Safety Engineering

From SEBoK
Safety Engineering

Lead Author: Dick Fairley, Contributing Author: Alice Squires

In the most general sense, safety is freedom from harm. As an engineering discipline, system safety is concerned with minimizing hazards that can result in a mishap with an expected severity and with a predicted probability. These events can occur in elements of life-critical systems as well as other system elements. MIL-STD-882E defines system safety as “the application of engineering and management principles, criteria, and techniques to achieve acceptable risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle” (DoD 2012). MIL-STD-882E defines standard practices and methods to apply as engineering tools in the practice of system safety. These tools are applied to both hardware and software elements of the system in question.

Please note that not all of the generic below sections have mature content at this time. Anyone wishing to offer content suggestions should contact the SEBoK Editors in the usual ways.

Contents

- 1 Overview
- 2 System Description
- 3 Discipline Management
- 4 Discipline Relationships
  - 4.1 Interactions
  - 4.2 Dependencies
- 5 Discipline Standards
- 6 Personnel Considerations
- 7 Metrics
- 8 Models
- 9 Tools
- 10 References
  - 10.1 Works Cited
  - 10.2 Primary References
  - 10.3 Additional References

Overview

System safety engineering focuses on identifying hazards, their causal factors, and predicting the resultant severity and probability. The ultimate goal of the process is to reduce or eliminate the severity and probability of the identified hazards, and to minimize risk and severity where the
hazards cannot be eliminated. MIL STD 882E defines a hazard as "a real or potential condition that could lead to an unplanned event or series of events (i.e., mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment." (DoD 2012).

While systems safety engineering attempts to minimize safety issues throughout the planning and design of systems, mishaps do occur from combinations of unlikely hazards with minimal probabilities. As a result, safety engineering is often performed in reaction to adverse events after deployment. For example, many improvements in aircraft safety come about as a result of recommendations by the National Air Traffic Safety Board based on accident investigations. Risk is defined as "a combination of the severity of the mishap and the probability that the mishap will occur" (DoD 2012, 7). Failure to identify risks to safety and the according inability to address or "control" these risks can result in massive costs, both human and economic (Roland and Moriarty 1990).

**System Description**

Information to be supplied at a later date.

**Discipline Management**

Information to be supplied at a later date.

**Discipline Relationships**

**Interactions**

Information to be supplied at a later date.

**Dependencies**

Information to be supplied at a later date.

**Discipline Standards**

Information to be supplied at a later date.

**Personnel Considerations**

System Safety specialists are typically responsible for ensuring system safety. Air Force Instruction (AFI) provides the following guidance:

9.1. System safety disciplines apply engineering and management principles, criteria, and techniques throughout the life cycle of a system within the constraints of operational effectiveness, schedule, and costs.

9.1.1. System safety is an inherent element of system design and is essential to supporting system requirements. Successful system safety efforts depend on clearly defined safety objectives and system requirements.
9.1.2. System safety must be a planned, integrated, comprehensive effort employing both engineering and management resources.

(USAF 1998, 91-202)

Safety personnel are responsible for the integration of system safety requirements, principles, procedures, and processes into the program and into lower system design levels to ensure a safe and effective interface. Two common mechanisms are the Safety Working Group (SWG) and the Management Safety Review Board (MSRB). The SWG enables safety personnel from all integrated product teams (IPTs) to evaluate, coordinate, and implement a safety approach that is integrated at the system level in accordance with MIL-STD-882E (DoD 2012). Increasingly, safety reviews are being recognized as an important risk management tool. The MSRB provides program level oversight and resolves safety related program issues across all IPTs. Table 1 provides additional information on safety.

Table 1. Safety Ontology. (SEBoK Original)

<table>
<thead>
<tr>
<th>Ontology Element Name</th>
<th>Ontology Element Attributes</th>
<th>Relationships to Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure modes</td>
<td>Manner of failure</td>
<td>Required attribute</td>
</tr>
<tr>
<td>Severity</td>
<td>Consequences of failure</td>
<td>Required attribute</td>
</tr>
<tr>
<td>Criticality</td>
<td>Impact of failure</td>
<td>Required attribute</td>
</tr>
<tr>
<td>Hazard Identification</td>
<td>Identification of potential failure modes</td>
<td>Required to determine failure modes</td>
</tr>
<tr>
<td>Risk</td>
<td>Probability of a failure occurring</td>
<td>Required attribute</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Measure to take corrective action</td>
<td>Necessary to determine criticality and severity</td>
</tr>
</tbody>
</table>

Table 1 indicates that achieving System safety involves a close tie between Safety Engineering and other specialty Systems Engineering disciplines such as Reliability and Maintainability Engineering.

System safety engineering focuses on identifying hazards, their causal factors, and predicting the resultant severity and probability. The ultimate goal of the process is to reduce or eliminate the severity and probability of the identified hazards, and to minimize risk and severity where the hazards cannot be eliminated. MIL STD 882E defines a hazard as "a real or potential condition that could lead to an unplanned event or series of events (i.e., mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment." (DoD 2012).

While systems safety engineering attempts to minimize safety issues throughout the planning and design of systems, mishaps do occur from combinations of unlikely hazards with minimal probabilities. As a result, safety engineering is often performed in reaction to adverse events after deployment. For example, many improvements in aircraft safety come about as a result of recommendations by the National Air Traffic Safety Board based on accident investigations. Risk is defined as "a combination of the severity of the mishap and the probability that the mishap will occur" (DoD 2012, 7). Failure to identify risks to safety, and the according inability to address or "control" these risks, can result in massive costs, both human and economic (Roland and Moriarty 1990).

Metrics

Information to be supplied at a later date.
Models

Information to be supplied at a later date.

Tools

Information to be supplied at a later date.

References

Works Cited


Primary References

None.

Additional References


