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
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 straightforward 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

STAMP-Based Hazard Analysis

FHA (882E)

- System Decomposition
- Functional Descriptions of Subsystems and Components
- Functional Description of Interfaces
- Identifying Unsafe Functional Behavior
- Mishap Severity and Risk Assessment
- Functional Allocations
- SCC and SwCI Assessments
- Identifying Safety Requirements and Constraints

- 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

<table>
<thead>
<tr>
<th>Tasking Element</th>
<th>MIL-STD-882E FHA Tasking Element Description</th>
<th>Allocation</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td><em>Decomposition of the system and its related subsystems to the major component level.</em>[^3]</td>
<td>STAMP</td>
<td>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.</td>
</tr>
</tbody>
</table>

---


---

![Control Structure for a Generic Man/Machine System](image-url)
### Functional Descriptions of Subsystems and Components

<table>
<thead>
<tr>
<th>Tasking Element</th>
<th>MIL-STD-882E FHA Tasking Element Description</th>
<th>Allocation</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>b.</td>
<td>A functional description of each subsystem and component identified.³</td>
<td>STAMP</td>
<td>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.</td>
</tr>
</tbody>
</table>

---

![Control Structure for a Generic Man/Machine System](image-url)

---

### Functional Descriptions of Interfaces

<table>
<thead>
<tr>
<th>Tasking Element</th>
<th>MIL-STD-882E FHA Tasking Element Description</th>
<th>Allocation</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>c.</td>
<td>A functional description of interfaces between subsystems and components. Interfaces should be assessed in terms of connectivity and functional inputs and outputs.³</td>
<td>STAMP</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Control Structure for a Generic Man/Machine System**

## Identifying Unsafe Functional Behavior

<table>
<thead>
<tr>
<th>Tasking Element</th>
<th>MIL-STD-828E FHA Tasking Element Description</th>
<th>Allocation</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>d.</td>
<td>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</td>
<td>STPA</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Identifying Unsafe Control Actions²

<table>
<thead>
<tr>
<th>Action</th>
<th>Not Providing Causes Hazard</th>
<th>Providing Causes Hazard</th>
<th>Incorrect Timing / Order</th>
<th>Stopped Too Soon / Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

# Identifying Unsafe Functional Behavior

<table>
<thead>
<tr>
<th>Tasking Element</th>
<th>MIL-STD-82E FHA Tasking Element Description</th>
<th>Allocation</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>d.</td>
<td><em>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.</em>&lt;sup&gt;3&lt;/sup&gt;</td>
<td>STPA</td>
<td>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.</td>
</tr>
</tbody>
</table>

---

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

- **Example: Security**
  - Integrated approach to Safety and Security with STPA-Sec<sup>4</sup>
    - Physical, Cyber, Parts Tampering, etc.

---

### Risk Assessment

<table>
<thead>
<tr>
<th>Tasking Element</th>
<th>MIL-STD-882E FHA Tasking Element Description</th>
<th>Allocation</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>e.</td>
<td>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</td>
<td>STAMP STPA</td>
<td>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</td>
</tr>
</tbody>
</table>

\[
\text{Probability} \times \text{Severity} = \text{RAC}
\]

<table>
<thead>
<tr>
<th>Subsystem/Component</th>
<th>Function</th>
<th>Command</th>
<th>Unsafe Control</th>
<th>Hazard</th>
<th>Severity</th>
<th>Probability</th>
<th>RAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Electromechanical, • Digital, • Human, or • Social²</td>
<td>A well order set of unique commands</td>
<td>A specific order issued by a Subsystem/Component</td>
<td>A specific order issued by a Subsystem/Component that contributes/leads to a hazard</td>
<td>A real or potential condition that could lead to a mishap</td>
<td>An event or series of events that result in a loss</td>
<td>A quantitative or qualitative assessment used to express the likelihood of an events occurrence</td>
<td>An assessment comprised of mishap probability and severity</td>
</tr>
</tbody>
</table>

Risk Assessment (con’t)

STAMP-Based Hazard Analysis

- System
- Subsystems/Components
  - Functions
    - $C_1$, $C_2$, $C_3$, ..., $C_m$
  - Unsafe Control
    - $H_1$, $H_2$, $H_3$, ..., $H_n$
  - Requirements
    - $R_1$, $R_2$, $R_3$, ..., $R_o$
  - Constraints

Risk Assessment (882E)

- Use MIL-STD-882E Probability Level definition for ranking based on proposed/actual implementation (What is the likelihood of an unsafe control?)

- Probability x Severity = RAC

- Use MIL-STD-882E Mishap Severity definition for ranking (What is the severity of the Mishap associated with the Hazard?)

Key:
- $C_m$ Command$_m$
- $H_n$ Hazard$_n$
- $R_o$ Requirement$_o$
## Function Allocations

<table>
<thead>
<tr>
<th>Tasking Element</th>
<th>MIL-STD-882E FHA Tasking Element Description</th>
<th>Allocation</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>f.</td>
<td>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)</td>
<td>STAMP STPA</td>
<td>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</td>
</tr>
</tbody>
</table>

### Functional Decomposition

```
Key
C_{m,n,o}, \text{Command}_{m,n,o}, \text{Func}_n, \text{Function}_n

System
   ↓
  Subsystem/Component
     ↓
   Func_1
   ↓
  C_1 \ C_2 \ C_3 \ ... \ C_m
     ↓
   Func_2
     ↓
   C_n...
```

Function Allocations (con’t)

### Key

<table>
<thead>
<tr>
<th>Func_n</th>
<th>Function_n</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCI</td>
<td>Computer Software Configuration Item</td>
</tr>
<tr>
<td>CSC</td>
<td>Computer Software Component</td>
</tr>
<tr>
<td>CSU</td>
<td>Computer Software Unit</td>
</tr>
</tbody>
</table>

### Functional Hazard Traceability Matrix

<table>
<thead>
<tr>
<th>Function</th>
<th>Command</th>
<th>Control Interface Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Func_1</td>
<td>Command B_1</td>
<td>Hardware, Software, or Human</td>
</tr>
<tr>
<td></td>
<td>Command B_2</td>
<td></td>
</tr>
<tr>
<td>Func_2</td>
<td>Command B_3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Command B_4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Command B_5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Command B_6</td>
<td></td>
</tr>
<tr>
<td>Func_n</td>
<td>Command B_7</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCI</td>
</tr>
<tr>
<td>-------</td>
</tr>
</tbody>
</table>
Software Criticality Index Assessments

<table>
<thead>
<tr>
<th>Tasking Element</th>
<th>MIL-STD-882E FHA Tasking Element Description</th>
<th>Allocation</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>g.</td>
<td>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.</td>
<td>STAMP STPA</td>
<td>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.</td>
</tr>
</tbody>
</table>

Software Criticality Index Assessments (con’t)

**STAMP-Based Hazard Analysis**

- System
  - Subsystems/Components
    - Functions
      - \( C_1 \), \( C_2 \), \( C_3 \), ..., \( C_m \)
      - Unsafe Control
        - \( H_1 \), \( H_2 \), \( H_3 \), ..., \( H_n \)
          - Requirements
            - \( R_1 \), \( R_2 \), \( R_3 \), ..., \( R_o \)

**SwCI Assessment (882E)**

- Use MIL-STD-882E Mishap Severity definition for ranking (What is the severity of the Mishap associated with the Hazard?)

- Use MIL-STD-882E Software Control Category definition for ranking based on proposed/actual implementation (How do the characteristics of performance requirements map to the SCCs?)

**Key**

- \( C_m \) Command\(_m\)
- \( H_n \) Hazard\(_n\)
- \( R_o \) Requirement\(_o\)

**STAMP-Based SwCI Assessment**

Iterative approach continuously demands safer control of the systems commands

©2017 General Dynamics. All rights reserved.
Identifying Safety Requirements and Constraints

<table>
<thead>
<tr>
<th>Tasking Element</th>
<th>MIL-STD-882E FHA Tasking Element Description</th>
<th>Allocation</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>h.</td>
<td>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.</td>
<td>STAMP</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

Safety Requirements and Constraints Traceability Matrix

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
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

• 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


