



The Physics of System Safety

TJ Candy
DevSafe Consulting, LLC



The intent of this presentation is to make a case for grounding the System Safety discipline and profession in the fundamental truths (“physics” – captured in 5 “laws”) learned in the post-WWII era, defining the ‘modern approach to system safety’

This approach ushered in great improvements in the safety performance of aerospace products observed in the 1970’s and beyond

Recent events suggest an erosion of fidelity to this approach (supported by 5 observations) and return to a more reactive (Fly Around and Find Out) approach to system safety management

The goal of this presentation, if accepted, is to allow individuals or organizations to self-audit their fidelity to the “physics” of the system safety discipline and profession and respond accordingly to reverse this erosion

System Safety Ugly Truths

- “Nobody’s happy to see safety”
- 30-50% of Safety team activities are unplanned
- When safety works right... nothing happens
- A well organized and funded safety effort can have the same outcome as a lucky program
- You can’t take monetary credit for losses that were avoided
- You get the safety effort you pay for
- Hazard identification ends some time after the product is retired
- “The biggest threat to a safety department is a successful safety program”

The Physics of System Safety

Having multiple decades of experience as both an Aerospace Design Engineer and System Safety professional affords a unique view of how these two disciplines interact compared with those whose professional experience is bound exclusively to one or the other.

Much like the Engineering discipline is inextricably linked to established physical laws, this presentation seeks to establish similarly linked “physics” with regards to system safety.

While the physics supporting engineering analysis are more quantifiable, the physics behind the system safety is largely empirical but based on more than 6 decades of application.

Agenda

Background

Ground Rules & Assumptions

The 5 Laws of System Safety

Observations

Summary/Conclusions

Background

Background - Overview



- Retired Principal Engineer – Product Safety - GE Aerospace - April 2024
- Primary engagement in military gas turbine engine industry
- Bachelors in Mechanical Engineering – Michigan State University – 1981
- System Safety Certificate – USC Aviation Safety & Security Program – April 2016
- USC Safety Certification Instructor since October 2021
- Founder - DevSafe Consulting, LLC - 2024
- VP of ISSS Virtual Chapter - 2025

Background – Pre-USC

- Combustion Design Engineer – Advanced Design Team
- Joined Flight Safety Office in 2003 with no formal safety training
- Assign to F136 safety program in 2005 – First development program
- “17 years in the dungeon with only MIL-STD-882 to keep me warm”
 - Multiple engine designs for F-35 – Lockheed Safety/USAF Safety interactions
 - Developed development safety process and hazard tracking system “from scratch”
- Promoted to Principal Engineer in Safety
 - Process and tool utilized on multiple advanced military development programs
 - Co-wrote new Design Practice for all future GE military development programs



Background – USC

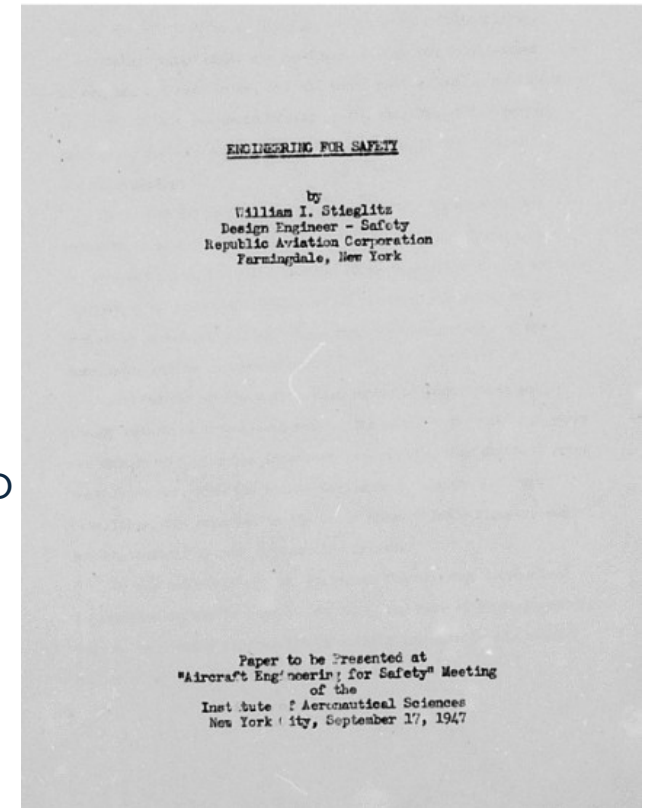
- Joined University of Southern California Viterbi School of Engineering Aviation Safety and Security Program as Certification Instructor
 - SSC – System Safety Course – 8 day course
 - ADVSS – Advanced System Safety Course – 5 day course
- To date
 - 185 Students
 - 12 countries
 - 27 organizations and institutions

Background – In Retirement

- Multiple decade experience in Engineering and Safety
- Objective view/understanding of competing perspectives
- Global USC exposure has revealed many common observations
- Consistent positive response to approach/USC materials
- ISSS Summit 2025 – “System Safety – A Profession in Crisis”
 - Very positive response from attendees and podcast viewers
 - This presentation aimed to set stage for resolving crisis
 - Future paper to address Senior Executive role
- “On mission” to share perspective and advocate for System Safety discipline and profession

Background – This presentation

- Continuation of thought from last year's ISSS paper "System Safety – A Profession in Crisis"
- Primary basis of System Safety exposure operating advanced military gas turbine engine development safety programs based on MIL-STD-882
- Heavily influenced by concepts derived from "Engineering for Safety" paper by William Stieglitz to IAS (now AIAA) published in 1947
- Format of presentation to follow
 - 5 Laws of System Safety – Establish foundation
 - 5 Observations of System Safety – Support validity



Ground Rules & Assumptions

Ground Rules and Assumptions

- Not a critique of GE Aerospace, any specific organization or discipline
- Modern approach to system safety encapsulated in two statements
 - Independent safety oversight needed for all critical product decisions
 - Engaged as early in product/process lifecycle as possible (concept)
- MIL-STD-882 captures the intent of the modern system safety approach
 - Applicable across multiple domains and at all stages of product lifecycle
 - Structured safety process approach (Management – Analysis – Test – Verification)
 - Concepts not techniques (“What not the how”)
 - Designed to be tailored to the specific application/product
 - Used as basis for other System Safety standards and practices

The 5 Laws of System Safety

5 Laws of System Safety

- Based on empirical observations of career/instructor experiences
- Applicable to the discipline and profession of System Safety
 - 0th – Foundation of System Safety
 - 1st – Goal of System Safety
 - 2nd – System Safety Requirements
 - 3rd – System Safety Skillsets
 - 4th – System Safety Tasking
 - 5th – System Safety Competency

0th Law - Foundation

The consequence of violating any of the System Safety laws is a default to a reactive System Safety Management approach commensurate to the degree of deviation.

- **Reactive** – Analysis conducted after loss event to preclude recurrence of event
- **Proactive** – Analysis conducted to identify risk reduction action(s) prior to loss event
- **Predictive** – Analysis conducted prior to use to identify risk reduction action(s) before loss exposure

0th Law – Foundation (con't)

- Historical approach (prior to WWII) – Reactive
 - Fly/Fix/Fly, Break/Fix, FAFO - after the fact
 - Led to founding of multiple organizations - Proactive
 - ASME (1880) – Steam boiler explosions
 - ASSP (1911) – Triangle Shirtwaist Factory Fire
 - NSC (1913) – Workplace deaths (NIOSH – OSHA)
 - Plenty more since (DOT, etc)
- Failure to apply modern (predictive) approach defaults to reactive safety management

1st Law – System Safety Goal

The fundamental goal of the System Safety discipline is to provide independent oversight of critical product and/or process decisions as early in the lifecycle as possible in order to enable a proactive or predictive Safety Management approach.

Modern approach to system safety encapsulated in two statements

- Independent safety oversight needed for all critical product decisions
- Engaged as early in product/process lifecycle as possible (concept)

1st Law – System Safety Goal (con't)

- Modern approach derived from lessons learned during post-WWII aerospace development (ICBM, early aviation)
- Bringing best engineering minds alone was insufficient to preclude loss events
 - Systems Theory – Complex systems require wholistic view full system
 - Human nature – Decisions driven without adequate safety focus
 - Fix problems before reaching the launching pad



<https://youtu.be/Z9EnUQltR9A?si=swrX3c9bLKEDEko->



1st Law – System Safety Goal (con't)

Independent oversight

- Critical product/process decisions made for many factors
 - Economic
 - Performance
 - Manufacturing/Assembly
 - Physical (weight, dimensions, integration, etc.)
 - Safety
- Independence need for objective “eyes wide open” Safety perspective to reduce hazard exposure
- Inform decisions, not make them

“The Safety Committee is composed of a group of staff engineers with the engineering safety specialist as chairman. Each staff engineer is responsible for all detail design in his specialty, and all drawings must be approved by the staff before release. This provides an **independent** check of all design by a technical specialist not a part of the project group, and affords a correlation between projects in eliminating safety hazards.”

William I. Stieglitz
“Engineering for Safety”
September 19, 1947

1st Law – System Safety Goal (con't)

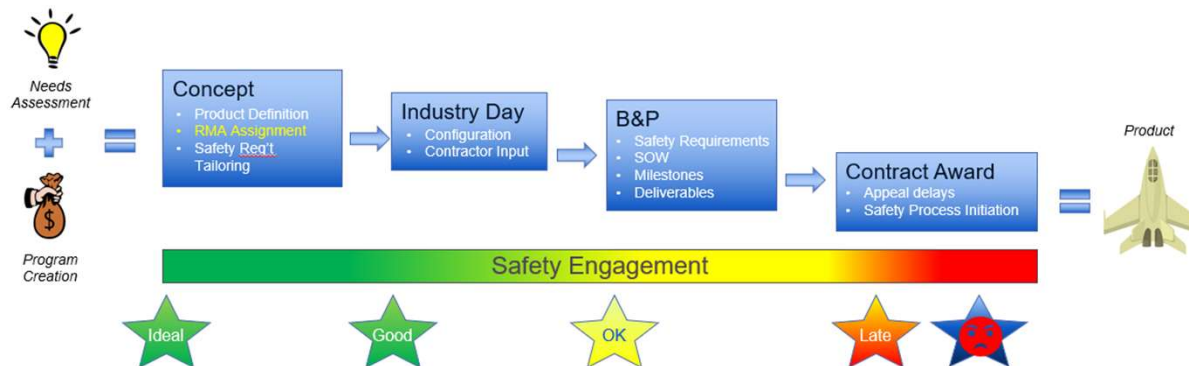
Early Safety Engagement

- Most common issue facing safety professionals
- Often applied after design has been finalized
 - Higher economic impact of design changes
 - Limited suite of solutions available

“it was evident that a safety program of broader scope was needed, ... the program must be organized to insure a constant close check on all detail design, especially of the functional systems. ... it followed that this check must start in the preliminary design stage in order to be fully effective”

William I. Stieglitz
“Engineering for Safety”
September 19, 1947

1st Law – System Safety Goal (con't)



Mitigation Action Order of Precedence

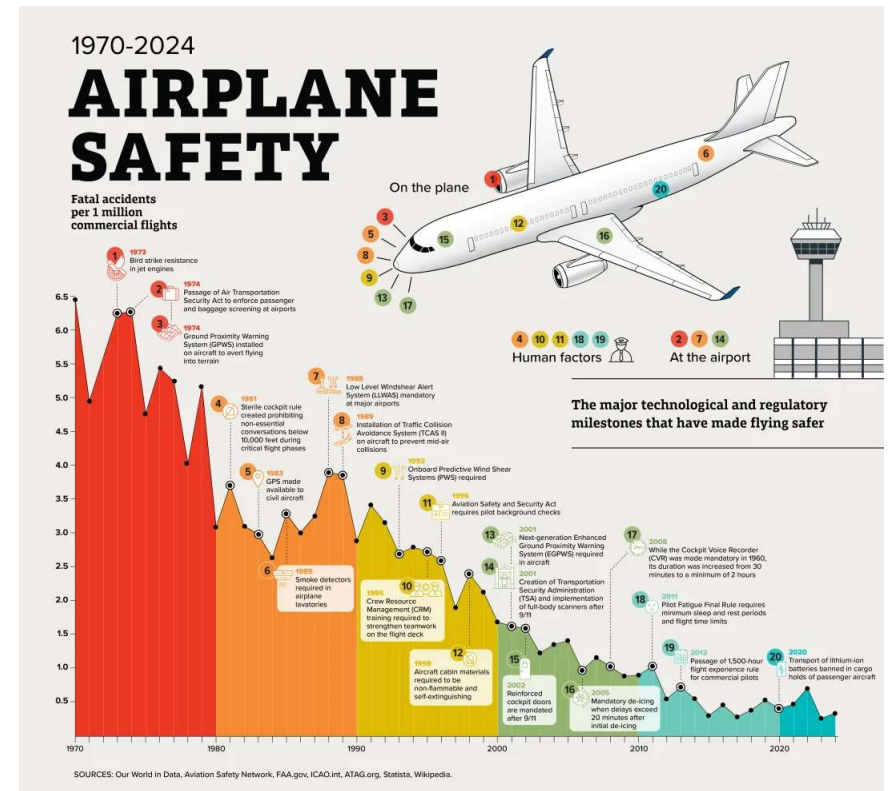
- Eliminate hazards through design selection
- Reduce risk through design alteration
- Incorporate engineered features or devices
- Provide warning devices
- Incorporate signage, procedures, training, and PPE

MIL-STD-8882 § 4.3.4

Order of Precedence

1st Law – System Safety Goal (con't)

- Impact of modern approach to system safety most evident in commercial aviation
- Minuteman missile program still operational today



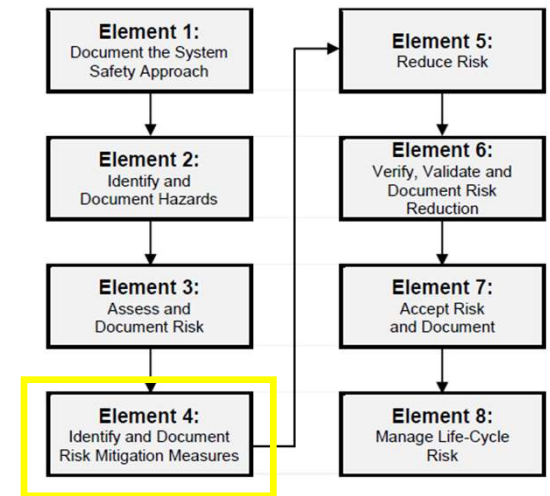
2nd Law - Requirements

The fundamental output of the System Safety discipline is the identification and verification of risk mitigation actions (requirements) necessary to meet established system safety risk acceptance criteria.

“During product development, requirements are safety”

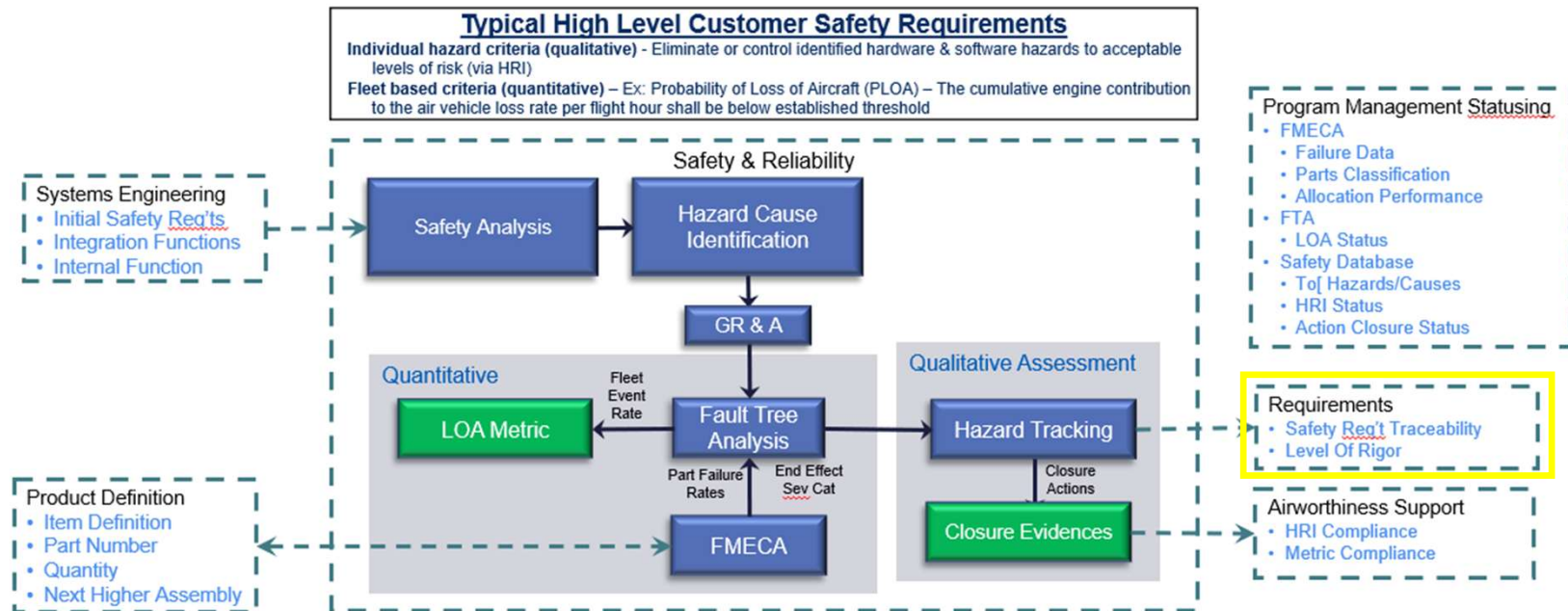
2nd Law – Requirements (con't)

- Determining risk reduction action(s) is the fundamental product of the System Safety process
- Analysis is needed to determine hazards and causal scenarios
- Assessment is needed to determine action(s) needed to adequately manage risk



MIL-STD-8882 – Figure 1
8 Safety Process Elements

2nd Law – Requirements (con't)



2nd Law – Requirements (con't)

How do you know when to stop?

- Clear risk acceptance guidelines need to be established early
- Typically communicated by some form of Risk Acceptance Matrix (“Heat Chart”, HRI, etc.)
 - High, Serious – Unacceptance
 - Medium, Low, Eliminated – Acceptable
 - Identification of action to reduce risk exposure (probability) until acceptable risk achieved
- High/Serious risk can be accepted via formal risk assessment process

RISK ASSESSMENT MATRIX				
SEVERITY PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

MIL-STD-8882 – Figure 5
Risk Assessment Matrix

3rd Law - Skillsets

The fundamental skillset of a System Safety expert is the ability to plan and conduct a product system safety effort.

This involves analysis of products/processes in order to identify hazards and risk causal scenarios which allow safety risk to be assessed, and action(s) identified to reduce risk to within established risk acceptance criteria.

“Safety is a specialized subject just as are aerodynamics and structures. Every engineer cannot be expected to be thoroughly familiar with all developments in the field of safety any more than he can be expected to be an expert aerodynamicist.”

William Steiglitz
“Engineering for Safety”
September 1947

3rd Law – Skillsets (con't)

- System safety origin is in Systems Engineering
- Specialized skillset - “Myopic Systems Engineer”
- Engineers can do Safety Analysis – not independently
- Economic and other factors often lead to an over-reliance on Engineering to perform Safety function -> erosion
- Engineers need to support the Safety team, not supplant them

4th Law - Tasking

The fundamental tasking of the System Safety expert is to create, initiate and oversee the conduct of a tailored system safety process which ultimately meets product/process regulatory safety requirements.



4th Law – Tasking (con't)

Typical System Safety Team Tasking

- Creation of a Safety Plan which defines the safety effort for the specific product which is aligned with the overall product development plan
- The definition, execution and management of a safety process which is tailored to the specific product intended to satisfy the customer safety requirements and engages the full organization.
 - Identify Safety Hazards
 - Conduct Safety Analysis
 - Perform Safety Assessments
- Presenting documentation validating compliance to all safety requirements to customers and/or regulatory agencies.

4th Law – Tasking (con't)

- System Safety tasking works in conjunction with organization safety policies, procedures and best practices
- Primary focus of product System Safety process is “Unknown/Knowable”

Hazard Existence	Hazard Discoverability	Hazard Identification Method
Known	Knowable	Corporate Memory (Lessons Learned, Safety Centers, etc.), Standards, Policies, Best Practices
Known	Unknowable	Undocumented Lessons Learned or Expert Loss, Protected Data
Unknown	Knowable	Safety Analysis (200 series tasks), SME engagement, open reporting
Unknown	Unknowable	Opportunistic Inspection (Fleet Leader), Analytics, Trial & Error (break/fix)

5th Law - Competency

The definition of a System Safety expert is a System Safety practitioner with suitable maturation typically requiring a minimum of 10 years of system safety-specific training and product/process-specific system safety experience to achieve.

Need for industry recognition of System Safety as distinct profession with concurred competency levels and more centralized credentialing

5th Law – Competency (con't)

- One of the biggest challenges to define is what constitutes a “Safety Expert”
- No globally recognized/central credentialling exists
 - BS/MS/PhD degree in System Safety
 - CSP certification
 - Other certification (USC, other)
 - SQEP – UK, others
- ISSS Credentialling initiative underway but not complete
 - ISSS delivered training
 - “Partnering initiative” – Organizations and Institutions

5th Law – Competency (con't)

- Challenges to centralized credentialling
 - Wide range of domains, interpretations and specialized skillsets
 - Concurrence on what is common to all domains
 - Codifying combination of training and experience
 - Safety profession has high number of self/internally trained/certified experts operating
 - Long (~10 year) “Pipeline” for achieving necessary competency which tends to be domain-specific
 - Getting experts to agree

5th Law – Competency (con't)

System Safety Domain Chart



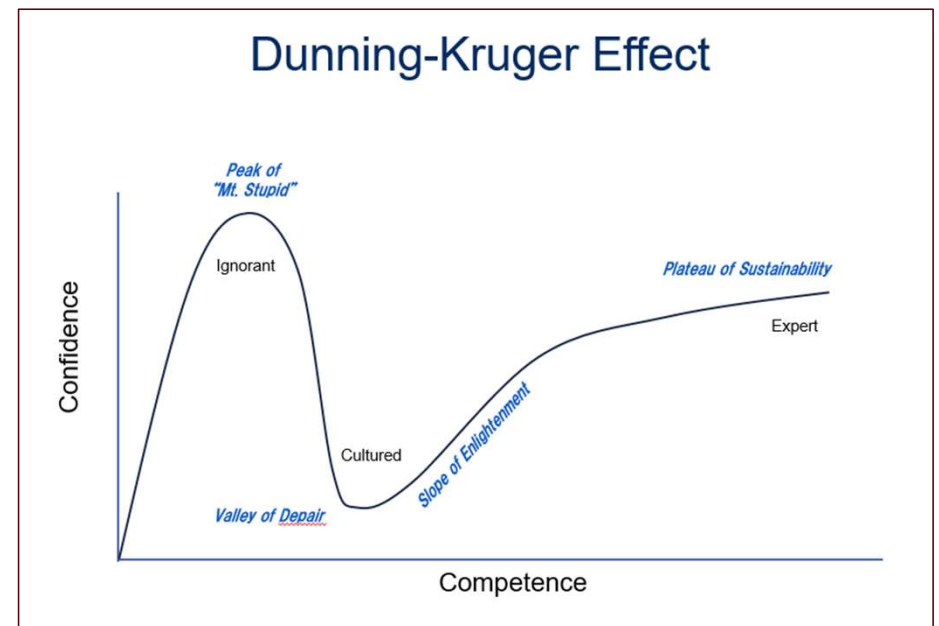
Domain Exercise

- Students circle their domain engagements
- Each “line of experience” can have unique
 - Safety Standards
 - Practices
 - Acronyms, Abb.
 - Forms of analysis
 - Regulatory engagements
- Individual exposure to System Safety can vary widely

Software could be its own parallel category

5th Law – Competency (con't)

- Dunning-Krueger Effect - general competency/maturation model
 - You don't know what you don't know
 - You don't know that you don't know
 - You think you know
- Observation and discussion with fellow safety experts cite ~10 years to achieve competency
- Strongly influenced by Domain considerations
- Best used to set expectation, not critique



5th Law – Competency (con't)

- “Wild West” characterization is valid
- Need for centralized credentialing competency model
 - Agreement on fundamental aspects of System Safety
 - Accommodate Domain considerations
- Requires
 - “Consensus of experts” to create
 - Concurrence of regulatory agencies to enforce
 - Engagement/Support of industry/institution Senior Executives to deploy

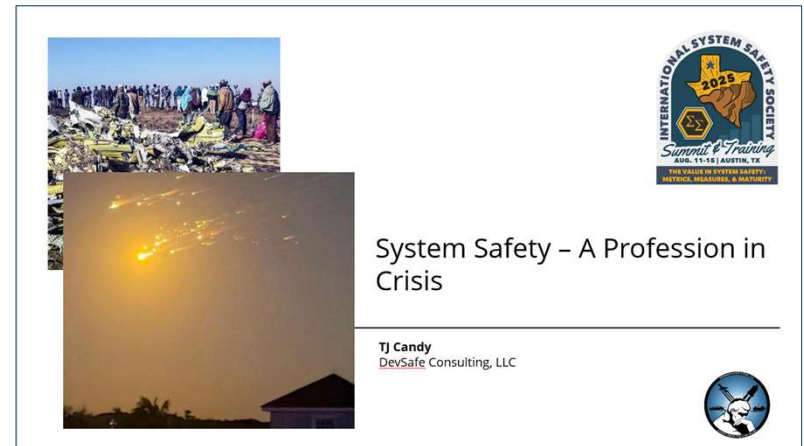
Observations

Observation - Preamble

- The following are a series of 5 personal observations which I believe affect fidelity to the fundamental aspects of the system safety discipline and profession
 1. Safety professional crisis
 2. Safety word disambiguation
 3. Risk managing authority proposal
 4. Software Safety perspective
 5. The path ahead

Observation #1 - Safety professional crisis

- Presentation at ISSS 2025 Summit and Training – “System Safety a Profession in Crisis”
- Podcast:
<https://www.youtube.com/watch?v=XXRyxJISLEA>
- Positive reaction to presentation, podcast across wide spectrum
- Overall summary
 - Crisis driven by loss of independence of the safety function, eroding back into Engineering function
 - Result is higher reliance on Reactive safety management which is increasingly evident in industry



Observation #1 - Safety professional crisis (con't)

- Independence erosion driven by many factors
- Intrinsic to the Engineering function
 - **Product advocacy** – Design ownership including safety performance. Adversarial response “don’t call my baby ugly”!
 - **Self-sufficiency** – Desire to expand their knowledge and capabilities. Engineers can conduct the safety tasking
 - **Chafing** – Human nature (“looking over my shoulder”). Enlightened perspective needed to recognize value
 - **Cost is King** – If safety oversight equals redundancy to engineering, funding, staffing and training reductions can result.
 - **Checkbox Mentality** – Blind compliance to safety guidance without interpretation can lead to inefficiencies and result in unnecessary risk

Observation #1 - Safety professional crisis (con't)

- Erosion spiral
 - Non-safety experts prone to misapplication of standards, etc.
 - Under-trained safety experts can result in lost confidence in safety input and reticence to engage them early in the lifecycle
 - Loss of engagement as well as lack of funding for training slows competence maturation of safety team members
 - Slow maturation can result in safety team attrition and vulnerability to “poaching” from other departments
 - Less effective safety team encourages increased safety tasking to Engineering further reducing maturation and compromise of independent oversight function

Observation #1 - Safety professional crisis (con't)

- Worst case outcome:
 - Under-experienced safety team brought in late to provide safety evidences from a sub-standard safety process to regulatory functions for approval
 - Compromise of predictive (“knowable”) hazard identification
 - Reactive safety management
- Solution will require high level leadership oversight to assure vitality and proper engagement of safety teams

Observation #2 - Safety word disambiguation

- Wielding the “S Word” gets attention
- In the right hands
 - Cut through bias
 - Create priority and focus
- In the wrong hands
 - Distract/disrupt discussion
 - Create confusion/inefficiencies
 - Mislead decision making process



Observation #2 - Safety word disambiguation (con't)

Some of the Safety “blades”

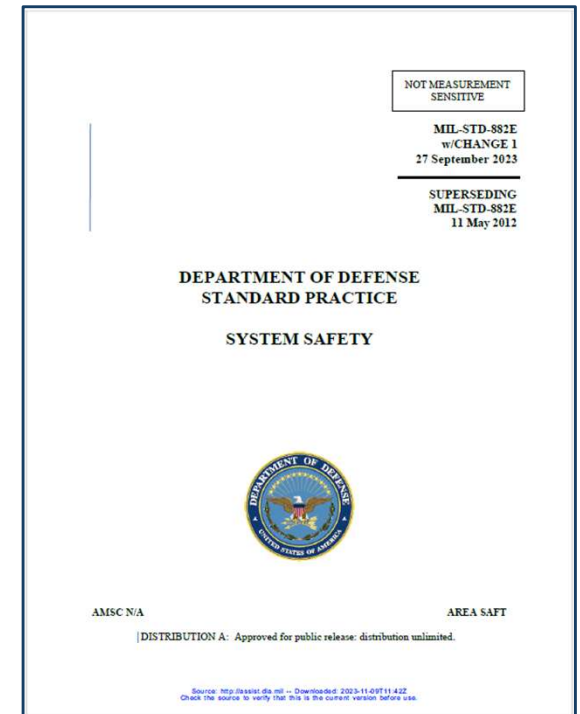
- **System Safety** - Structured approach to hazard identification, risk assessment and corrective action verification
- **Functional Safety** - System safety concepts applied to sub-systems or subfunctions (e.g., ADAS, Gas Turbines)
- **Software Safety** - Functional Safety in the context of software-controlled systems
- **Flight Safety** - System safety concepts applied to the initiation, sustainment or termination of flight
- **EHS or Industrial Safety** - System safety concepts applied to environmental or personnel risks, particularly in work environments
- **Operational Safety** - Compliance with established safety guidance

Observation #2 - Safety word disambiguation

- The word “Safety” alone can have multiple contexts
- Most people think they understand safety intrinsically
- Attempting to have safety discussions without understanding context and domain can create problems
- Dueling safety expert scenario
 - Safety experts from different domains and contexts can appear to be clashing when they are actually in “violent agreement”
 - Dueling Safety experts confound non-Safety people and cause them to withdraw back to their own interpretations (professional erosion)

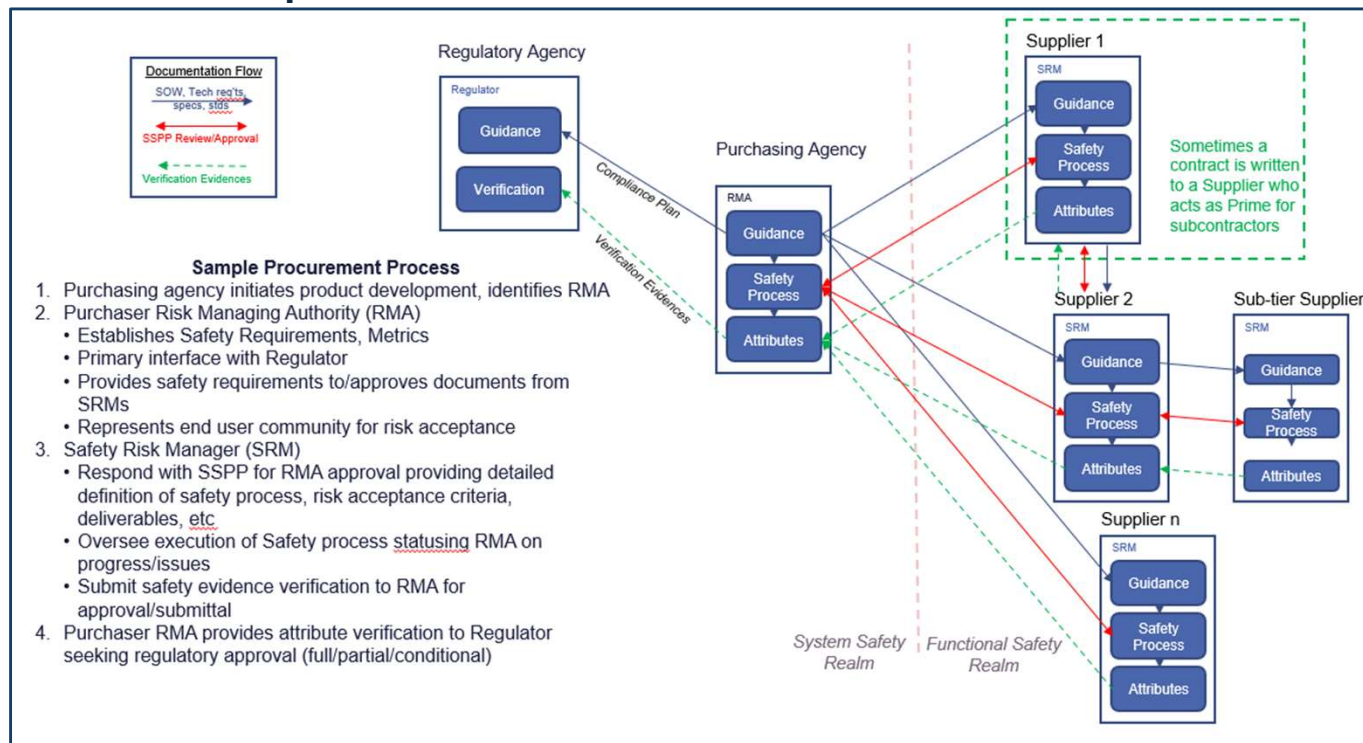
Observation #3 - Risk managing authority proposal

- In every safety effort, individuals take leadership roles in formulating, overseeing, managing and approving the system safety effort and the products it produces
- Current MIL-STD-882 makes multiple references to authorities
 - Risk acceptance/approval authority
 - Contract safety requirement execution/user concurrent authority
- Proposal: Formalize these roles in the context of how product safety efforts are typically conducted



Observation #3 - Risk managing authority proposal (con't)

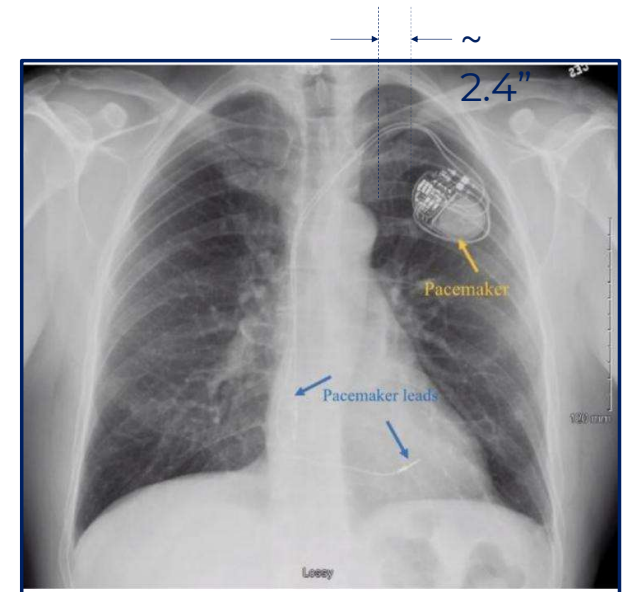
Proposed RMA/SRM Functional Interaction



- Define roles of regulators and risk managing authorities (RMA/SRM) consistent with how projects run
- Focus on identifying individuals holding risk manager tasking
- Note proposed System/Function Safety boundary

Observation #4 - Software Safety perspective

- Need for better organization of how software is handled within System Safety Discipline
- Complexity of software has increased drastically since introduction of the modern approach to system safety (even before AI)
- Observation: Can be viewed from two perspectives
 - Within historical System Safety tasking
 - Outside historical System Safety tasking



“Software is very close to my heart” – TJ Candy

Observation #4 - Software Safety perspective (con't)

Within historical System Safety Tasking

- Interface with Software Development Team
 - Safety Critical Functions (SCF's) are identified during FHA
 - Level of Rigor (SwCI) guidance provided along with software-based mitigation actions (HLR's) identified during the conduct of the system safety effort
 - Any derived safety requirements from decomposition of HLR's are added to new or existing hazards tracked in the HTS
- Oversight of the software development safety process is usually handed off to a member of the software team
- Software team only reports validation of HLR's to Safety Team

Observation #4 - Software Safety perspective (con't)

Outside historical System Safety Tasking

- Receives SCF's and HLR's from the Safety Team
- Create Software Safety Program Plan
- Oversees compliance to software analysis and software testing requirements commensurate with SwCI guidance
- Coordinates software-specific hazards identified during analysis and testing phase with Safety team
- Provides validations of HLR's to Safety Team

Observation #4 - Software Safety perspective (con't)

- There is a need for the identification of Software System Safety professionals within the system safety discipline and profession
- Sample competencies
 - Analysis techniques to find vulnerabilities
 - Software (OS and AS)
 - Software architecture
 - Electronic hardware architecture
 - Software test levels and LoR coordination
 - AI (developing)

Observation #4 - Software Safety perspective (con't)

- Hardware based System Safety and Software System Safety are parallel efforts but require similar but distinct and specialized skillsets from one another
- Historical development efforts have typically “deputized” a member of the software development team to serve in this capacity and coordinate with the hardware safety team
- There is a need for a similar “independent oversight” organizational implementation relative to the software development effort
- There is a need for a similar competency and credentialing requirements parallel to historical System Safety professionals

Observation #5 - The path ahead

- To address the crisis observed in the System Safety profession, actions within the realms of safety organization leadership and business leadership will be needed
- Safety Organization
 - Assure compliance with internal safety policies and procedures
 - Manage staffing and competence maturation progress (“pipeline of safety experts”) is maintained
 - Assure timely engagement of safety resources consistent with product lifecycle
- Senior Executive (CEO)
 - Assure “vitality” of Safety Organization and ability to meet business safety goals

Summary/Conclusions

Summary/Conclusions

The System Safety discipline is governed by “physics” which, when defied, produce undesirable results

System Safety “physics” are empirically based and substantiated by wholesale improvements in safety performance after WWII

A long-term erosion of fidelity to these “physics” have resulted in a regression from predictive to reactive (FAFO) safety management as evident in many current events

Evolution of thought in areas of independent oversight, safety credentialing, software safety and risk management is needed

The greatest hope for restoration of the System Safety profession and discipline lie in Senior Leadership assuring fidelity of their System Safety organization to these “physics” as well as the vitality of the individuals within it



Contact TJ Candy
Tj.candy@devsafeconsulting.com
<https://devsafeconsulting.com>
 LinkedIn (Anthony Candy)

