Safety Case Workshop

by Tom Pfitzer, Tom DeLong, Saralyn Dwyer, A-P-T Research, Inc.
John Frost, Safety Engineering Services
Dave West, SAIC, SAE International G-48 Chair

Abstract
In January 2013, a two-day Safety Case Workshop was conducted in Huntsville, AL under 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 the 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. There is a current movement to use the evidence-based Safety Case approach to validate safety of systems. At the conclusion of the workshop, participants reached the consensus view that the Safety Case approach has merits worthy of being accepted among the best world-wide system safety practices.

Background
At the 2013 International System Safety Conference (ISSC), the SAE International G-48 System Safety Committee[*] accepted an action to investigate the utility of the Safety Case approach vis-à-vis ANSI/GEIA-STD-0010-2009. The Safety Engineering and Analysis Center (SEAC) of A-P-T Research, Inc. 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, led by Moderator, John Frost. Panel 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, UK; Barry Hendrix, Lockheed Martin; Dr. Homayoon Dezfuli, National Aeronautics and Space Administration (NASA); Robert Schmedake, Boeing; and Tom DeLong, APT. Members of Industry, Government, and Academia were represented to include AMCOM, APT, Boeing, NASA, Northrop Grumman, Missile Defense Agency (MDA), SAIC, and the University of York.

Scope
The scope 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 a continuation to define the best practices of system safety. Approaches reviewed and the findings of each are summarized below.

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

Safety Cases: Purpose, Process, and Prospects

The basic concepts and processes of the Safety Case approach were briefed by John McDermid, University of York, UK. 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 be initially unfounded and during the course of the safety program, evidence is gathered to confirm or deny the claims. The focus of the program is on gathering evidence. This evidence 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 UK 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 which 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.

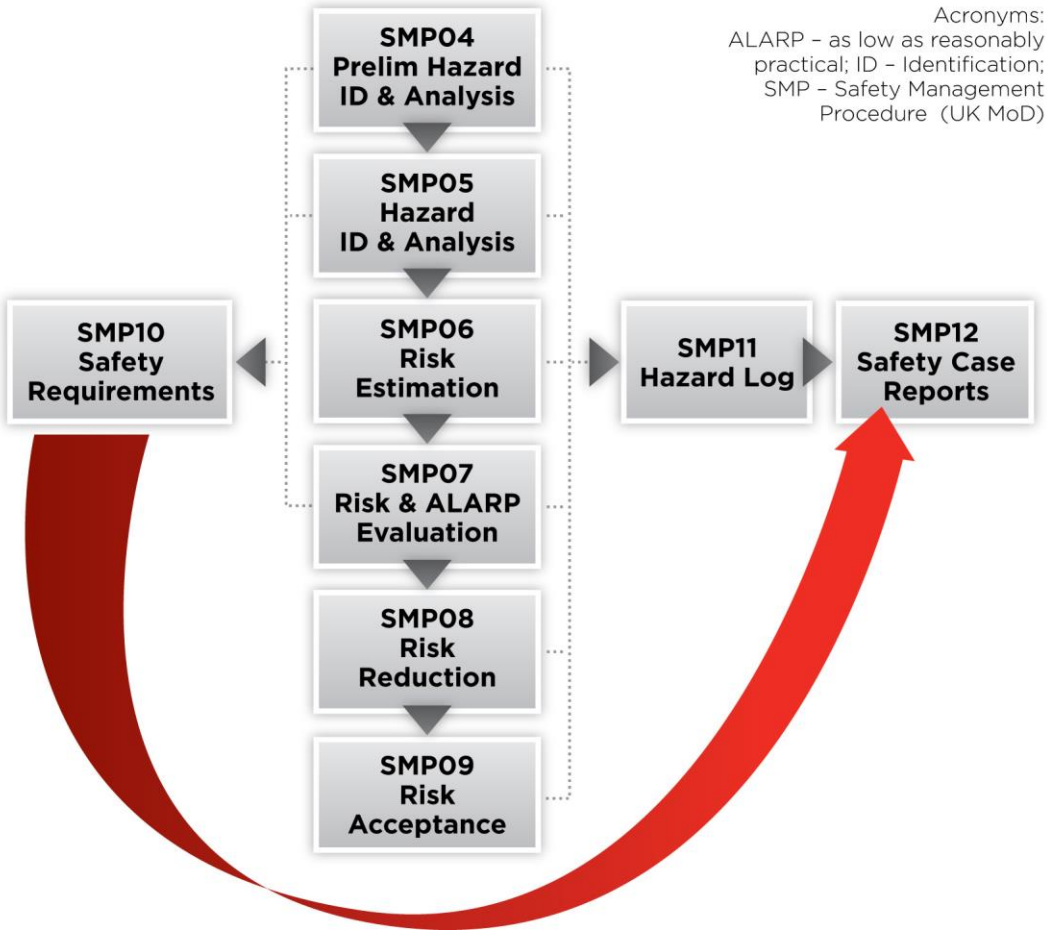

Figure 1 — Role of (Final) Safety Case

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 was 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.

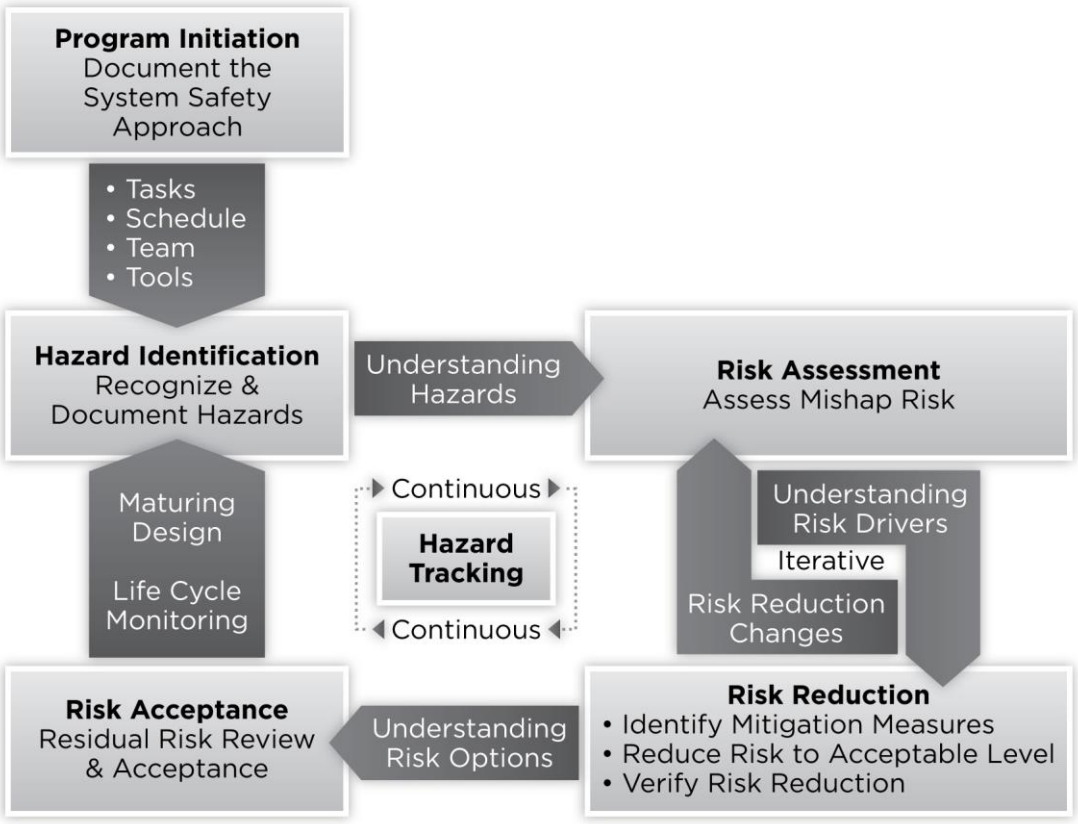

Figure 2 — ANSI/GEIA-STD-0010-2009 System Safety Approach

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 briefed, as well as background information on the standard. The basic elements of an effective system safety program defined by MIL-STD-882E are shown in Figure 3.

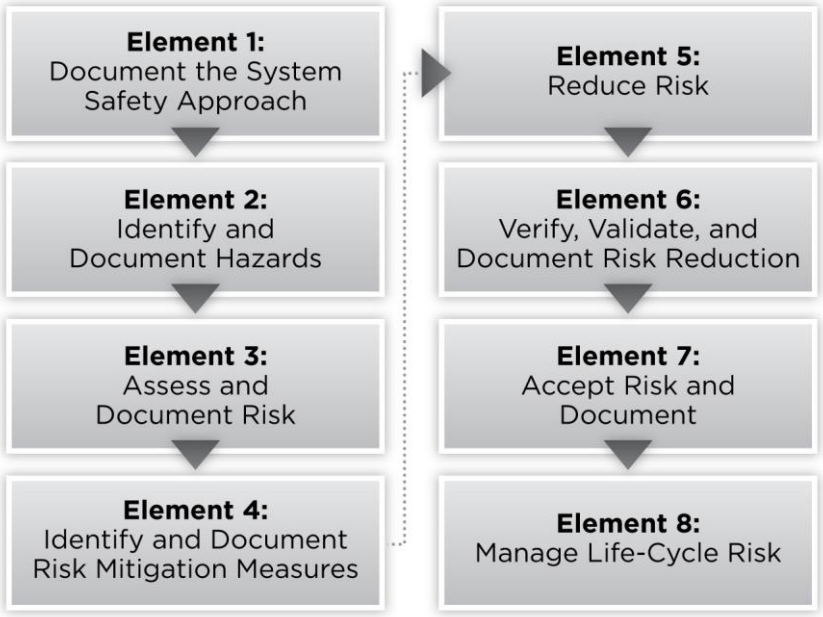

Figure 3 — MIL-STD-882E System Safety Approach

SAE ARP 4761 Process

The SAE ARP 4761, SAE ARP 4754, IEEE STD 1228, and DO-178 process was briefed 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 ARP process as requirements must be met with few exceptions. The safety processes associated with aircraft systems are summarized in Figure 4.

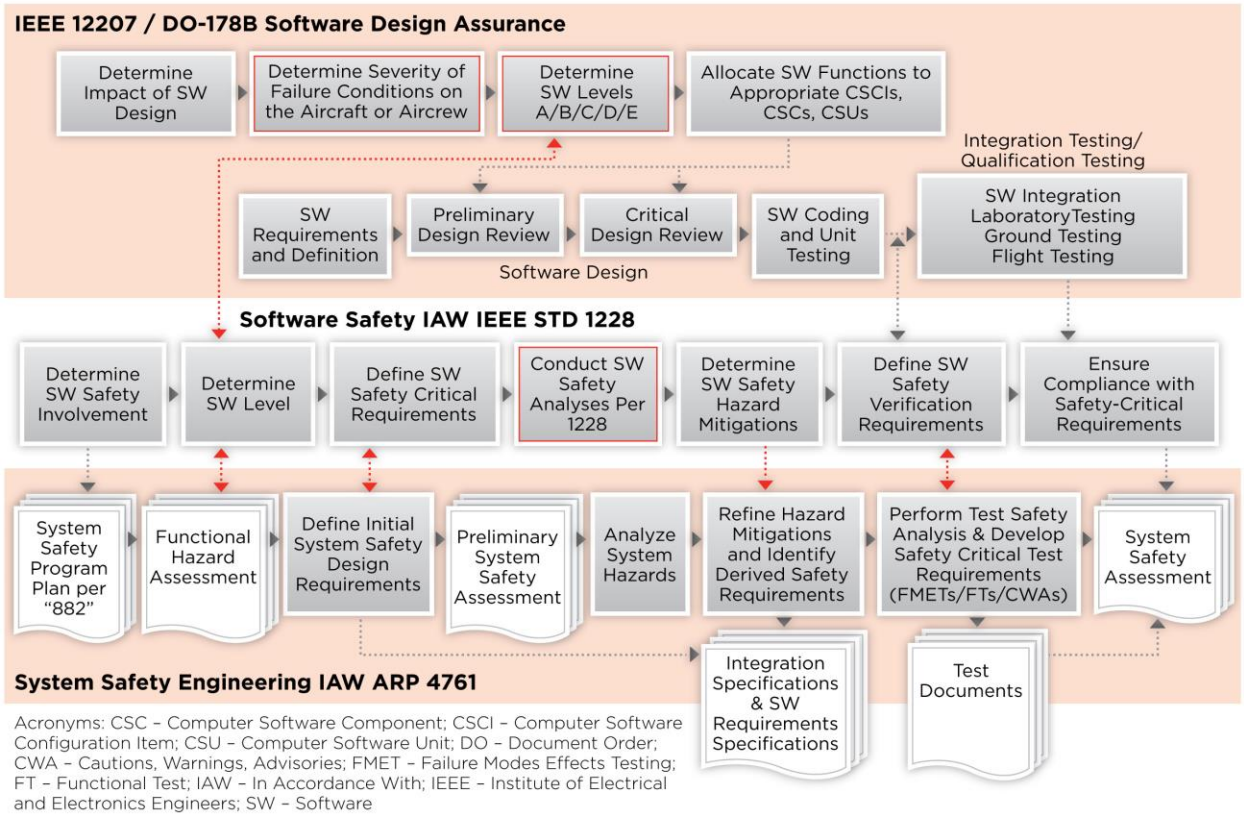

Figure 4 — Top Level System Safety Process used by ARP

Application of "Safety Case" at NASA

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

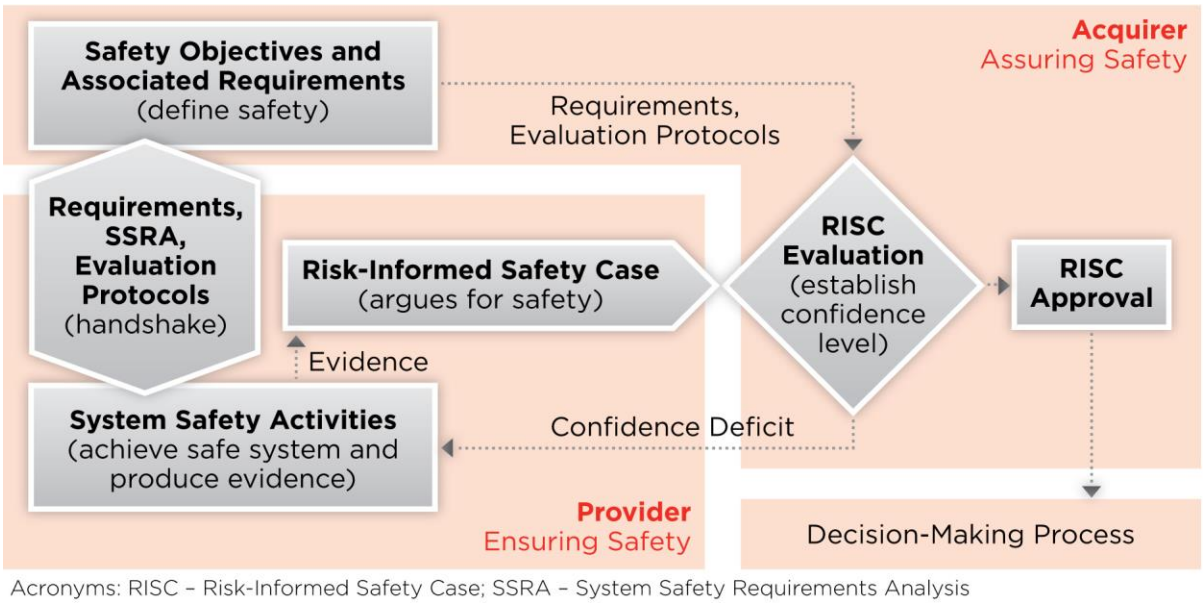

Figure 5 — NASA System Safety Framework

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

The Safety Case approach and how it can be used in software development was discussed by Robert Schmedake, Boeing. 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 the claim. The disadvantages include: the requirement for expertise in the system domain of the developed system. Also, it can make the reuse of prior analysis problematic since the original case would be 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 United States, 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 a 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 these characteristics: rather complete requirements which 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 provide the same benefits for a broader set of domains.

The Safety Case approach is a structured way of showing the work done on the safety program and highlights the importance of an independent evaluation group.

By defining arguments at the beginning of a program, safety could become the advocate rather than the protagonist. This approach could change the profession in profound ways by providing 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 approaches, as mapped by Figure 6. Strengths found in the Safety Case approach which are not included in the U.S. approaches include a beginning step to articulate the rationale, or requirements, to be used and an independent review of the safety approach.

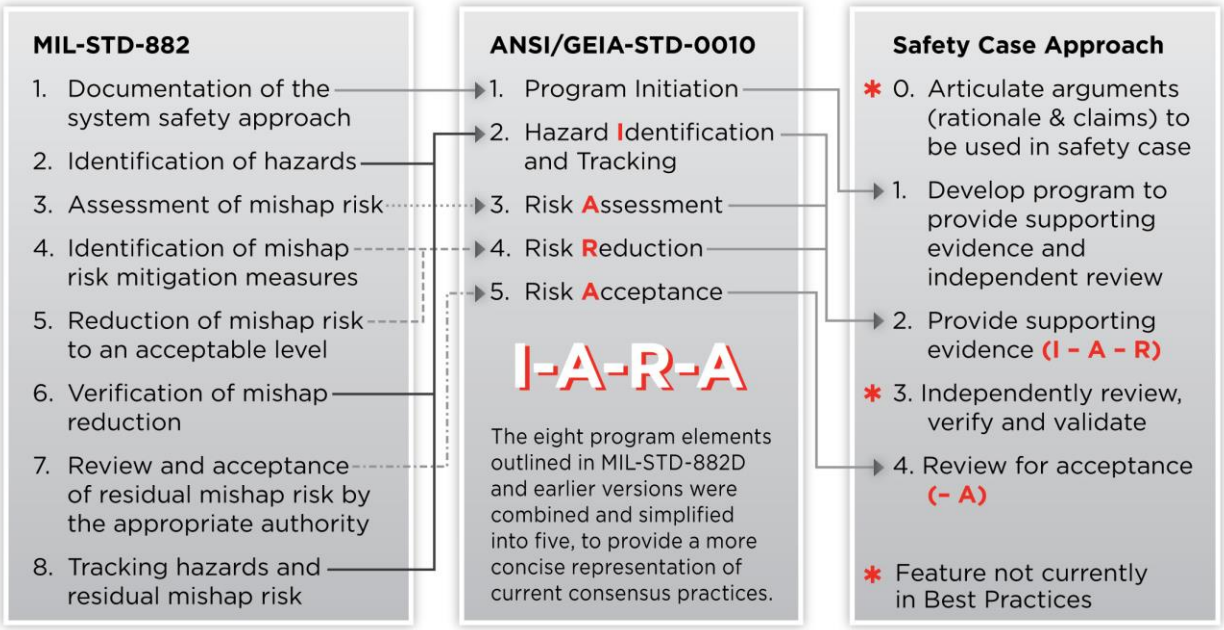

Figure 6 — Mapping Between Standard Approaches

Traceability has been defined between ANSI/GEIA-STD, MIL-STD, and Safety Case Approach.

A significant portion of the workshop was dedicated to investigating the strength of the Safety Case. It was noteworthy that with over 1,000 person-years of safety experience in the room, there were very few negatives 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 the table

below. 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, to risk takers, and to other stakeholders	
6. Requires robust evidence to support key decisions (e.g., to operate systems)	
7. Explicitly addresses the needs of the decision maker deciding whether to accept a system/permit a system to proceed to the next phase of development, or going 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 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 the negative aspect 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 roadmap 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	Save costs on multi-national programs
19. Facilitates a holistic view of complex systems knowing that safety is an emergent property	

Strengths	Observations
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	
24.	This method requires expertise in the system domain of the developed system
25.	Requires up front work and may make reuse of prior analysis problematic
26.	Requires training and implementation strategies
27.	Requires oversight (extensive) by qualified practitioners

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 which combine into the safety argument. After evidence is developed, the claims and evidence are reviewed independently leading to risk informed decisions.

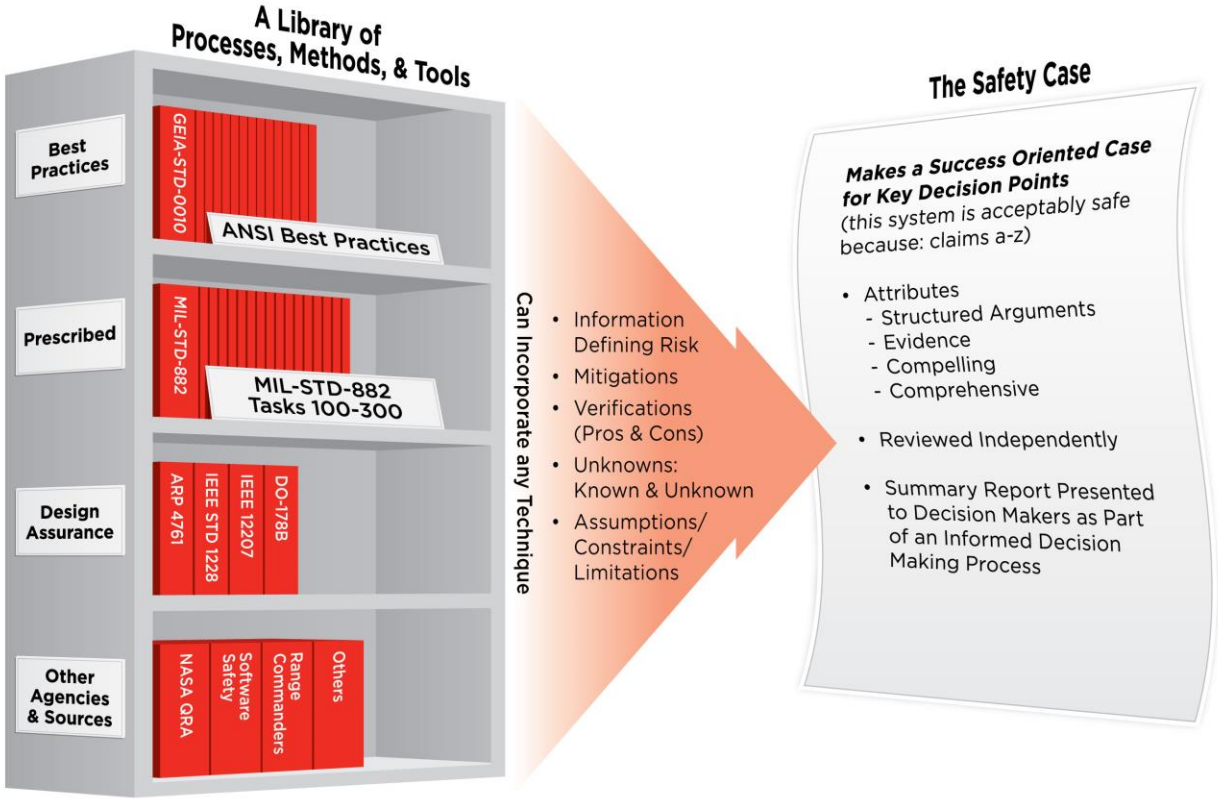

Figure 7 — What is the Safety Case ~ An Evidence Based Approach

Recommendations Presented to the G-48

The workshop recommends that the G-48 Committee take steps to fully embrace the Safety Case approach as a recognized "best practice." It is also notes 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 expertise prior to risk acceptance decisions.
- Incorporation of the evidence that the claims have been substantiated in safety assessments of the system.

Actions Taken by the G-48 Committee

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

Conclusions

For over 40 years, the process-based approach has been used within the U.S. to manage system safety programs. These include the eight-step MIL-STD process and the IARA process used in the ANSI/GEIA Standard. During the last 15 years, a growing number of advocates have been using the evidence-based Safety Case approach to validate safety of systems. A review and comparison of the methods show that the Safety Case approach includes strengths not included 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

“You haven’t heard the end of this, just the beginning.”

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

References

1. John McDermid, OBE FREng, “Safety Cases: Purpose, Process and Prospects.”†
2. Dave West, CSP, P.E., CHMM, Fellow, “The ‘ANSI’ Process for System Safety Assurance.”†
3. ANSI/GEIA-STD-0010-2009, “Standard Best Practices for System Safety Program Development and Execution,” 12 February 2009.
4. Don Swallom, “The MIL-STD Process.”†
5. MIL-STD-882E, “Department of Defense Standard Practice System Safety,” 11 May 2012.

† Safety Case Workshop, 14-15 January 2014.
Briefing available online at www.apt-research.com/news/newsBlog2014.html#SafetyCase

6. Barry Hendrix, “SAE ARP 4761 Process.”†
7. SAE ARP 4761, “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,” 1 December 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,” 1 December 1992.
10. IEEE STD 1228, “IEEE Standard for Software Safety Plans,” 17 March 1994.
11. Homayoon Dezfuli, Ph.D., “Application of ‘Safety Case’ at NASA.”†
12. Robert Schmedake, “Safety Case and Software Development,”†
13. Tom Delong, “Define & Compare Flowcharts of Each Method.”†

Bios

John Frost, Moderator

Current NASA Aerospace Safety Advisory Panel Member; owns successful safety consulting company; Senior Member of the International System Safety Society (ISSS); Professional Member of the American Society of Safety Engineers; active in various system safety organizations and initiatives, including G-48; 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

Professor of Software Engineering at the University of York UK; Head of the Computer Science Department from 2006 to 2012; set up the High Integrity Systems Engineering research group; instrumental in developing techniques for producing safety arguments and safety cases which are now used worldwide; Fellow of the Royal Academy of Engineering; Officer of the Order of the British Empire (OBE).

Dave West, CSP, P.E., CHMM, Fellow

Senior Director & Chief Safety Engineer of a 1000-employee Operation of SAIC; current Chairman of the SAE International G-48 System Safety Committee; former President of the ISSS Tennessee Valley Chapter; 25+ years' experience performing safety work for Army aviation and weapon systems, chemical demilitarization, spaceflight programs, chemical plants, and nuclear facilities.

Don Swallom

Safety Engineer U.S. Army AMCOM; Fellow Member of ISSS and former President of Tennessee Valley Chapter; former pilot, staff officer, and developmental engineer in the U.S. Air Force; former Chief of Safety for the Arnold Engineering Development Center.

Barry Hendrix

Lockheed Martin Technical Fellow Emeritus for Aviation Safety and Airworthiness; 40+ years’ experience on various weapon systems; IBCS System Safety Lead for Northrop Grumman;

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.

NASA System Safety Technical Fellow and the Manager of System Safety in the Office of Safety and Mission Assurance at NASA Headquarters; 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; leading the development of the NASA System Safety and Mission Success Standard.

Robert Schmedake

Boeing Technical Fellow; 25+ years' experience in system safety engineering; Fellow Member and Current President of ISSS; Secretary of the G-48; U.S. Co-Chair of the S5000F Committee; Member of the joint Aerospace Industries of America & Aerospace and Defense Industries of Europe Integrated Logistic Support Specification Council; served in the U.S. military from 1986 to 2012.

Tom Delong

Former Lead Systems Safety Engineer for SMDC; 35+ years of safety experience; chaired several missile anomaly investigations during a LAW alternative source selection; managed SETA contract and Range Safety Analysis contract at SMDC; Lead Instructor for APT's System Safety Training program which provides instruction to over 100 professionals annually.