Unsafe Functional Behavior

STPA step 1 is used by the safety practitioner to determine 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. Performing interface analysis aids the safety practitioner in understanding the consequences associated with the presence of adverse control actions. This is achieved through the application of What-if-Analysis which is a technique that varies the sequence of signal initiation. In the same way that unsafe control actions can be determined unsecure control actions can be determined as well.

Unsafe control actions can also be associated with security implications. Modifying the context of the analysis to consider unsafe control actions linked to security vulnerabilities provides the practitioner with an opportunity to apply hypothetical point directed system penetrations. This reveals the systems theoretical response and allows mitigations to be developed in the form of security features. Security requirements and constraints characterize these features. While safety and security are contextually different conceptually they can equally contribute to mishaps or in general terms loss.

Table 2 shows the four categories of unsafe control actions that can be applied to a control process. The green shading is intended to place emphasis on the types of unsafe control actions that can occur for any given system.

Table 2 Identifying Unsafe Control Actions

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

4.2.5 Mishap Severity and Risk Assessment

MIL-STD-882E instructs the safety practitioner to perform an assessment of the risk associated with each identified failure of a function, subsystem, or component. Additionally, it requires that the safety practitioner estimate severity, probability, and Risk Assessment Code (RAC) using the process it describes in its own Section 4. These activities are clearly not identified as being a part of either STAMP or STPA but Figure 8 attempts to demonstrate a potential approach to using information obtained through STAMP-Based Hazard Analysis to determine the probability and severity assessments required to develop a risk assessment.

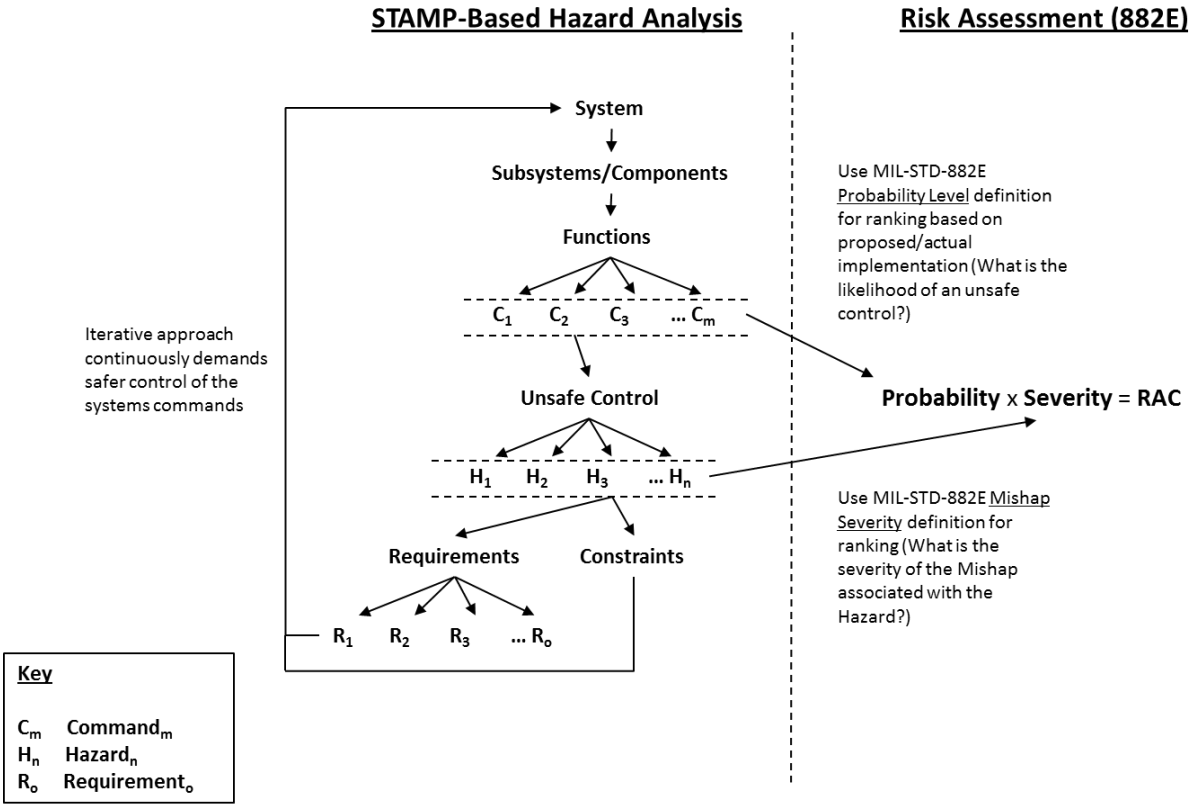


Figure 8 STAMP-Based Risk Assessment

STPA and STAMP 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. Additionally, it should be acknowledged that Hazards are not just the result of functional failure or malfunction. 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.[2]

As the safety practitioner goes through the iterative STAMP and STPA process they can begin assigning mishap severities and probabilities of occurrence (qualitative or quantitative) to the hazards identified. As the safety requirements and constraints are developed educated design decisions can be made to alter the control structure which will in theory improve the safety of the system. It should also be mentioned that the safety requirements and constraints are intended to reduce the likelihood of occurrence through their implementation. For the readers' clarity Figure 9 depicts the Risk Assessment Matrix found in Section 4 of MIL-STD-882E. Through the identification of a hazards probability of

occurrence and mishap severity a ranked risk can be calculated and used as a method for describing the magnitude of risk.

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Figure 9 Risk Assessment Matrix [4]

PRA as it pertains to complex systems is inherently flawed but in order to maintain compliance with MIL-STD-882E it is necessary to complete the risk assessment tasking element. The information collected while performing STAMP-Based Hazard Analysis can be combined with risk assessment specific data and managed using a traceability matrix like the one provided in Table 3.

Table 3 Risk Assessment Traceability Matrix

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

4.2.6 Function Allocations

STAMP and STPA are used by the safety practitioner to perform 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 MIL-STD-882E 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). Figure 10 illustrates a proposed approach for depicting the functional decomposition of a system subsystem/component down to the command level.

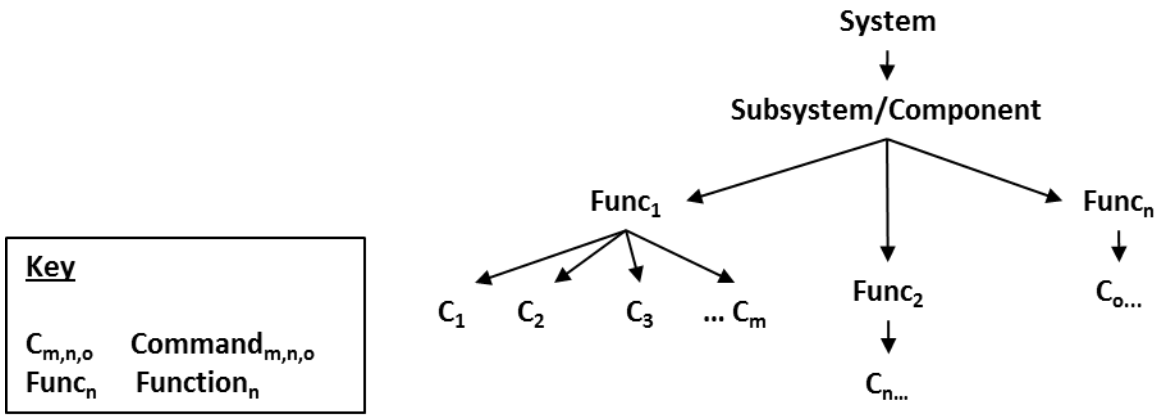


Figure 10 Functional Decomposition

When embarking down the path of FHA the practitioner can easily become lost in the breakdown of the eight tasking elements. What must be done to satisfy them? Is there an order of operations that works best? And lastly, how do they relate to each other? In other words – are their shared dependencies between tasking elements and does that drive a sequence that which they need to occur? Advance knowledge of this can aid in the efficiency of the exercise. Case and point – certain steps can be performed in parallel which can help the safety practitioner manage the process more efficiently. To be successful in the analysis these questions must be understood.

Depending on the complexity of the system there can be several factors driving its composition. Today's systems reflect *both complex technical and social processes*[2]*.* The relationship between man, machine, and software has led to the development of socio-technical systems that represent a mixture of people, technology, and their environment.

The first three elements of FHA instruct the practitioner to perform detailed system decomposition. The goal of this exercise is to develop a control structure that captures the systems characteristics. A common mistake that safety practitioners fall prey to is misrepresenting their functions. Often it is easy to assume that individual system inputs and outputs (signals) are functions. This is not the case. Signals represent a single result that is dependent upon specific system processing but not a function per say. A simplified way of conceptualizing this is by taking a mathematical approach. In mathematics, a set is a well-defined collection of distinct objects. The objects within the set are referred to as elements. Thus, to complete the comparison – a system function can be characterized as a well-defined collection of distinct signals.

The development of functions begins first by defining the characteristics of the systems control structure. The controls are to be identified by drawing a control structure that identifies each of the subsystems that make up the greater system. If the system depends on operator of environmental inputs these should be represented as separate subsystems. The subsystems are the controls within the control structure. Such an approach is simple, straight forward and conveniently enables others who are less familiar with the system to gain a high-level perception of its composition. The practitioner must define the interfaces between the controls to complete the control structure. These interfaces carry control actions that are representative of the stimulus outputted by the controls. Figure 11 depicts a generic control structure.

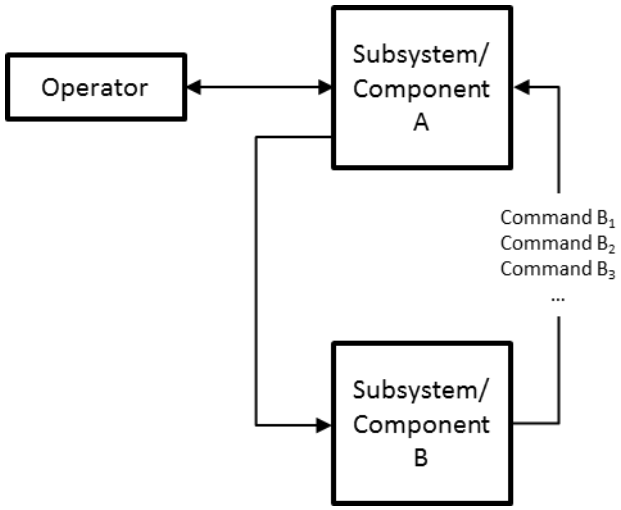
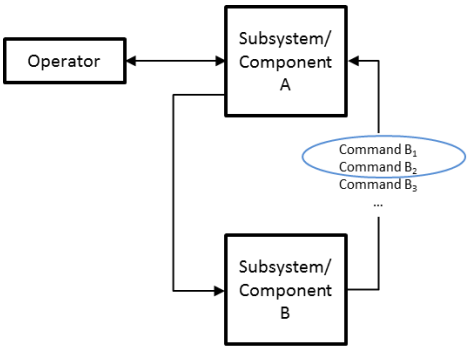


Figure 11 Generic Control Structure

Once the control structure has been created the safety practitioner can begin establishing functional categories by grouping control actions together based on their shared intent. The functional categories will ultimately become the system functions. This is necessary for establishing traceability to the hazards identified during the first step of STPA. Figure 12 depicts a generic functional hazard traceability exercise.



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				

Key

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

Figure 12 Functional Hazard Traceability Matrix

Greater granularity can be established by taking the traceability and integrating additional layers of detail that pertain specifically to how the functions are to be implemented. Will the function be hardware? Is the function intended to be a combination of hardware and software? Perhaps the functional will be reflective of a human characteristic? Further detail into the relationship between system functions and their implementation will allow the practitioner to specify safety-significant hardware, software, and operator controls through the already established hazards. Careful consideration can be applied to detailed implementation with such an approach.

4.2.7 Software Control Category and Software Criticality Index Assessments

STPA step 1 is used to determine 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. Every step of the way STPA lays the framework necessary to perform a FHA. Its order of operations allows for straight forward execution. Additionally, the simplicity of its format makes it easy for safety practitioners to use the process on new and legacy systems alike.

Table 4 depicts the Software Safety Criticality Matrix and Level of Rigor (LoR) Tasking provided in Section 4 of MIL-STD-882E.

Table 4 Software Safety Criticality Matrix [4]

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

For systems in which software is present STPA aids in identifying where safety-significant functionality resides. This information when combined with the appropriate SCC and Mishap Severity can be used to determine the SwCI and associated LoR tasking that is required per MIL-STD-882E. This provides the safety practitioner with an opportunity to apply code, architecture, and requirements analysis and safety specific testing if deemed necessary by the LoR tasking instructions. The JSSSEH describes these tasks in detail. Additionally, it defines software process, standards, and guidance in the form of

requirements. These are to be interpreted as recommended best practices and are tailorable to meet the needs of any given system. The information collected while performing STAMP-Based Hazard Analysis can be combined with SwCI assessment specific data and managed using a traceability matrix like the one provided in Table 5.

Table 5 SwCI Assessment Traceability Matrix

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]

SCC and SwCI are unique to MIL-STD-882E but its calculation can be treated as a function of the STPA outputs. Figure 13 attempts to demonstrate a potential approach to using information obtained through STAMP-Based Hazard Analysis to determine the SCC and severity assessments required to develop a SwCI assessment.

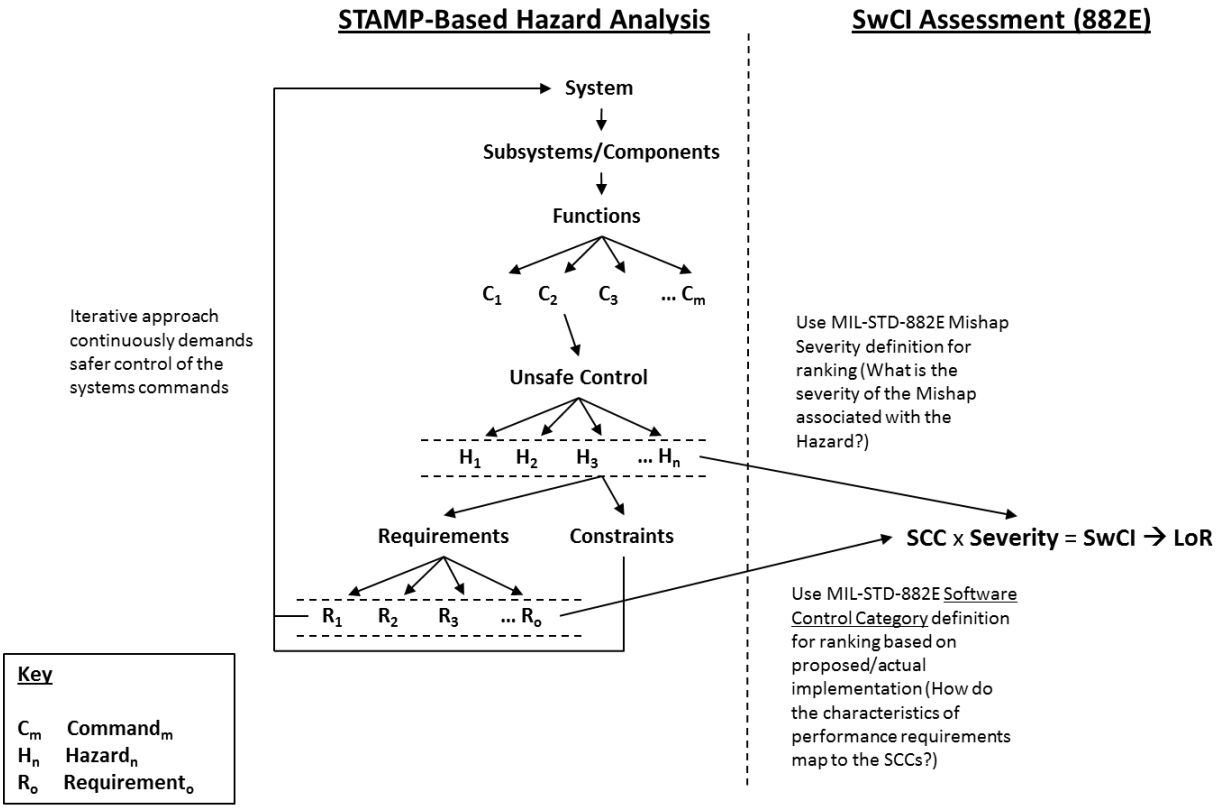


Figure 13 STAMP-Based SwCI Assessment

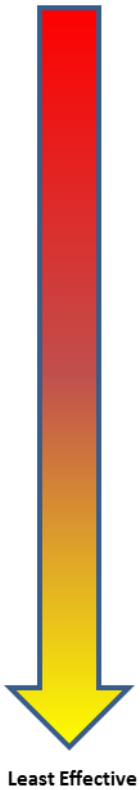
Mishaps are determined throughout the execution of STPA step 1 to aid in the determination of unsafe control actions and their associated hazards. Assessments of the documented mishaps in accordance with MIL-STD-882E guidance are required. Combining the SCCA and Mishap Severity assessment provides the safety practitioner with the data needed to calculate the SwCI and determine the associated LoR tasking required for standard compliance.

4.2.8 Identifying Safety Requirements and Constraints

STPA step 2 is used to develop 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. The list of potential hazards threatening the safety of a system is the driving force behind the development and implementation of safety requirements and design constraints.

Once the hazards have been identified and documented the practitioner can begin to determine how they will be prevented. This is accomplished through the hierarchy of controls in traditional system safety theory. The hierarchy of controls is an engineering approach used to manage risk at a level that is reasonably practicable. This is accomplished through the utilization of a series of six controls which are elaborated upon in Table 6.

Table 6 Hierarchy of Controls[6]



Controls	Examples
Elimination	Design to eliminate Hazards, such as falls, hazardous materials, noise, confined spaces, and manual material handling
Substitution	Substitute for less hazardous material Reduce energy. For example: Lower speed, force, amperage, pressure, temperature, and noise.
Engineering Controls	Ventilation systems Machine guarding Sound enclosures Circuit breakers Platforms and guard railing Interlocks Lift tables, conveyors, and balancers
Warnings	Signs Backup alarms Beepers Horns Labels
Administrative Controls	*Procedures* Safe job procedures Rotation of workers Safety equipment inspections Changing work schedule *Training* Hazard Communication Training Confined space entry
Personal Protective Equipment	Safety glasses Hearing protection Face shields Safety harnesses and lanyards Gloves Respirators

The examples provided in Table 6 are intended to create a sense for what safety design constraints are seeking to achieve. A constraint is a statement of restriction that modifies a requirement or set of requirements by limiting the range of acceptable solutions. In a socio-technical system it should not be surprising that design constraints associated to system performance, operability and personal protection are present. When considering the implementation of the controls it is evident that the preferred approach is hazard elimination. This can drive cost increases so it may be decided that less effective approaches will be exercised to reduce the associated risk to an acceptable level.

Maintaining the documented risks through a traceability matrix is an effective approach to keeping track of the hazards present in a systems design and the safety design constraints that have been developed to address them. The information collected throughout the iterative execution of STAMP-Based Hazard Analysis can be managed using a traceability matrix like the one provided in Table 7.

Table 7 Safety Requirements and Constraints Traceability Matrix

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]

System-level constraints are refined and allocated to each component during the systems engineering decomposition process.[2] it's possible that as the design process progresses constraints may conflict with each other. There is great value in this because *identifying these types of conflicts early in the design process will lead to better solutions. Choices may be more limited later when it may not be possible or practical to change the early decisions*[2]*.* Ideally, as a system is developed and then further refined through more targeted design decisions the safety requirements and constraints will mature with the obvious result being a safer system.

5 Conclusion

STAMP-Based Hazard Analysis provides the needed conceptual rigidity and contextual flexibility to perform accurate and complete FHA consistently. It is especially useful for the safety practitioner to have at their disposal an approach to hazard analysis that is constructed upon iterative steps. These steps and their repetition add consistency and repeatability. It also enables safety practitioners to easily delegate work to associated team members without the burden of excessive tutelage being required.

The mapping Exercise works. Using a table to break down the eight MIL-STD-882E FHA tasking elements allows for easy traceability from the appropriate STAMP-Based Hazard Analysis process to an associated tasking element. There are certain tasking elements which call out PRA and various software (functional control) specific assessments that are based on software implementation and unique to MIL-STD-882E. Although, this is not a problem considering that these assessments can be influenced by the information captured from the STAMP-Based Hazard Analysis approach.

This mapping exercise should be used as the basis for generating a document that serves to instantiate STAMP-Based Hazard Analysis to perform MIL-STD-882E FHA. In doing so safety practitioners would be

provided with the continued flexibility that MIL-STD-882E is intended to offer along with the strength of a consistent hazard analysis approach. Recognizing a consistent approach for the FHA in MIL-STD-882E would ensure that all safety practitioners can begin their safety programs on the right foot.

6 References

1. DoD. (2012). *Department of Defense Standard Practice: System Safety.* Washinton DC.: Department of Defense (DoD).
2. Kotter, J. P. (2012). *Leading Change.* Boston, Massachusetts: Harvard Business Review Press.
3. Leveson, N. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety.* Cambridge, Massachusetts: The MIT Press.
4. Leveson, N. (2016). *STPA Compliance with Army Safety Standards and Comparison with SAE ARP 4761.* Cambridge, Massachusetts: The MIT Press.
5. Young, W., & Leveson, N. (2014). Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory. *Communications of the ACM*, 1-5.
6. Bidez, M. W. (n.d.). Module 1a: Fundemental Concepts ASEM 610. Birmingham, Alabama, United States.