Safety Case Workshop

by Tom Pfitzer, Tom DeLong, Saralyn Dwyer, John Frost, Dave West
Huntsville, Alabama

In January 2013, a two-day Safety Case Workshop was conducted in Huntsville, Alabama under the sponsorship of the SAE International G-48 System Safety Committee and A-P-T Research, Inc. (APT). Attendees from industry, government and academia participated, with several making formal presentations on various safety methods. Industry focus is turning to international pursuits, which involve a broader understanding of different approaches to ensuring safety. The United States has typically used a process-based approach in managing system safety programs, but there is a current movement to use the evidence-based Safety Case approach to validate the safety of systems. At the conclusion of the workshop, participants reached the consensus view that the Safety Case approach merits being accepted among the best world-wide system safety practices.

Background

During the 2013 International System Safety Conference (ISSC), the SAE International G-48 System Safety Committee[1] accepted an action to investigate the utility of the Safety Case approach in relation to ANSI/GEIA-STD-0010-2009. The Safety Engineering and Analysis Center (SEAC) of A-P-T Research, Inc. (APT) offered to organize and host a workshop for that purpose. The SEAC was formed as a division of APT to support independent studies and risk assessments with special capabilities in safety. Leaders in the field were invited to present at the workshop, and a panel was selected. Moderated by John Frost, the panel's presenters included Dave West, SAIC; Don Swallom, U.S. Army Aviation and Missile Command (AMCOM); John McDermid, professor of software engineering at the University of York, U.K.; Barry Hendrix, Lockheed Martin; Dr. Homayoon Dezfuli, National Aeronautics and Space Administration (NASA); Robert Schmedake, Boeing; and Tom DeLong, APT. Representative members of industry, government and academia included AMCOM, APT, Boeing, NASA, Northrop Grumman, Missile Defense Agency (MDA), SAIC and the University of York.

Scope

The purpose of the workshop was to identify the best relative approach to benefit the system safety discipline and make a recommendation to the G-48 Committee in an effort to define the best practices of system safety. The approaches reviewed and the findings of each are summarized here.

Safety Cases: Purpose, Process and Prospects

The basic concepts and processes of the Safety Case approach were presented by John McDermid, University of York, U.K. In Ministry of Defence (MoD) practice, a Safety Case is defined as a structured argument supported by claims of why the system is adequately safe. The claims may initially be unfounded; during the course of the safety program, evidence is gathered to confirm

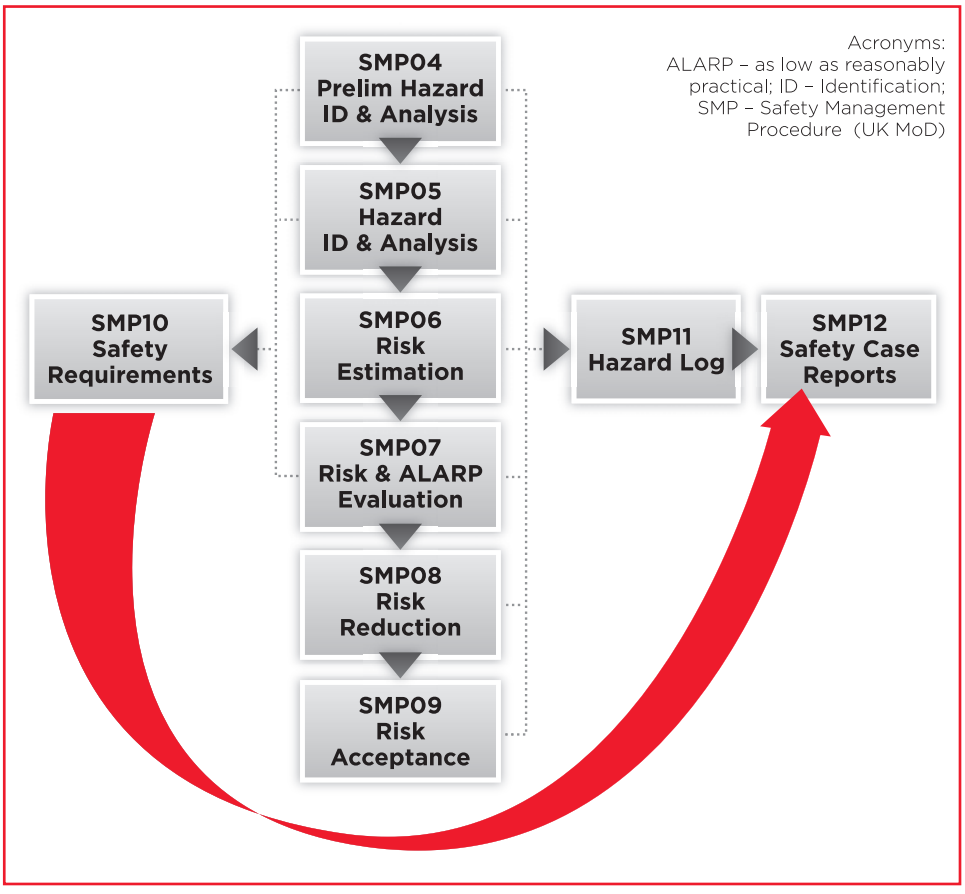

Figure 1 — Role of (Final) Safety Case.

[1] The charter of the G-48 Committee includes establishing national best practices in system safety.

or deny the claims. The focus of the program is on gathering evidence, which consists of analyses and data which correlate with the tasks in the ANSI/GEIA Standard and the MIL Standard. As shown in Figure 1, which reflects U.K. MoD practice, the final safety case offers evidence, which provides a comprehensive and compelling case that a system is safe to operate in a given scenario. Because these arguments are defined at the beginning of a program, they establish safety requirements that need evidentiary support to eventually conclude that the system is adequately safe. These claims and the supporting evidence must be independently reviewed prior to the risk acceptance decision.

Other Approaches Presented for Comparison

The ANSI/GEIA Process for System Safety Assurance

The background and principles of the ANSI/GEIA Standard (ANSI/GEIA-STD-0010-2009) developed by the G-48 were presented by Dave West, SAIC. The primary focus of this document is to simplify work elements and process flow, modernize the risk assessment matrix and introduce risk summing. The basic elements of an effective system safety program defined by the ANSI/GEIA Standard are shown in Figure 2.

The MIL-STD-882 Process

The principles of MIL-STD-882E were presented by Don Swallom, AMCOM Safety. The basic elements of the standard were presented, as was background information on the standard. The basic elements of an effective system safety program, defined by MIL-STD-882E, are shown in Figure 3.

SAE ARP 4761 Process

The SAE ARP 4761, SAE ARP 4754, IEEE STD 1228 and DO-178 process was presented by Barry Hendrix, Lockheed Martin. These documents focus on complex aircraft systems and the development of safety assessments that lead to certifications. The basic products include a Functional Hazard Assessment (FHA), a Preliminary System Safety Assessment (PSSA) and a System Safety Assessment (SSA). Residual risk is not part of the Aerospace Recommended Practice (ARP) process, as requirements must be met with few exceptions. The safety processes associated with aircraft systems are summarized in Figure 4.

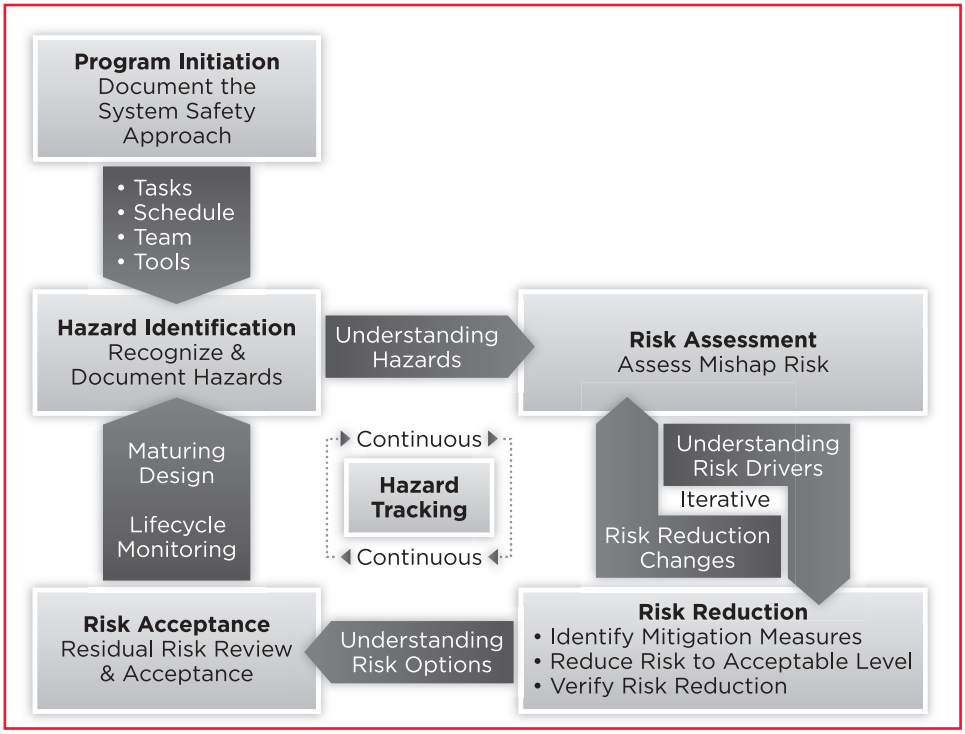

Figure 2 — ANSI/GEIA-STD-0010-2009 System Safety Approach.

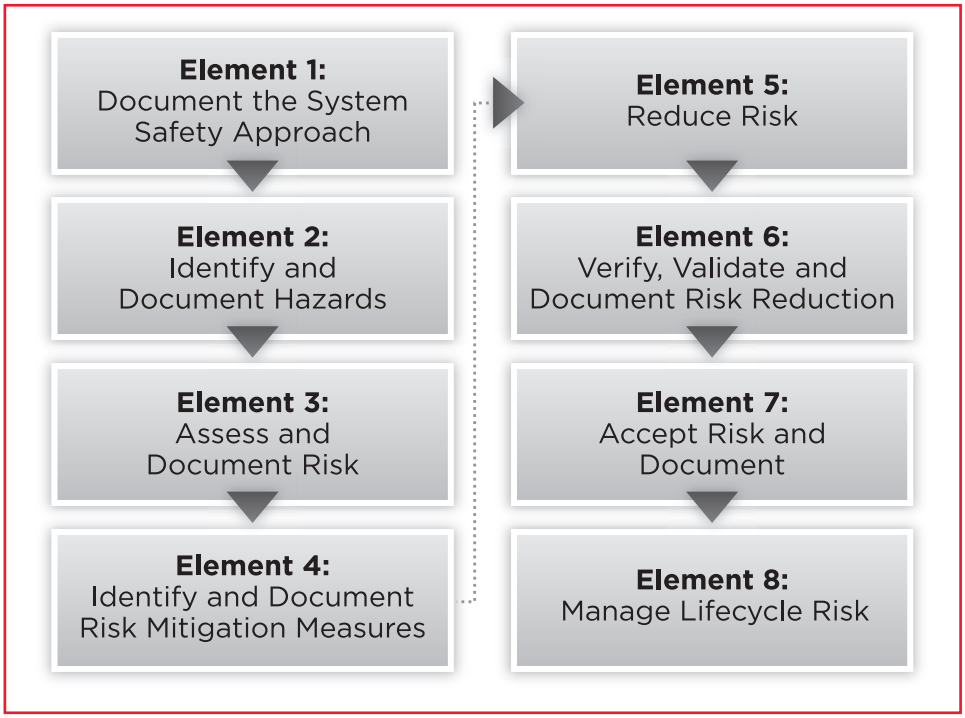

Figure 3 — MIL-STD-882E System Safety Approach.

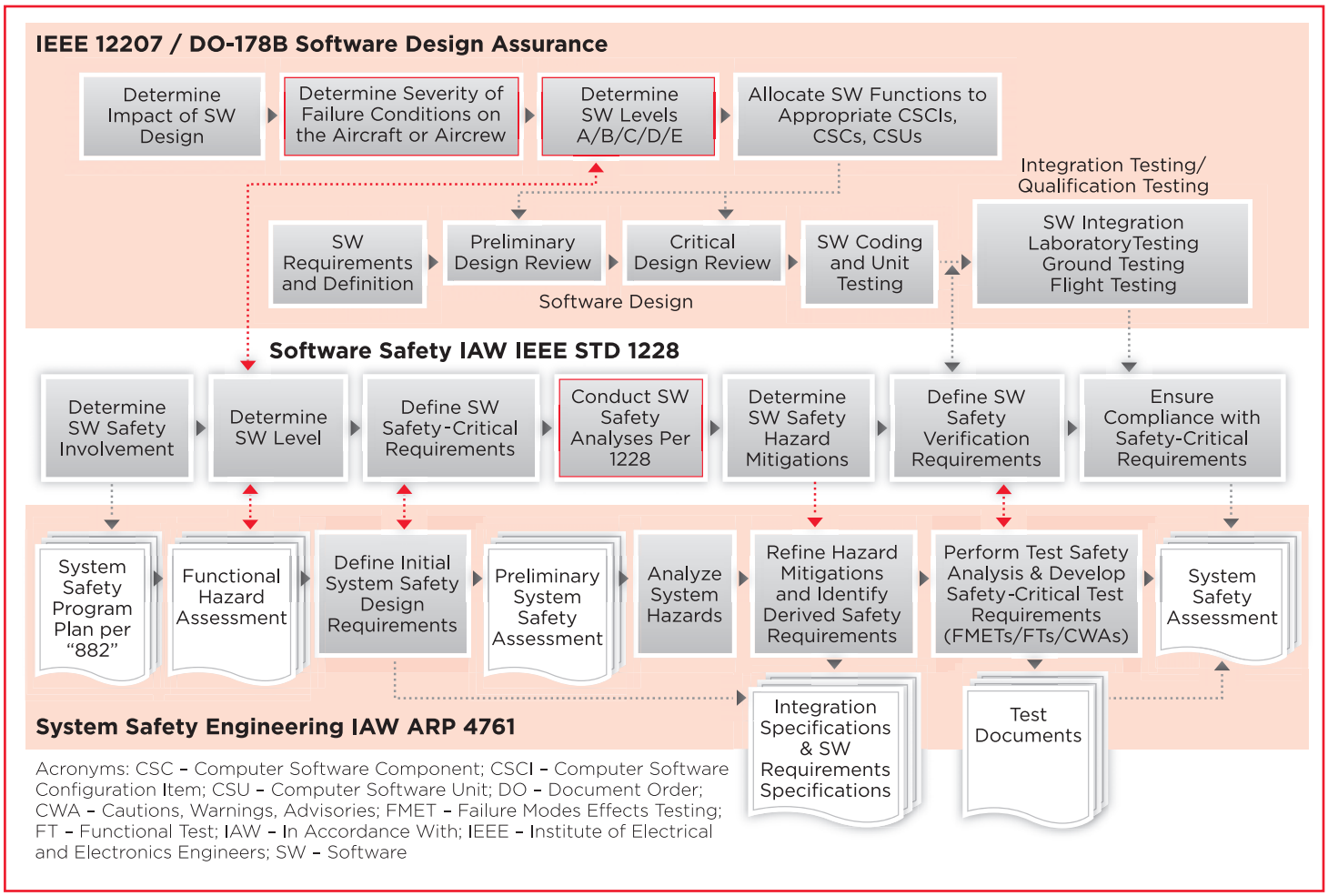

Figure 4 — Top-Level System Safety Process Used by ARP.

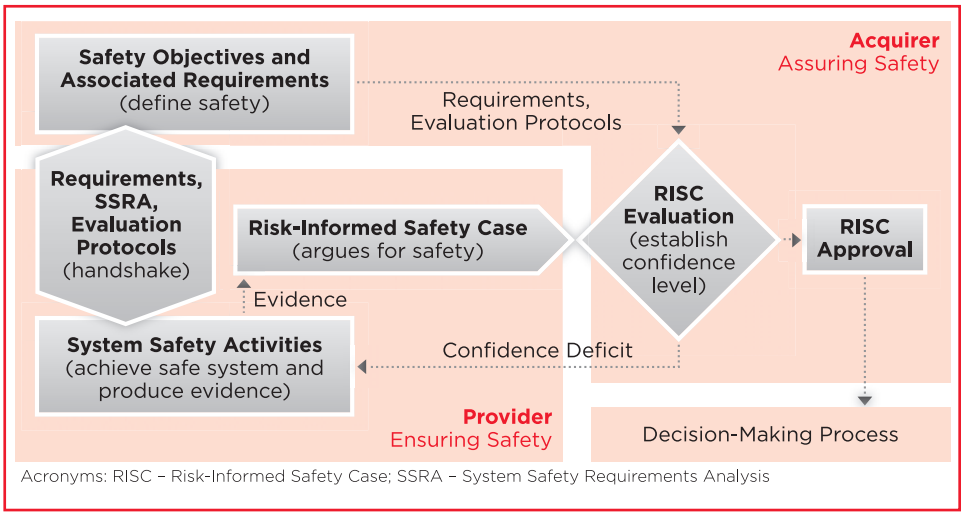

Figure 5 — NASA System Safety Framework.

Application of Safety Case at NASA

Dr. Homayoon Dezfuli presented the NASA evolution of system safety and risk management, as well as the current thinking regarding system safety. The NASA system safety framework, documented in NASA/SP-2010-580, is shown in Figure 5.

Of note was a concept of how to account for Unknown/Underappreciated (UU) risks. NASA recognized the need to consider the gap between the known risk and actual risk when applying safety thresholds and goals. The concept of safety performance margin is used to account for UU risks. This provides a rational basis for deriving verifiable requirements on known risks.

Safety Case and Software Development

Robert Schmedake, Boeing, discussed the Safety Case approach and how it can be used in software development. The current methods in the standards are not bad; however, there is room for improvement where software is concerned. The advantages of using the Safety Case approach include defining explicit claims for the safety design up front, giving safety claims to build an argument and providing evidence (analysis, inspection, demonstrations and tests) to support claims. The disadvantages include: a system-domain requirement for

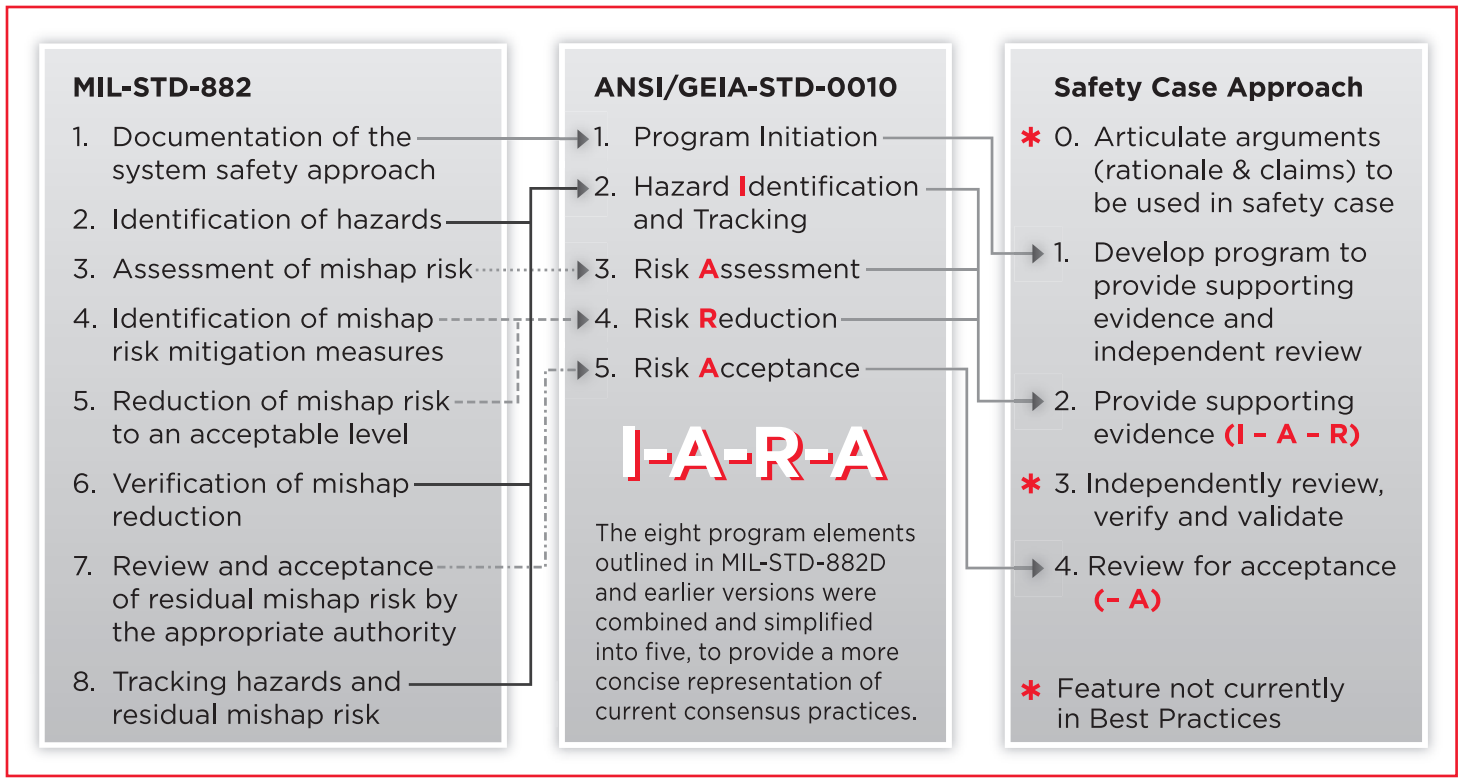

Figure 6 — Mapping Between Standard Approaches — Traceability Has Been Defined Between ANSI/GEIA-STD, MIL-STD and Safety Case Approach.

expertise of the developed system. Also, re-use of prior analysis can be problematic since the original case is specific to the original system context.

Comparison of Methods

Tom DeLong, APT, summarized the various methods and led a group discussion on each. It was noted that in the U.S., NASA and the FAA are moving toward the Safety Case approach.

In the U.S., the safety assessment report (SAR) comes closest to the Safety Case approach; however, a Safety Case is broader in scope than the SAR. A Safety Case is a structured argument, supported by evidence, which provides a comprehensive and compelling case that a system is safe to operate in a given scenario. When compared to the SAR, the biggest difference is the use of arguments and associated evidence to justify them.

When looking at U.S. Army systems, safety processes that seem to be working best include fuzes, rocket motor ignition systems, insensitive munitions and similar items with the following common characteristics: detailed requirements that are included in contracts, well-defined processes to meet the requirements and demonstrate compliance, and a designated group of experts to validate compliance. The safety case approach can also provide the same benefits for a broader set of domains.

The Safety Case approach is a structured way of showing the work done on a safety program and highlights the importance of an independent evaluation group. By defining arguments at the beginning of a program, safety becomes the advocate rather than the protagonist. This approach could change the profession in profound ways by using a positive, front-loaded approach.

Findings

Comparison of existing ANSI/GEIA-STD-0010 and MIL-STD-882 techniques found that the Safety Case approach includes the most critical elements of these techniques, as mapped in Figure 6. Strengths found in the Safety Case approach that are not included in the U.S. approaches include a beginning step that articulates the rationale, or requirements, to be used and an independent review of the safety approach.

A significant portion of the workshop was dedicated to investigating the strength of the Safety Case. It was noteworthy that with more than 1,000 person-years of safety experience in the room, there were few negative responses and a great many positives. The highlight of the second day of the workshop was reaching consensus on these strengths and observations, as shown in Table 1. The structured, evidence-based approach to satisfying the safety arguments established at the start of the program offers benefits that were not included in other techniques. The consensus of the workshop is summarized in Table 1.

Table 1 — Strengths and Observations Concerning the Safety Case Approach.

Strengths	Observations
1. Includes clear, early definition of most compelling issues	Not included in ANSI/GEIA or 882
2. Burden of proof is on the provider	
3. Provides a baseline (normalcy map) for safety of the system	
4. Explicit argument tying objective and robust evidence to support proof of claim	
5. Essential narrative communicates effectively to decision makers, risk takers and other stakeholders	
6. Requires robust evidence to support key decisions (e.g., to operate systems)	
7. Explicitly addresses the needs of the decision maker in deciding whether to accept a system, permit a system to proceed to the next phase of development or go to operation	
8. The approach is highly tailorable to fit the need for evidence and the complexity of the system	All safety processes are tailorable; however, this approach seems to be more so because the arguments are unique to the decision
9. Inclusion of independence in review of the case (claims, arguments)	Not included in ANSI/GEIA or 882
10. Evidence and independent review can aid in risk acceptance phase	Review panels or experts will develop consistent rules
11. Encourages multiple approaches to capture evidence/ facts vs. assumptions	Existing SARs may not include all supporting evidence
12. Promotes a comprehensive assessment of the positive safety aspects of a design but does not overlook negative aspects of the design	Fills potential gaps in 882
13. Facilitates incorporation of methods, processes and tools from all existing sources	Freedom for broad tailoring
14. Enables development of risk acceptance criteria in context of overall system risk	Enables focus on overall system level risk and does not mandate individual hazard risk assessment code
15. Visibility of progress toward achieving and demonstrating safety objectives	Serves as a road map for the program manager
16. Derived safety requirements from the statement of the arguments and hazard analysis can be put into systems engineering earlier than is currently being done	
17. Earlier visibility of shortcomings (e.g., gaps in evidence) and understanding significance	
18. International standardization of safety methodology	Saves costs on multi-national programs
19. Facilitates a holistic view of complex systems, acknowledging that safety is an emergent property	
20. Supports legal defense	List of hazards can impede legal defense
21. Encourages system safety approach to become more evidence-based as opposed to product-or process-driven	
22. Is compatible with and unifies otherwise potentially fragmented system safety processes and approaches	
23. Encourages systematic attempt to identify where claims may not be satisfied	
	This method requires expertise in the system domain of the developed system
	Requires up-front work and may make reuse of prior analysis problematic
	Requires training and implementation strategies
	Requires extensive oversight by qualified practitioners

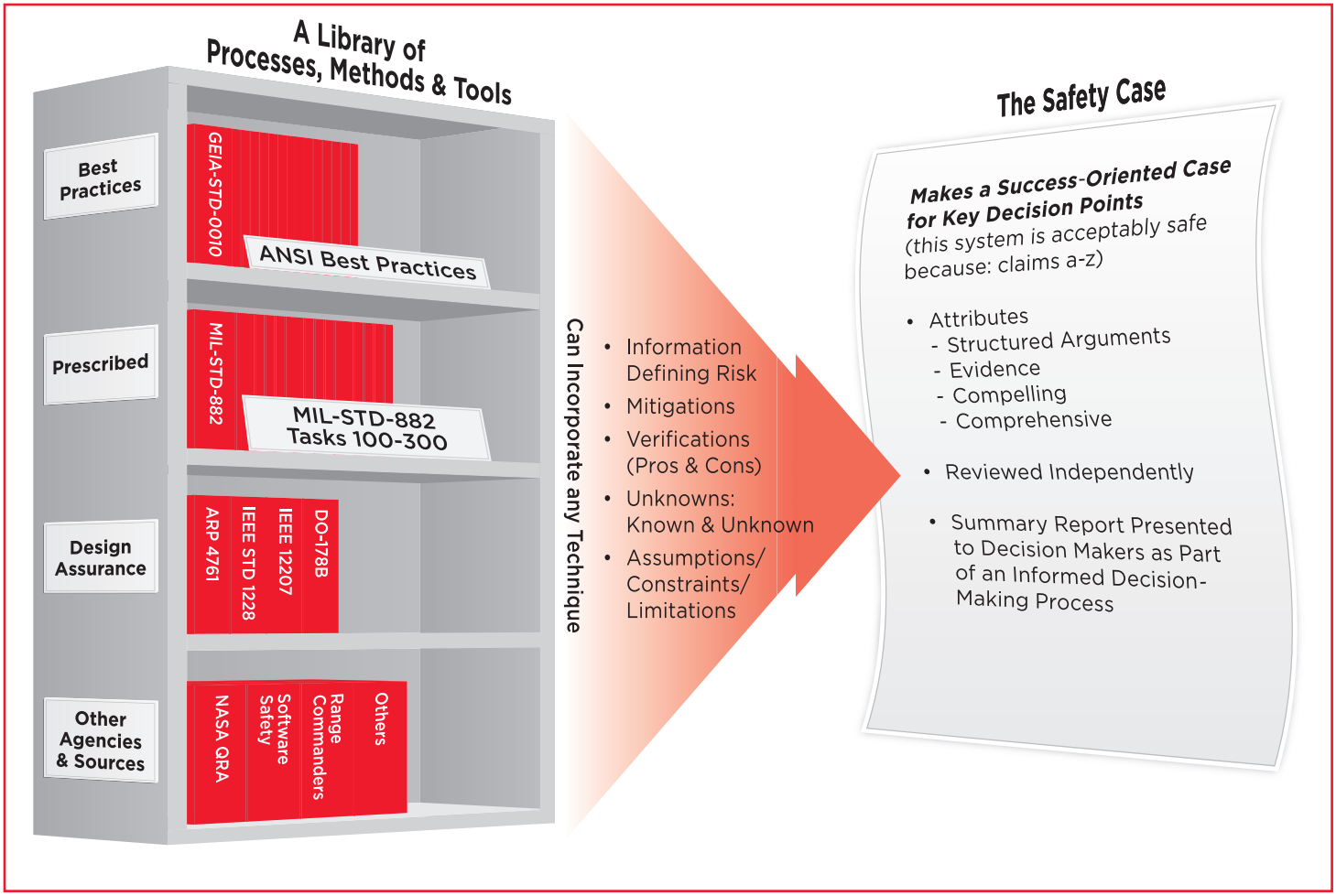

Figure 7 — What is the Safety Case? An Evidence-Based Approach.

A concept of what should be included in the Safety Case approach was developed, as shown in Figure 7. Ideally, a Safety Case makes success-oriented claims that, when combined, form the safety argument. After evidence is developed, the claims and evidence are reviewed independently, leading to risk-informed decisions.

Recommendations Presented to the G-48

The workshop recommended that the G-48 Committee take steps to fully embrace the Safety Case approach as a recognized "best practice." It is also noted that multiple U.S. organizations, including NASA, major aerospace companies and the Chemical Safety Board, are already embracing the Safety Case approach.

Further, the workshop recommends that key features of the Safety Case approach be incorporated into existing approaches documented in ANSI/GEIA-STD-0010. These features include:

- Early identification of arguments required to demonstrate that a system is adequately safe
- Development of compelling and comprehensive evidence to underpin the claims of safety
- Independent review by qualified experts prior to risk acceptance decisions
- Incorporation of evidence that the claims have been substantiated in safety assessments of the system

Actions Taken by the G-48 Committee

On the following day, January 16, the SAE International G-48 System Safety Committee convened a meeting, which included review of the previously outlined strengths and recommendations. During that meeting, the G-48 Committee endorsed the recommendations of the workshop and defined actions that would ultimately incorporate the Safety Case approach into documented "Best Practices." The actions assigned included developing a workshop paper documenting the findings of the group, developing a track/panel on this approach for the International System Safety Conference (ISSC), and planning the path forward for including the Safety Case approach in a future version of ANSI/GEIA-STD-0010-2009.

Conclusion

For more than 40 years, the process-based approach has been used within the U.S. to manage system safety pro-

grams. These include the eight-step MIL-STD process and the IARA process used in the ANSI/GEIA Standard. During the past 15 years, a growing number of advocates have been using the evidence-based Safety Case approach to validate the safety of systems. A review and comparison of the methods show that the Safety Case approach includes strengths not found in the process-based approach. Therefore, it is concluded that the Safety Case approach has merits worthy of being accepted among the best world-wide system safety practices.

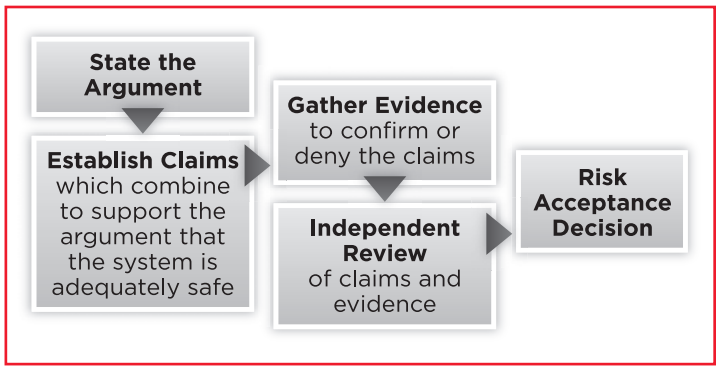

Figure 8 — Safety Case Process.

About the Contributors

John Frost, moderator, is a current NASA Aerospace Safety Advisory Panel member who owns a successful safety consulting company. He is a Senior member of the International System Safety Society (ISSS), a professional member of the American Society of Safety Engineers and active in various system safety organizations and initiatives, including G-48. He is the former chief of safety for U.S. Army AMCOM, chaired the Army's Ignition Safety Review Board and served as an Army Explosive Hazard Classification authority.

John McDermid, OBE FREng, is professor of software engineering at the University of York, U.K. and was head of the Computer Science Department from 2006 to 2012. He set up the High Integrity Systems Engineering research group, and was instrumental in developing techniques for producing safety arguments and safety cases that are now used worldwide. He is a Fellow of the Royal Academy of Engineering, and an Officer of the Order of the British Empire (OBE).

The Safety Case Workshop — Standing, left to right: Stephanie Wacenske, MDA; Tracy Conklin, Cargo Safety; Jim Gregoire, Northrop Grumman; Melissa Emery, A-P-T Research, Inc.; Ray Applebaum, A-P-T Research, Inc.; Willie Fitzpatrick, RDECOM, AMRDEC; Terrell Swindall, AMCOM Safety; Bob Youngblood, Idaho National Labs; Jason Kirkpatrick, PM UAS; Saralyn Dwyer, A-P-T Research, Inc.; Homayoon Dezfuli, NASA.
Seated, left to right: Tom DeLong, A-P-T Research, Inc.; Don Swallom, AMCOM; John McDermid, University of York; Tom Pfitzer, A-P-T Research, Inc.; John Frost, Moderator; Dave West, SAIC; Robert Schmedake, Boeing; Barry Hendrix, Northrop Grumman.

Dave West, CSP, PE, CHMM, Fellow, is senior director and chief safety engineer of a 1,000-employee operation of SAIC, and is current chairman of the SAE International G-48 System Safety Committee. He is a former president of the ISSS Tennessee Valley Chapter, and has more than 25 years of experience performing safety work for Army aviation and weapon systems, chemical demilitarization, spaceflight programs, chemical plants, and nuclear facilities.

Don Swallom is a safety engineer for the U.S. Army AMCOM and a Fellow member of ISSS. He is a former president of the Tennessee Valley Chapter, former pilot, staff officer and developmental engineer in the U.S. Air Force, and former chief of safety for the Arnold Engineering Development Center.

Barry Hendrix is a Lockheed Martin Technical Fellow Emeritus for aviation safety and airworthiness and has more than 40 years of experience on various weapon systems. He is the IBCS System Safety Lead for Northrop Grumman and served 10 years in the U.S. Navy aboard aircraft carriers as an aviation fire control system specialist on fighter and attack aircraft.

Homayoon Dezfuli, Ph.D., is a NASA system safety technical fellow and the manager of system safety in the Office of Safety and Mission Assurance at NASA Headquarters. He led development of and co-authored several NASA procedures guides and handbooks, devised a safety goal implementation framework that has helped shape the NASA safety goal policy for human space flight, and is leading the development of the NASA System Safety and Mission Success Standard.

Robert Schmedake is a Boeing Technical Fellow, with more than 25 years of experience in system safety engineering. He is a Fellow member and current president of the ISSS, secretary of the G-48, U.S. co-chair of the S5000F Committee and a member of the joint Aerospace Industries of America & Aerospace and Defense Industries of Europe Integrated Logistic Support Specification Council. He served in the U.S. military from 1986 to 2012.

Tom Delong is the former lead systems safety engineer for SMDC, and has more than 35 years of safety experience. He chaired several missile anomaly investigations during a LAW alternative source selection and managed SETA contract and Range Safety Analysis contract at SMDC. He is lead instructor for APT's system safety training program, which provides instruction to more than 100 professionals annually.

References*

1. McDermid, John. "Safety Cases: Purpose, Process and Prospects," Safety Case Workshop, January 14-15, 2014.
2. West, Dave. "The 'ANSI' Process for System Safety Assurance," Safety Case Workshop, January 14-15, 2014.
3. ANSI/GEIA-STD-0010-2009, "Standard Best Practices for System Safety Program Development and Execution," February 12, 2009.
4. Swallom, Don. "The MIL-STD Process," Safety Case Workshop, January 14-15, 2014.
5. MIL-STD-882E, "Department of Defense Standard Practice System Safety," May 11, 2012.
6. Hendrix, Barry. "SAE ARP 4761 Process," Safety Case Workshop, January 14-15, 2014.
7. SAE ARP 4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," December 1, 1996.
8. IEEE 12207, "Standard for Information Technology – Software Life Cycle Processes," May 1998.
9. DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," December 1, 1992.
10. IEEE STD 1228. "IEEE Standard for Software Safety Plans," March 17, 1994.
11. Dezfuli, Homayoon. "Application of 'Safety Case' at NASA," Safety Case Workshop, January 14-15, 2014.
12. Schmedake, Robert. "Safety Case and Software Development," Safety Case Workshop, January 14-15, 2014.
13. Delong, Tom. "Define & Compare Flowcharts of Each Method," Safety Case Workshop, January 14-15, 2014.

* Briefing available online at www.apt research.com/news/newsBlog2014.html#SafetyCase