

# System Safety

---

## System Safety

The printable version is no longer supported and may have rendering errors. Please update your browser bookmarks and please use the default browser print function instead.

---

**Lead Author:** Dick Fairley, **Contributing Authors:** Art Pyster, 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.



## Contents

---

Overview

Personnel Considerations

References

Works Cited

Primary References

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 U.S. 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). 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)."

## **Personnel Considerations**

---

System Safety Specialists are typically responsible for ensuring system safety. Chapter 11 of Air Force Instruction (AFI) 191-202 (USAF 2020) is a lengthy exposition of the responsibilities of system safety specialists. AFI 191-202 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." The AFI identifies eight activities to achieve systems safety:

1. Documenting the system safety approach
2. Hazard identification and analysis over the system life cycle
3. Assessment of risk, expressed as severity and probability of consequences
4. Identification and assessment of potential risk mitigation measures
5. Implementation of measures to reduce risks to

acceptable levels

6. Verification of risk reduction
7. Acceptance of risks by appropriate authorities
8. Tracking of hazards and risks throughout the system life cycle

Although these activities are documented in an Air Force Instruction, they are actually quite generic and applicable to almost any system safety process.

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)

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

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

# References

---

## Works Cited

DoD. 2012. *Standard practice for System Safety*. Arlington, VA, USA: Department of Defense (DoD). MIL-STD 882E. Accessed April 2, 2021. Available at [http://everyspec.com/MIL-STD/MIL-STD-0800-0899/MIL-STD-882E\\_41682/](http://everyspec.com/MIL-STD/MIL-STD-0800-0899/MIL-STD-882E_41682/).

Roland, H.E. and B. Moriarty. 1990. *System Safety Engineering and Management*, 2nd Ed. Hoboken, NJ, USA: Wiley.

USAF. 2020. *The US Air Force Mishap Prevention Program*. Air Force Instruction 91-202. Washington, DC, USA: US Air Force. Accessed April 2, 2021. Available [https://static.e-publishing.af.mil/production/1/af\\_se/publication/afi91-202/afi91-202.pdf](https://static.e-publishing.af.mil/production/1/af_se/publication/afi91-202/afi91-202.pdf).

## Primary References

DoD. 2012. *Standard practice for System Safety*. Arlington, VA, USA: Department of Defense (DoD). MIL-STD 882E. Accessed April 2, 2021. Available at [http://everyspec.com/MIL-STD/MIL-STD-0800-0899/MIL-STD-882E\\_41682/](http://everyspec.com/MIL-STD/MIL-STD-0800-0899/MIL-STD-882E_41682/).

## Additional References

Bahr, N.J. 2015. *System Safety Engineering and Risk Assessment: A Practice Approach*, 2nd Ed. Boca Raton, FL, USA: CRC Press.

ISSS. 2015a. "System Safety Hazard Analysis Report." The International System Safety Society (ISSS). DI-SAFT-80101C. Accessed April 2, 2021. Available at [http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80101C\\_53803/](http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80101C_53803/).

ISSS. 2015b. "Safety Assessment Report." The International System Safety Society (ISSS). DI-SAFT-80102C. Accessed April 2, 2021. Available at [http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80102C\\_53802/](http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80102C_53802/). Accessed on April 2, 2021.

ISSS. 2015c. "Engineering Change Proposal System Safety Report." The International System Safety Society (ISSS). DI-SAFT-80103C. Accessed April 2, 2021.

Available at  
[http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80103C\\_52427/](http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80103C_52427/).

ISSS. 2015d. "Waiver or Deviation System Safety Report." The International System Safety Society (ISSS). DI-SAFT-80104C. Accessed April 2, 2021. Available at [http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80104C\\_53816/](http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80104C_53816/).

ISSS. 2015e. "System Safety Program Progress Report." The International System Safety Society (ISSS). DI-SAFT-80105C. Accessed April 2, 2021. Available at [http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80105C\\_53817/](http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80105C_53817/).

ISSS. 2015f. "Health Hazard Assessment Report." The International System Safety Society (ISSS). DI-SAFT-80106C. Accessed April 2, 2021. Available at [http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80106C\\_53814/](http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80106C_53814/).

ISSS. 2003. "Explosive Ordnance Disposal Data." The International System Safety Society (ISSS). DI-SAFT-80931B. Accessed April 2, 2021. Available at [http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80931B\\_15713/](http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-80931B_15713/). .

ISSS. 2015. "Explosive Hazard Classification Data." The International System Safety Society (ISSS). DI-SAFT-81299C. Accessed April 2, 2021. Available at [http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-81299C\\_53809/](http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-81299C_53809/).

ISSS. 2001. "System Safety Program Plan (SSPP)." The International System Safety Society (ISSS). DI-SAFT-81626. Accessed April 2, 2021. Available at [http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-81626\\_11514/](http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-81626_11514/).

ISSS. 2015. "Mishap Risk Assessment Report." The International System Safety Society (ISSS). DI-SAFT-81300B. Accessed April 2, 2021. Available at [http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-81300B\\_53813/](http://everyspec.com/DATA-ITEM-DESC-DIDs/DI-SAFT/DI-SAFT-81300B_53813/).

Joint Software System Safety Committee. 1999. *Software System Safety Handbook*. Accessed April 2, 2021. Available at: <https://www.acqnotes.com/Attachments/Joint-SW-Systems-Safety-Engineering-Handbook.pdf>.

Leveson, N.G. 2016 reprint edition. *Engineering a Safer*

*World: Systems Thinking Applied to Safety*. Cambridge, Mass: MIT Press. Accessed April 2, 2021. Available at <https://mitpress.mit.edu/books/engineering-safer-world>.

Leveson, N.G. 2012. "Complexity and safety." In *Complex Systems Design & Management*, ed. Omar Hammami, Daniel Krob, and Jean-Luc Voirin, 27-39. Springer, Berlin, Heidelberg. Accessed April 2, 2021. Available at [http://dx.doi.org/10.1007/978-3-642-25203-7\\_2](http://dx.doi.org/10.1007/978-3-642-25203-7_2).

NASA. 2004. *NASA Software Safety Guidebook*. Accessed April 2, 2021. Available at <https://standards.nasa.gov/standard/nasa/nasa-gb-871913>.

SAE. 1996. *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. ARP 4761. Warrendale, PA, USA: Society of Automotive Engineers. Accessed April 2, 2021. Available at: <https://www.sae.org/standards/content/arp4761/>.

SAE. 2010. *Guidelines for Development of Civil Aircraft and Systems*. ARP 4754. Warrendale, PA, USA: Society of Automotive Engineers. Accessed April 2, 2021. Available at <https://www.sae.org/standards/content/arp4754a/>.

---

< Previous Article | Parent Article | Next Article >

**SEBoK v. 2.10, released 06 May 2024**

---

Retrieved from

"[https://sandbox.sebokwiki.org/index.php?title=System\\_Safety&oldid=71655](https://sandbox.sebokwiki.org/index.php?title=System_Safety&oldid=71655)"

---

**This page was last edited on 2 May 2024, at 22:53.**