The Safety Case Approach and Other Pressing Issues

A Recap of the G-48 Panel at ISSTS 2014

David B. West, CSP, P.E., CHMM, Fellow; Senior Director and Chief Safety Engineer, SAIC
19 November 2014

Overview of Presentation

- The 2014 International System Safety Training Symposium (ISSTS)
- Brief Summary of SAE International's G-48 System Safety Committee
- Background of the "Most Pressing Issues" Panel
- The Panelists and Their Presentations
  - Tom Pfitzer, A-P-T Research – *Risk Assessment Codes: Problem or Solution?*
  - Dave West, SAIC – *The Safety Case Approach*
  - Warren Naylor, Northrop Grumman – *System Safety: A Glimpse into the Future*
  - Jay Naphas, FAA – *Communicating Safely*
  - Linda Thomas, Boeing – *Update of NAS-411*
  - Tom Martin, FAA – *System Safety Challenges to Human Commercial Space Flight*

The 2014 International System Safety Training Symposium

The 2014 International System Safety Training Symposium

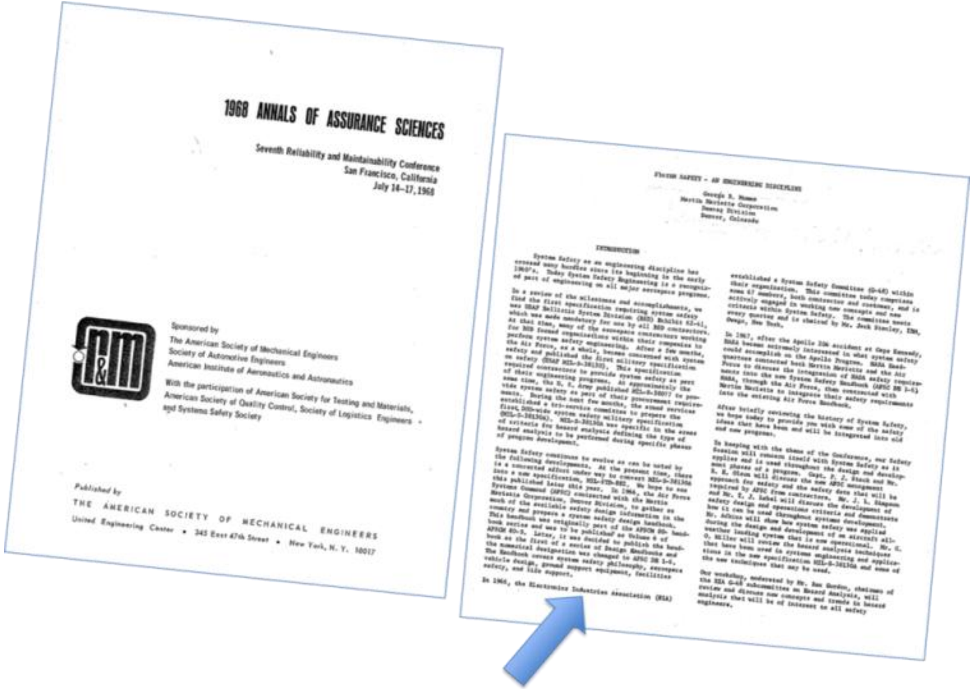
The 2014 International System Safety Training Symposium

INTERNATIONAL SYSTEM SAFETY TRAINING SYMPOSIUM
GATEWAY TO SAFETY
ST. LOUIS, MISSOURI · AUGUST 4-8, 2014

- Over 200 attendees from 10 countries
- 39 technical papers
- 13 tutorials, 6 workshops, 3 panels

SAIC®

Brief Summary of SAE International's G-48 System Safety Committee



1968 ANNALS OF ASSURANCE SCIENCES

Seventh Reliability and Maintainability Conference
San Francisco, California
July 14–17, 1968

Sponsored by
The American Society of Mechanical Engineers
Society of Automotive Engineers
American Institute of Aeronautics and Astronautics

With the participation of American Society for Testing and Materials, American Society of Quality Control, Society of Logistics Engineers and Systems Safety Society

Published by
THE AMERICAN SOCIETY OF MECHANICAL ENGINEERS
United Engineering Center • 345 East 47th Street • New York, N. Y. 10017

SYSTEM SAFETY – AN ENGINEERING DISCIPLINE

George B. Mumma
Martin Marietta Corporation
Denver Division
Denver, Colorado

INTRODUCTION

System Safety as an engineering discipline has crossed many hurdles since its beginning in the early 1960's. Today System Safety Engineering is a recognized part of engineering on all major aerospace programs.

In a review of the milestones and accomplishments, we find the first specification requiring system safety was USAF Ballistic System Division (BSD) Exhibit 62-41, which was made mandatory for use by all BSD contractors. At that time, many of the aerospace contractors working for BSD formed organizations within their companies to perform system safety engineering. After a few months, the Air Force, as a whole, became concerned with system safety and published the first military specification on safety (USAF MIL-S-38130). This specification required contractors to provide system safety as part of their engineering programs. At approximately the same time, the U. S. Army published MIL-S-58077 to provide system safety as part of their procurement requirements. During the next few months, the armed services established a tri-service committee to prepare the first, DOD-wide system safety military specification (MIL-S-38130A). MIL-S-38130A was specific in the areas of criteria for hazard analysis defining the type of hazard analysis to be performed during specific phases of program development.

System Safety continues to evolve as can be noted by the following developments. At the present time, there is a concerted effort under way to convert MIL-S-38130A into a new specification, MIL-STD-882. We hope to see this published later this year. In 1966, the Air Force Systems Command (AFSC) contracted with the Martin Marietta Corporation, Denver Division, to gather as much of the available safety design information in the country and prepare a system safety design handbook. This handbook was originally part of the AFSCM 80- handbook series and was to be published as Volume 6 of AFSCM 80-3. Later, it was decided to publish the handbook as the first of a series of Design Handbooks and the numerical designation was changed to AFSC DH 1-6. The Handbook covers system safety philosophy, aerospace vehicle design, ground support equipment, facilities safety, and life support.

In 1966, the Electronics Industries Association (EIA) established a System Safety Committee (G-48) within their organization. This committee today comprises some 47 members, both contractor and customer, and is actively engaged in working new concepts and new criteria within System Safety. The committee meets every quarter and is chaired by Mr. Jack Stanley, IBM, Owego, New York.

In 1967, after the Apollo 204 accident at Cape Kennedy, NASA became extremely interested in what system safety could accomplish on the Apollo Program. NASA Headquarters contacted both Martin Marietta and the Air Force to discuss the integration of NASA safety requirements into the new System Safety Handbook (AFSC DH 1-6). NASA, through the Air Force, then contracted with Martin Marietta to integrate their safety requirements into the existing Air Force Handbook.

After briefly reviewing the history of System Safety, we hope today to provide you with some of the safety ideas that have been and will be integrated into old and new programs.

In keeping with the theme of the Conference, our Safety Session will concern itself with System Safety as it applies and is used throughout the design and development phases of a program. Capt. P. J. Stack and Mr. R. E. Olson will discuss the new AFSC management approach for safety and the safety data that will be required by AFSC from contractors. Mr. J. L. Simpson and Mr. T. J. Kabel will discuss the development of safety design and operations criteria and demonstrate how it can be used throughout systems development. Mr. Adkins will show how system safety was applied during the design and development of an aircraft all-weather landing system that is now operational. Mr. C. O. Miller will review the hazard analysis techniques that have been used in systems engineering and applications in the new specification MIL-S-38130A and some of the new techniques that may be used.

Our workshop, moderated by Mr. Dan Gordon, chairman of the EIA G-48 subcommittee on Hazard Analysis, will review and discuss new concepts and trends in hazard analysis that will be of interest to all safety engineers.

Brief Summary of SAE International's G-48 System Safety Committee

- Founded in 1966 under (then) EIA
- System Safety experts from Industry, Government, Military, Liaison Orgs.

Brief Summary of SAE International’s G-48 System Safety Committee

- Founded in 1966 under (then) EIA
- System Safety experts from Industry, Government, Military, Liaison Orgs.
- Meets 3x/year
- Previous Parent Organizations: EIA, GEIA, ITAA, TechAmerica

EIA
Electronic Industries Alliance

ITAA

GEIA
Government Electronics & Information Technology Association

TechAmerica
WHERE THE FUTURE BEGINS

Brief Summary of SAE International’s G-48 System Safety Committee

- Founded in 1966 under (then) EIA
- System Safety experts from Industry, Government, Military, Liaison Orgs.
- Meets 3x/year
- Previous Parent Organizations: EIA, GEIA, ITAA, TechAmerica
- Transfer to SAE International announced 7/10/13

Brief Summary of SAE International’s G-48 System Safety Committee

- Founded in 1966 under (then) EIA
- System Safety experts from Industry, Government, Military, Liaison Orgs.
- Meets 3x/year
- Previous Parent Organizations: EIA, GEIA, ITAA, TechAmerica
- Transfer to SAE International announced 7/10/13
- Mission Statement:

  To promote the development of safe systems, products, and processes: the G-48 Committee compiles, develops, improves and publishes best practices in the discipline of System Safety.

- Scope:

  Best practices in System Safety that are the subject of the G-48 Committee’s work are not exclusive to any one domain. They are applicable to hardware, software, human, and environmental aspects of systems for government, commercial, military, aerospace, transportation, industrial, and the medical field.

- Current Leadership

  Chairman: Dave West, SAIC

  Secretary: Gary Braman, United Technologies / Sikorsky Helicopters

SAIC®

Background of the “Most Pressing Issues” Panel

- Action Item #0007 from G-48 Meeting at Las Vegas conference, August 2011
  - Originally intended to be a tutorial on Best Practices, planned for Atlanta conference, 2012
  - May 2012 – changed focus to be a panel, similar to the “Adding Discipline to Our Discipline” series from the mid- to late-2000’s, led by APT Research
  - May 2013 – decided on the “Most Pressing Issues” theme
  - First panel held at Boston conference, August 2013; decided to repeat the “Most Pressing Issues” theme this year in St. Louis
- Format
  - Similar to a Technical Paper session
  - Confer with panelists and each other
  - Time for Q&A, open discussion
- This Year’s Presentations are all available at:

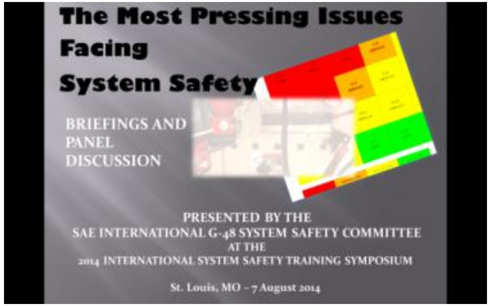
  http://issc2014.system-safety.org/pressing.html

2013

The Most Pressing Issues
Facing
System Safety

A Panel Discussion Presented By
The SAE G-48 System Safety Committee
At the 31st International System Safety Conference
Thursday, August 15th, 2013, 8:00-11:30 am – Suffolk Room

2014



The Most Pressing Issues
Facing
System Safety

BRIEFINGS AND
PANEL
DISCUSSION

PRESENTED BY THE
SAE INTERNATIONAL G-48 SYSTEM SAFETY COMMITTEE
AT THE
2014 INTERNATIONAL SYSTEM SAFETY TRAINING SYMPOSIUM

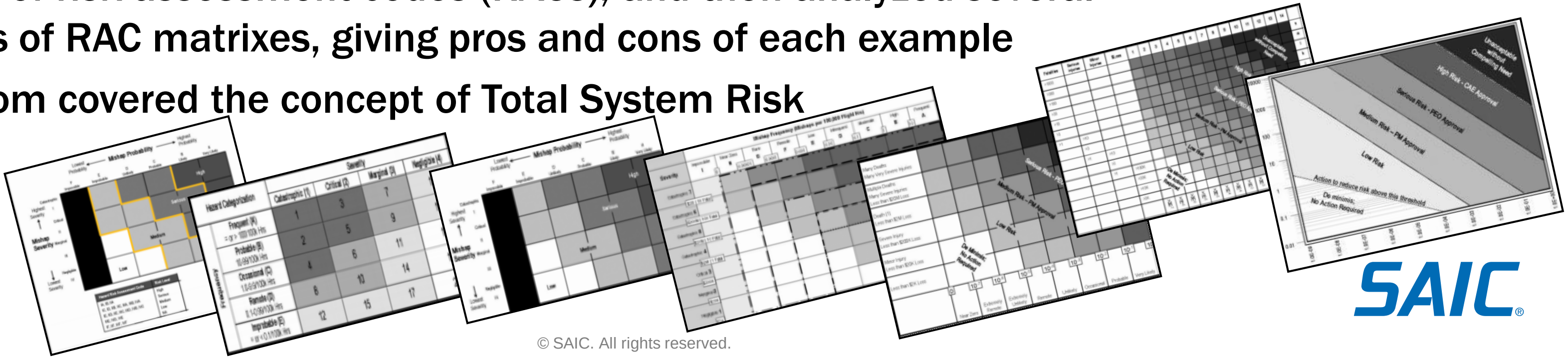
St. Louis, MO – 7 August 2014

The Panelists and Their Presentations

Tom Pfitzer, A-P-T Research: “Risk Assessment Codes: Problem or Solution?”

- Tom Pfitzer is the Founder and President of A-P-T Research
  - A-P-T Research is a SB headquartered in Huntsville, AL
  - A-P-T Research specializes in providing expert System Safety services
  - Tom has over 40 years in System Safety, Range Safety, and Risk Analysis
- Tom started with the following quote from Pat Clemens:

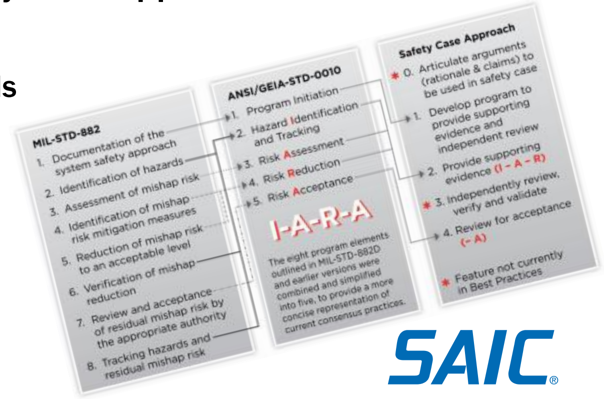
  “I abhor the use of RACs and even worse, the misuse of RACs. But until we come up with something better, it is the best thing we have.”
- Tom’s presentation looked in-depth at the desired features and purposes of risk assessment codes (RACs), and then analyzed several examples of RAC matrixes, giving pros and cons of each example
- Finally, Tom covered the concept of Total System Risk



The Panelists and Their Presentations (Cont.)

Dave West, SAIC: “The Safety Case Approach”

- Dave West is a Senior Director and Chief Safety Engineer with SAIC
- At the “Pressing Issues” panel, Dave’s presentation was about the Safety Case approach
  - The Safety Case approach was brought up a few times at the 2013 ISSC in Boston
  - The Safety Case approach is prevalent in the U.K. and some other European countries
    - Safety Case is defined as a structured argument supported by claims of why the system is adequately safe
    - Evidence is gathered to confirm or deny the claims
    - Evidence consists of analyses and data, similar to tasks in GEIA-STD-0010 and MIL-STD-882
  - G-48 Committee took an action to investigate the utility of the Safety Case approach
  - A-P-T Research hosted a Safety Case workshop in January 2014
    - Presentations of GEIA-STD, MIL-STD, ARP, NASA, and Safety Case methods
    - Compared methods
    - Findings: Safety Case has some strengths not included in U.S. methods
    - Recommendation: incorporate Safety Case approach in best practices
    - Paper published in Spring/Summer 2014 Journal of System Safety



MIL-STD-882

1. Documentation of the system safety approach
2. Identification of hazards
3. Assessment of mishap risk
4. Identification of mishap risk mitigation measures
5. Reduction of mishap risk to an acceptable level
6. Verification of mishap reduction
7. Review and acceptance of residual mishap risk by the appropriate authority
8. Tracking hazards and residual mishap risk

ANSI/GEIA-STD-0010

1. Program Initiation
2. Hazard Identification and Tracking
3. Risk Assessment
4. Risk Reduction
5. Risk Acceptance

I-A-R-A

The eight program elements outlined in MIL-STD-882D and earlier versions were combined and simplified into five, to provide a more concise representation of current consensus practices.

Safety Case Approach

* 0. Articulate arguments (rationale & claims) to be used in safety case

1. Develop program to provide supporting evidence and independent review
2. Provide supporting evidence (I – A – R)

* 3. Independently review, verify and validate

4. Review for acceptance (– A)

* Feature not currently in Best Practices

The Panelists and Their Presentations (Cont.)

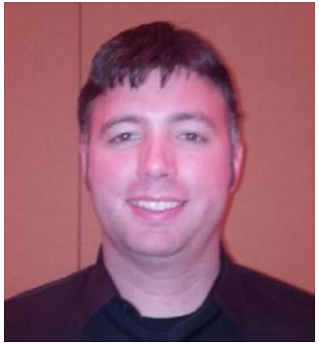
Warren Naylor, Northrop Grumman: "System Safety: A Glimpse into the Future"

- Warren Naylor is a Lead Sr. System Safety Consulting Engineer with NGC
  - Past President of the ISSS and of the D.C. Chapter
  - Co-Founder and Chair of NGC's System Safety Community of Practice
  - Chaired the 2007 ISSC in Baltimore
- Warren started with a brief history of System Safety as a discipline
- Pointed out that "System Safety tends to look into the rear view mirror"
  - Past accidents
  - Lessons learned
  - Prior service history, etc.

- He then made key points about "Where We Are Today and Tomorrow"
  - Globalization and related concerns (international standards, need to reach out to all S.S. societies)
  - Lack of a current professional certification in System Safety (INCOSE establishing an "extension")
  - Summarized additional concerns about the economy, SOWs, communication, and the workforce

The Panelists and Their Presentations (Cont.)

Jay Naphas, FAA: "Communicating Safely"



- Jay Naphas is a Technical Liaison with the FAA
  - Was an FAA intern in 2005-2006 and a Lead for S.S. & SW Safety from 2007-2012
  - Active participant on the G-48 Committee; represented FAA/AST
  - Published works in JSS, IAASS Proceedings, and USAF Wingman
- Jay gave a thought-provoking presentation
  - Focused on "Interpersonal Communication in System Safety Analyses"
  - Started with an audience participation exercise: "Pick a State"
  - Made several points about "Free Will" and its role in our decision processes
- Expressed his General Theory of System Safety
  - All unsafe system behaviors are the result of errors in mental models (latent or consciously accepted)
  - Suggested implications, including that communication content constrains future decisions
  - Recommends looking for losses of information or awareness rather than errors in decision logic
- He believes Safety depends inextricably on communication in all phases

The Panelists and Their Presentations (Cont.)

Linda Thomas, Boeing: “Update of NAS-411”

- Linda Thomas is an Associate Technical Fellow at Boeing
  - Chemical Risk Assessment Lead in Renton, WA
  - Over 20 years consulting on design for environment principles
  - Served as the system safety SME to the NAS-411 work group
- Summarized the development and publishing of NAS-411 (R3), 9/30/2013
  - NAS-411 is the Hazardous Materials Management Program (HMMP) Standard
  - New revision was a collaborative effort between DoD and industry
  - Included new companion document, NAS411-1, Hazardous Material Target List (HMTL)
  - Presentation slides include good detail on content of new revision (first in 20 years!) and the HMTL
- Summarized the Working Group’s next steps
  - Periodic review and update
  - Develop a separate “Tracked HAZMAT” list; list of chemical names and CAS numbers for HMTL items
  - Explore opportunities to harmonize NAS411-1 where feasible with other lists/requirements

SAIC®

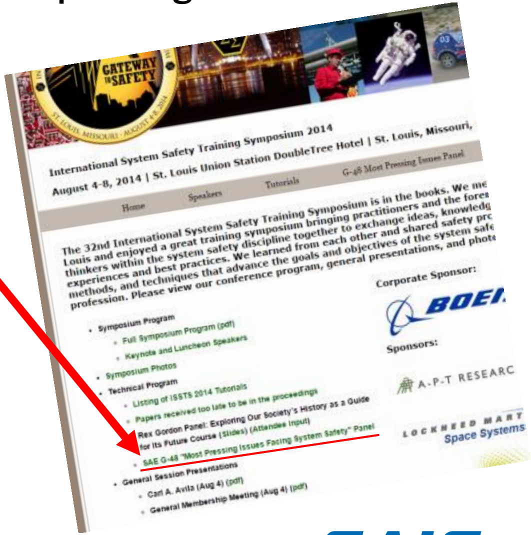
The Panelists and Their Presentations (Cont.)

Tom Martin, FAA: “System Safety Challenges to Human Commercial Space Flight”

- Tom Martin is the Program Technical Lead for System Safety in FAA/AST
  - 24 years with NASA
  - Former Mission Evaluation Room Manager for International Space Station (ISS)
  - Former Chief of technical staff System Safety for Constellation program
- Started with a chronicling of major U.S. and Russian space flight failures
- Listed technical challenges, including extreme energies and environments
- Characterized commercial space flight as “the next step”
  - Explained FAA’s role in establishing a system safety process for commercial human space flight
  - FAA to follow airline approach, organized by major functions of design, manufacturing and operations
  - Requirements will be performance-based and consistent with spiral development technique
- Challenges to regulations
  - Not specifying standards or approaches; instead, evaluating proposed designs against regulations
  - New HSF regulations will follow a more traditional route

Summary

- The 2nd Annual “Most Pressing Issues” Panel was a tremendous success
  - Six quality presentations (originally only sought four)
  - Well attended
  - General consensus from attendees was that issues discussed were indeed “pressing” issues
  - Panel prominently featured on web archives of 2014 ISSTS
  - One panelist already volunteered to present again next year



International System Safety Training Symposium 2014

August 4-8, 2014 | St. Louis Union Station DoubleTree Hotel | St. Louis, Missouri,

Home Speakers Tutorials G-48 Most Pressing Issues Panel

The 32nd International System Safety Training Symposium is in the books. We me
Louis and enjoyed a great training symposium bringing practitioners and the fore
thinkers within the system safety discipline together to exchange ideas, knowledg
experiences and best practices. We learned from each other and shared safety pro
methods, and techniques that advance the goals and objectives of the system safe
profession. Please view our conference program, general presentations, and photo

- Symposium Program
  - Full Symposium Program (pdf)
  - Keynote and Luncheon Speakers
- Symposium Photos
- Technical Program
  - Listing of ISSTS 2014 Tutorials
  - Papers received too late to be in the proceedings
  - Rex Gordon Panel: Exploring Our Society's History as a Guide for Its Future Course (Slides) (Attendee Input)
  - SAE G-48 "Most Pressing Issues Facing System Safety" Panel
- General Session Presentations
  - Carl A. Avila (Aug 4) (pdf)
  - General Membership Meeting (Aug 4) (pdf)

Corporate Sponsor:

Sponsors:

Questions?