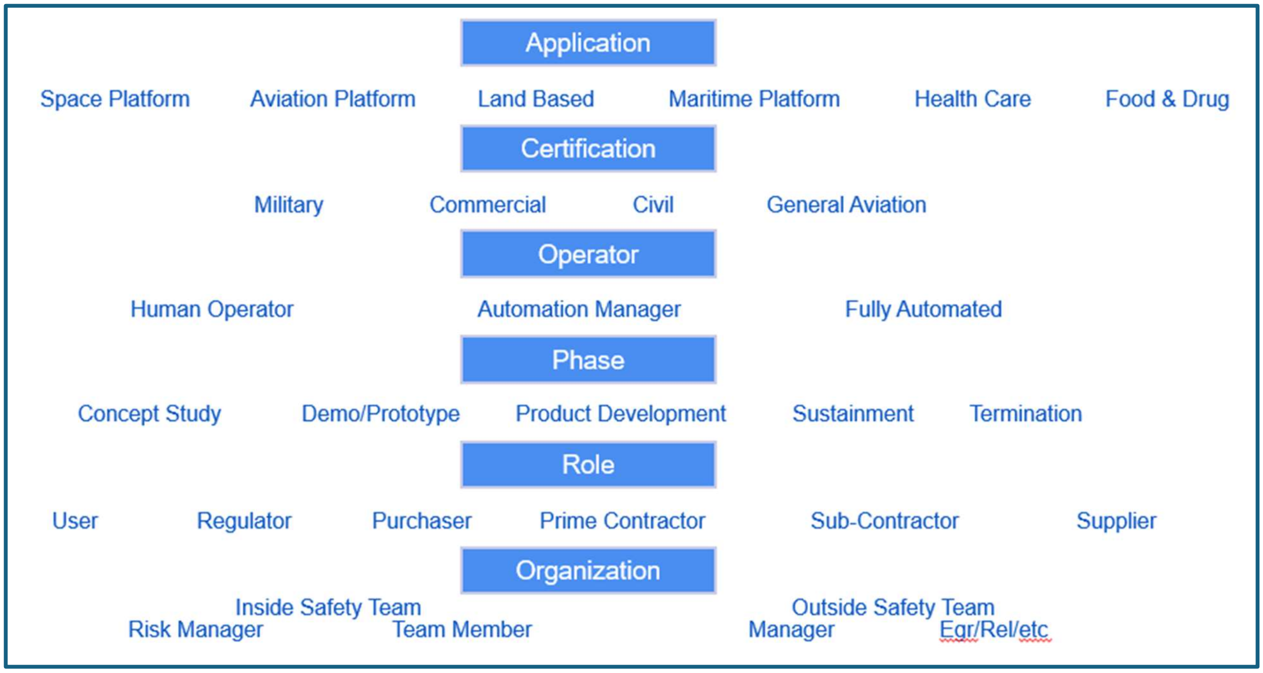
The System Safety Challenge

Forward – Who are we, anyway?

As we complete the first quarter century of this millennium, many of us considering ourselves "system safety experts" find ourselves in a conundrum in responding to the many recent high-profile safety issues. Design issues, quality problems, human errors, new technologies, AI and other challenges elicit no shortage of strong words and opinions on what the problem is and what to do to move forward both from inside and outside the system safety profession.

The variation in "what to do" from the "safety experts" can confound any well-intentioned person trying to get a warm feeling that the industry is headed in the right direction with regards to safety.

The first thing to realize is that there are many flavors of safety experts. Depending on the product application you are working on, where it's used, who is using it, where it is on the product lifecycle, your role relative to safety and even what organization you are in can make a large difference in your terminology, abbreviations, catch phrases and skill sets required.



System Safety Scope of Engagement Chart

The problem is exacerbated by the fact that so many of these various safety experts can be fully or partially right, even if it sounds like they're saying vastly different things.

As a system safety certification instructor at the University of Southern California Aviation Safety and Security Program, I have a chart I like to show students that illustrates just how wide the definition of “safety expert” is. I ask students to circle where they are on this chart and in what capacity they operate and connect the circles with a line. Then I say that each top to bottom line can represent a different interpretation of what system safety is and result in safety experts sounding like they’re disagreeing when in reality, they are not.

While I’m sure this chart can be expanded to some degree, the point is that depending on where the product you are developing fits into this chart, your “safety expert” may have different applications of safety standards, safety processes, and even terminology. While there are underlying fundamental truths about system safety, each “line” you draw from top to bottom for your specific application can carry its own unique path of how to make/keep a safe product.

The crosshairs of the system safety challenge lie with those in the “Role” line of the above chart. They are the risk managers, decision makers and recipients of the consequences from an unsafe product making it to the marketplace. The problem is that the definition of what a “safety expert” is for each of these roles really doesn’t have a firm industry accepted basis for definition. It is sometimes difficult even for safety professionals to know when they are talking to a tried-and-true safety expert or someone just assuming the role.

I plan in the coming weeks and months to share highlights of what I believe has become my vision and mission for system safety coming from my 40+ years in the aerospace industry and nearly 20 years as a system safety professional. The reaction to date from my USC students on what I have had to say from has been very gratifying and encourages me to take on this topic in this forum.

Chapter 1 – Foundations

My vision for addressing the challenges facing the system safety profession today is grounded in what I understand as the 'founding era' of the modern system safety discipline; the post-WWII ICBM development experience.

While accountability for safety is documented as far back as the Code of Hammurabi, the historical approach to safety was primarily reactive. Something bad happened, lessons were learned and corrective actions were applied to try to avoid the same thing from happening again. This is referred to as a "break/fix" cycle. This is still the primary approach to manage safety during the operational/sustainment phase of the product lifecycle.

During the ICBM development, the threat of nuclear annihilation and the number of early development test failures provided the motivation and the emergence of systems theory as well as more capable analytical tools and provided the means for new forms of safety specific analysis to be created. This allowed for proactive and predictive methods to be brought to bear to try to detect and address hazards as early in the design lifecycle as possible. Preferably before new designs made it to the launch pad.

Early ICBM MIssile Failure

Additionally, the need for objective safety oversight of critical product design and operational decisions became evident to assure safety considerations were adequately and objectively represented in what went into the final product.

The net result was a reduction in losses, a successful Minuteman missile program and ultimately the creation of a structured approach to system safety encapsulated in the DoD standard practice for system safety, MIL-STD-882, which was first released in 1969 and is maintained to this day (Rev E Change 1 released 27 Sept 2023).

The question posed in looking back is "how are we doing?". Do we have independent and experienced safety teams providing safety oversight throughout the product development lifecycle (even at the concept phase)? How well are we doing with the proactive and predictive forms of safety analysis to keep up with new technologies and processes? Or are we backsliding into a "break/fix" reactive approach to system safety?

My vision for system safety is for an accountability to the system safety teams and senior leadership at all levels of the procurement chain (sub, prime contractors, purchasers, regulators -

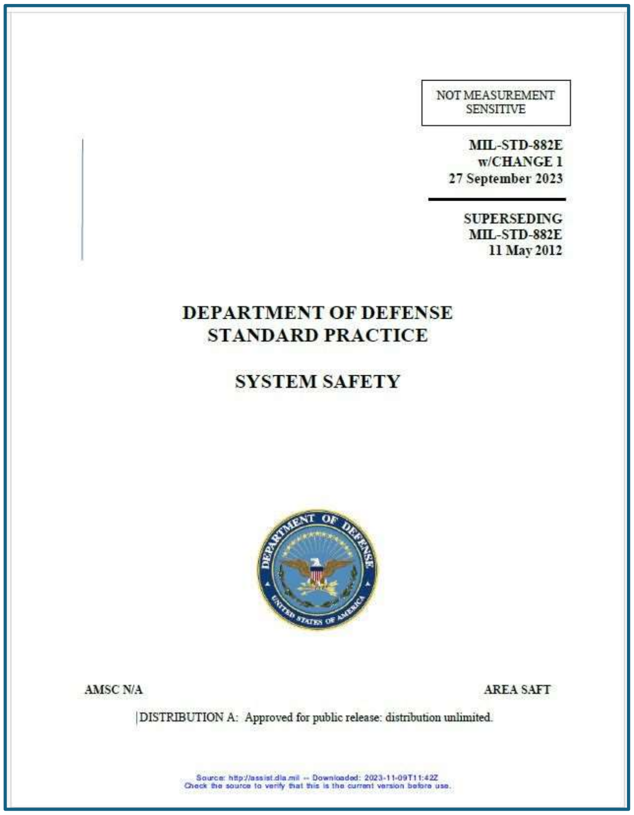
"Role" in my prior post) to take a soul searching look at their fidelity to what I call the fundamentals of system safety during new product development. And build from there.

Chapter 2 – Understanding MIL-STD-882

In my prior LikedIn post, I talked about how the lessons learned from the post-WWII ICBM development resulted in the creation of MIL-STD-882, a best practice for conducting a structured approach to manage system safety risk over the entire product lifecycle for defense system procurement.

The results of this approach and it's positive impact on safety in the years which followed are a matter of historical record. The safety improvements for the Minuteman missile program led to a successful deployment. In fact, it remains in service nearly 60 years later. The DoD acquisition programs which followed this approach have benefitted in terms of safety performance even as technology continued its rapid advancement through the turn of the century.

But here we are decades later facing events which seem to fundamentally question our ability to manage product safety risk. Does the "old" safety system approach no longer work or have we strayed from the path they set?



NOT MEASUREMENT SENSITIVE

MIL-STD-882E
w/CHANGE 1
27 September 2023

SUPERSEDING
MIL-STD-882E
11 May 2012

DEPARTMENT OF DEFENSE
STANDARD PRACTICE

SYSTEM SAFETY

AMSC N/A AREA SAFT

DISTRIBUTION A: Approved for public release: distribution unlimited.

Source: http://assist.dla.mil -- Downloaded: 2023-11-09T11:42Z
Check the source to verify that this is the current version before use.

I spent a large part of my career as a system safety professional trying to understand MIL-STD-882 and not just simply comply with the safety tasking listed in the Statement of Work. What I learned was that MIL-STD-882 is not intended as a cookbook for system safety that just anyone can follow. It provides concepts and not techniques. It covers all phases of the product lifecycle for a wide range of products and is meant to be tailored by a knowledgeable authority that owns the responsibility to adequately manage the product safety risk.

MIL-STD-882 is intended for use by trained and experienced system safety professionals. Those without training or experience can accomplish system safety tasking, however, I believe the potential for mis-application of safety standards and lack of independent safety oversight is a pathway back to the pre-ICBM "break/fix" era. This misuse, however justified, can result in an inefficient and less effective safety process as a minimum.

The challenge facing the industry today is exacerbated by understaffing and the exodus of highly trained and experienced safety experts leaving the industry through frustration, retirement and death. Further, the use of many other authoritative system safety standards, practices, handbooks that have been developed over international, industry and institutional boundaries can create obfuscation in terminology and definitions for even the same concepts, even amongst experts.

I believe there needs to be a revival within the system safety function across the industry. To return to the fundamentals the originators of MIL-STD-882 implemented. And continue to evolve it to match the business environment, tools and challenges of today.

I believe it can be done and I will be expanding on my vision for this in future posts.

Chapter 3 – The Physics of Safety

There was a saying we used to use during my 14 year tenure as a design engineer that helped focus discussion around some vexing problems; "you can't fight physics".

Having a common ground amongst engineers helped to focus discussion and reduce time spent running down rabbit holes based on our common understanding of basic physics.

While not physics in the classical sense, there are some bedrock truths I observed during my 19 years as a system safety professional that seemed to apply in all safety efforts and are in line with the core ICBM safety learnings.

I would sum up these core learnings as 1) have independent project oversight by trained and experienced safety professionals and 2) execute a structured safety plan (described in concept in MIL-STD-882) as early in the design phase as possible.

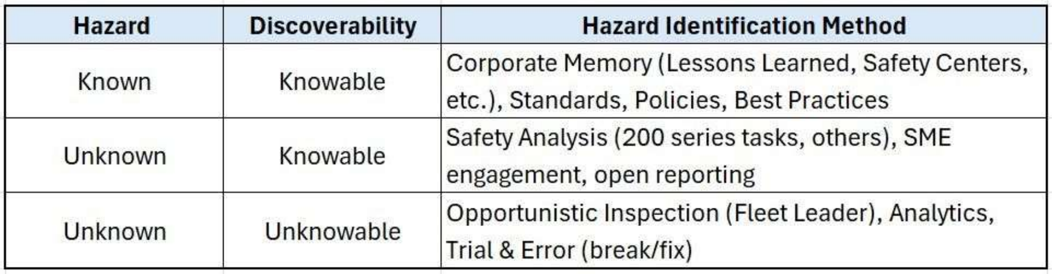
While independent oversight is an easily understood idea, I've concluded that a structured safety plan needs to have 5 fundamental elements. What I call the "physics of safety".

1) Identify safety hazards
2) Analyze and assess hazards
3) Determine risk reduction actions and assess residual risk
4) Assure implementation of identified actions
5) Document residual safety risk

While each one of these steps can involve a myriad of application-specific approaches and methodologies to complete, without completing all 5 steps, I would maintain that safety risk can be left on the table.

Unless you are working with a duplicate of a proven product, residual risk is present even if all internal and external safety specifications are being complied with.

As expected, step 1 is the biggest and most critical. It is the burden of the safety process to identify the "knowable" hazard causes (see below) and subject all plausible hazards to the remaining 4 steps as necessary.



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

Steps 2 and 3 should be accomplished with the engagement of subject matter experts (SME's). This assures concurrence and technical accuracy of the safety data long before the design is finalized. Revelations and changes after this time can get very expensive for a lot of reasons.

Giving a regulator access to the evidences produced in steps 4 and 5 provides the basis for substantiating a product safety readiness assessment.

In a cost-conscious world where challenges are high, time is short and access to expertise is limited, there will always be temptation to bypass or cut corners on the safety process. Especially by those who don't fully understand it or believe it works. I see this as one of the main drivers for the erosion in the ICBM safety learnings and why we find ourselves facing the safety challenges we do today.

If you lose truly independent oversight, you're headed for break/fix cycles. And you can only mitigate the risks for the hazard causes you know about.

Chapter 4 - The Path Ahead

In this series of posts I've sought to provide my high level view of the safety challenges facing the industry today. The perspective is that of a safety professional and system safety certification instructor.

My hope with these posts is to trigger thoughtful self-examination of how safety organizations are functioning today as they compare with the system safety process learnings of the past. Especially in light of current high profile safety issues.

I believe a key part of the path ahead lies outside the system safety profession and in the hands of those running the organizations who are bringing new technologies to the marketplace. What those who define where the safety function resides in their businesses and who charter and staff their system safety departments believe and understand about system safety.

Are they assuring the functional independence of the safety department? Are they directing adherence to a grounded and structured safety program relying on trained and experienced safety personnel? Is the safety team integral to the product development effort or standing on the side waiting to be called in?

The reality today is that organizations face fierce cost challenges. Everyone seems to be operating with skeleton crews in all areas of their businesses. But attempting to meet the rising safety challenges of advancing technology without an adequately structured safety process or trying to work with an under-staffed, under-trained or inexperienced safety team carries the inevitable outcome of increasing levels of residual product safety risk. Possibly like we're seeing today?

The staffing challenge is exacerbated by the loss of expertise as well as the time constant associated with the pipeline for creating new safety professionals being measured in years, not weeks or months.

The challenge is compounded by the reality that the safety team may spend large amounts of time supporting unplanned activities. Things happen, questions arise that need immediate and focused attention. If this allowance isn't cooked into the safety manpower plan for development programs, then the unplanned activities are done at the expense of needed planned activities.

Many high-profile safety issues confront the industry today. I firmly believe the path ahead requires business leaders to understand the foundations of the system safety discipline, an 'eyes wide open' self-assessment of where they are now and vision for where they need to go to allow their safety teams to function as intended. Not only to meet the challenges of today, but those on the road ahead.