System Safety – A Profession in Crisis

T.J. Candy
DevSafe Consulting, LLC

ABSTRACT

The System Safety profession is facing a crisis in responding to recent industry events. Driven not only by new technologies and an aggressive pace of product development, but also failures to follow established safety policies and procedures. This crisis is exacerbated by the exodus of tried-and-true system safety experts via retirement and simply leaving the discipline. Often handing the reigns of major development programs to newcomers to the system safety discipline.

The existing System Safety experts must operate in a challenging cost-driven environment where understaffing, under-training, high workload and high personnel turnover is the norm. In addition, a lack of consensus on minimum training and standards creates confusion and disagreement in the industry on the safety process itself (even amongst system safety experts). This has led to "new" approaches to system safety offered to industry. The net result being a slow migration of the system safety function back into the Engineering domain and increased instances of finding serious issues after products are introduced into the marketplace.

This paper presents observations gained from four (4) decades spent in both Engineering and System Safety developing advanced military products as well as four (4) years teaching system safety at the University of Southern California (USC) Viterbi School of Engineering – Aviation Safety and Security Program.

This paper will present these observations in the framework of the system safety lessons learned from the post WWII Intercontinental Ballistic Missile System (IBCM) program. It will propose a multi-level strategic approach to be considered to address the current state of the System Safety profession going forward.

1) BACKGROUND

The author of this paper is a recently retired System Safety Controlled Title Holder (CTH) at GE Aerospace (GE) with 43 years aerospace experience with 20 years as a design engineer and 19 years as a system safety professional. The remaining time was spent as an information technology (IT) professional based on time spent as a Computer Science major prior to switching to Mechanical Engineering at Michigan State University (MSU) before graduating with a bachelor's in mechanical engineering (BSME) in 1981.

The combination of the design background prior to joining the Flight Safety Office at GE provided a distinct insight into the forces which not only created the need for the System Safety profession, but also the source of the erosion which continues to this day and is the subject of this paper.

Let it be established clearly and up front that this paper is in no way a critique or criticism of GE or any other specific organization. In fact, this paper is a testimonial of compliance to GE's stated mission statement to "advance the future of flight" by employees the freedom to advance the understanding and practice of their discipline. In my case, system safety. GE consistently encouraged and supported my interest in increasing my knowledge of system safety. I was allowed to apply my learnings to multiple engine development programs and write the design practice to be used on all future military engine development safety programs.

2) INTRODUCTION

When I was assigned to the System Safety effort for the F136 engine development program (F-35 application) provided a significant challenge to the safety team and the decision was made to create a new development safety process "from scratch" to comply with the contract requirement for a MIL-STD-882 based safety process.

In parallel, based on my IT background, the decision was made to likewise create a new hazard tracking tool (reference MIL-STD-882 Task 106).

Over the next 17 years, the process and tool were refined and integrated into the product development process. The result was not only an example of a practical aerospace application of MIL-STD-882 in the development lifecycle phase, but also a tool which greatly facilitated the process and provided a valuable resource for the operational and sustainment phases.

In doing this, appreciation was gained for the structure and content of MIL-STD-882 (then in Revision C) for the thoroughness of the design standard after hearing many criticisms and complaints regarding the loss of relevance and cumbersome aspects associated with using this standard practice document.

As word of this work began to circulate within GE, more engine development programs began to make inquiries and request assistance on their safety tasking. In addition, comments to instructors made while obtaining my System Safety Certificate at USC led to an invitation to join the program as an instructor.

As a result of this expanded exposure, many insights into the system safety profession itself were gained.

My observations are listed and described in the body of this paper for review and assessment.

The net conclusion is a high degree of concern for the health of the System Safety profession itself. It is my hope that this paper will inform and enlighten those both inside and outside the system safety profession on the state of the system safety profession and need for centralized credentialing and industry acceptance and support.

It is my further hope that individuals and organizations act on multiple levels to bring the health of their safety departments back to where they were intended to function from the very start of the modern era.

I firmly believe this will not only improve the quality of the safety efforts today but position the safety discipline for the challenges of the future.

3) What Crisis?

While it is generally understood that nothing is without risk, the quantity and frequency of high-profile safety issues in the news today have captured the public's attention and focus on the topic of safety.

High profile incidents such as.

- Challenger and Columbia Space Shuttles
- Lion Air and Ethiopian Airlines 737 Max
- Oceangate Titan Submersible
- Self-driving vehicles
- Boeing CEO testifying before Congress
- Spacex Starship explosions

And more each bears witness not only to the inherent risk of advancing technology but beg the questions around the performance of the safety process not only while in operation but what was/wasn't done in the development process.

Many factors play into the effectiveness of any safety effort. Key factors of interest to safety professional are fidelity to established safety processes and procedures as well as the qualifications of those responsible for "safeguarding" the users, operators and the public from risk of harm from these products.

The issue is that often in incident investigation and reporting, especially in high profile events, the strong desire to find the "smoking gun" root cause, which is ostensibly the goal of any investigation, can hinder a full investigation. The problem comes if the investigative focus diminishes after the first root cause is found. Not only can this potentially mask other causal sources, but unless it pushes down to where the safety process itself might have fallen short, the opportunity to learn valuable safety process lessons can be lost.

The result is that safety improvements may be found for the specific product involved in the accident, but improvements to the safety process itself, which can potentially benefit all products, are not made leaving a residual vulnerability for those products.

Since investigations do not delve into the safety process itself, the qualifications of those responsible for the safety process are rarely, if ever, addressed. Part of this is the litigious society that exists, and the love of the "blame game" that tends to result in useful information not being offered up or exposed during an investigation.

Even without this specific data, it is intrinsically understood that the higher the qualifications the better, but with a lack of centralization in the definition and certification of what constitutes a "safety expert", there is no objective gauge to assess expertise against.

The result is the potential for low quality and ineffectiveness in execution of the safety process.

From the perspective of this author, if we cannot answer these 3 questions, then I would put forth that we have a crisis in the system safety profession:

1. What is a "safety expert"?
2. What is minimum training/experience to create and oversee safety processes?
3. What should a CEO know about System Safety?

4) Where we started

The modern System Safety discipline has its roots in the post WW-II Intercontinental Ballistic Missile Program (ICBM). The emergence of a distinct System Safety discipline was discussed as early as 1947.

> *"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."*
>
> "Engineering for Safety"
> William I. Stieglitz
> September 17, 1947

Frustration with repeated launch failures for various seemingly preventable reasons led the ICBM development team to find ways to identify problems before they made it to the launch pad or test site.

The result was two major conclusions which had an immediate and positive impact:

1. The need for independent safety perspective and oversight of major product decisions.
2. The need for a proactive/predictive methodology to identify and mitigate risk as early in the design process as possible.

The basic principles were that for the first item, Engineering and Program leadership are required to balance many inputs on critical product decisions. Factors such as cost, weight, performance, operability, safety, reliability, manufacturability and others must be balanced to optimize the product. Too often it was found that the lure of potential benefits resulted in downplaying the safety risk with often disastrous results. A clear, objective and honest safety input needed to be assured in the decision-making process.

For the second item, the need for a safety process, with its own distinct discipline and skills required to define an analysis-based safety process which could identify potential risk factors as early the design process (including the conceptual phase). While many attempts at defining a safety process have occurred previously, MIL-STD-882 (originally released in 1969 – see Figure 1) provided a structured and complete safety process which could be used on a variety of Department of Defense (DoD)

MIL-STD-882 Release Dates	
Revision	**Date**
Original	Jul-69
A	Jun-77
B	Mar-84
C	Jan-93
D	Feb-00
E	May-12
E (C1)	Sep-23

Figure 1

products

While many attempts at defining a safety process had occurred previously, MIL-STD-882 provided an outline for a structured system safety process (see Figure 2) which could be used on a variety of products.

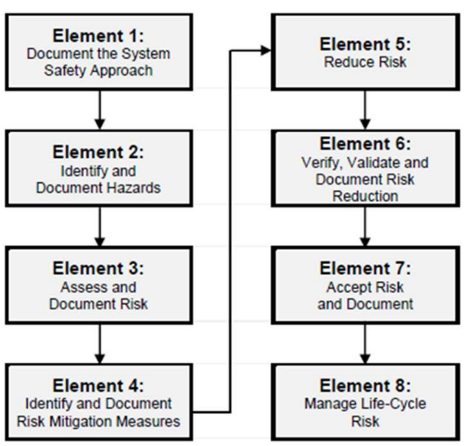

Figure 3 - MIL-STD-882 Eight Elements of the System Safety Process

The net result was the emergence of a "safety group" of individuals trained specifically to support the safety process. A parallel but separate organization to the classical engineering organizations.

> *"Safety must be designed and built into airplanes, just as are performance, stability, and structural integrity. A safety group must be just as important a part of a manufacturer's organization as a stress, aerodynamics, or a weights group...."*
>
> "Engineering for Safety"
> William I. Stieglitz
> September 17, 1947

While the connection can be debated, the 1960's and 1970's were an era of vast improvement in safety, particularly in commercial aviation (Figure 2). The analytical techniques and continued application of lessons learned combined to reduce accident rates dramatically.

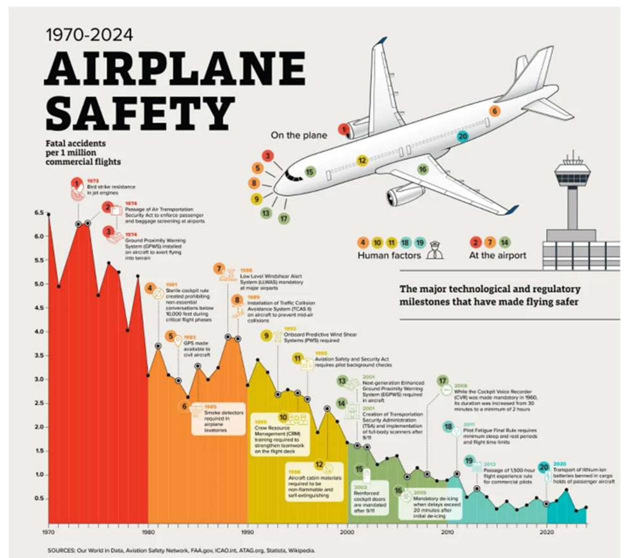

Figure 2

As early as the late 1980's though, evidence of erosion of safety discipline was becoming evident.

5) How did we get here?

On January 28, 1986, the Space Shuttle Challenger broke apart 73 seconds after liftoff, killing all seven astronauts on board. While the immediate cause of the accident was an O-ring failure and a re-design was implemented before the shuttle program resumed, digging deeper uncovered a deeper root cause.

The Roger's Commission report cited a flawed launch decision process where Allan McDonald, the director of the Space Shuttle Solid Rocket Motor Project for Morton-Thiokol, refused to sign off on the Challenger launch based on the air temperature being below a minimum (53F) they had presented to NASA before the launch. NASA pressured Thiokol to sign off on the launch and one of Thiokol's executives relented and signed off. The result was seven astronauts losing their lives.

Figure 4

This abrogation of the safety process was a clear example of "bypassing" the independent oversight function. While many changes were subsequently made to the NASA safety process, the Space Shuttle Columbia disaster 17 years later gave evidence that erosion of the safety process had occurred once again.

Figure 5

The reason for the erosion of fidelity to the safety process evidenced in the Space Shuttle accidents can be debated.

In both cases, however, concerns were raised internally prior to the accident events. The mitigating action which could have prevented the incidents was not taken resulting in the loss events.

What cannot be specifically determined is whether all critical decisions were overseen by suitably trained and experienced system safety experts in accordance with the ICBM learnings. And where in the predefined safety process did failures occur that allowed unsafe conditions to persist?

These are questions I would maintain a prudent system safety expert would focus. Without asking these questions of this accident or any accident or mishap for that matter, the opportunity to improve the safety process is missed and the vulnerability remains for the next product to be developed with it.

Causal Factors

Causal factors for erosion of the system safety function and discipline have many potential sources:

- Exodus of experienced system safety experts (burnout/retirement/death)
- Insufficiently trained/experienced safety experts can result in:
  - Lack of understanding/misapplication of system safety fundamentals
  - "Fad" approaches to safety
- Cost is King
  - Safety can be done by Engineering
  - No cost avoidance substantiation
  - 30%-50% of safety activity unplanned

> *"The evaluation of safety work in positive terms is extremely difficult. When an accident does not occur, it is impossible to prove that some particular design feature prevented it."*
>
> "Engineering for Safety"
> William I. Stieglitz
> September 17, 1947

An additional observation is that Safety Experts can be their own worst enemy. Starting from my earliest days in the System Safety profession, the hallmark of safety discussions is heated debate. Sometimes very emotional which can be defended in a profession that involves life or death decisions to be made.

Understanding this, I have observed multiple instances of "dueling safety experts" in meetings and classrooms where the underlying cause of disagreement isn't the safety process, but their differing experience with the safety process.

To my observation, two factors drive many disagreements between experts: differing Scope of Engagement and the Dunning-Kruger Effect.

Scope of Engagement

Despite the process shown on Figure 3 being applicable to virtually any safety process for any product, the conduct of the safety process itself can have unique definitions, standards, specialized analysis and skillsets for each "path" on Figure 6.

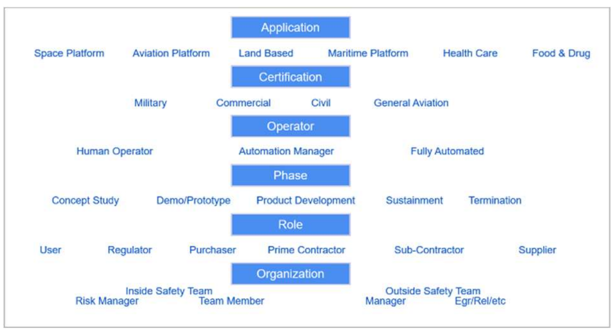

Figure 6

Understanding this discrepancy could help quell many perceived disagreements and facilitate better discussion between safety experts.

Skillset

Related to the Scope of Engagement in creating friction in system safety discussions is awareness of the differing skillsets required for the safety professional in different product lifecycle phases (Figure 7).

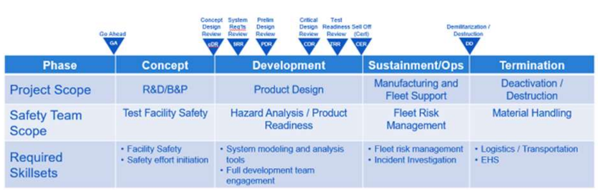

Figure 7 – Safety Skillset by Lifecycle Phase

A more specific source the Development and Operational/Sustainment Phases.

Many safety organizations operate in a "pool" environment where individuals are tasked based on availability at time of need. This is particularly evident in accident investigation response. However, with the needs of the safety department subject to availability, the same pool may need to be used to support development and sustainment safety tasking. This can be problematic if some manner of skillset progression is not included in the tasking.

Figure 8 provides a rationale for the differing skillsets required between development and sustainment safety team members.

For example, sustainment tasking does not typically require the same hazard analysis tasking (Functional Hazard Analysis, System Hazard Analysis, etc) as development. Conversely, development typically does not require accident investigation or fleet management skills.

Figure 8 – Development/Sustainment Comparison

One observation to make on Figure 8 is that within the normal progression of a product safety effort, the differences converge at regulator approval, which marks the end of the development life cycle and beginning of the operational support phase.

Dunning-Krueger Effect

This is a cognitive bias whereby an individual self-assesses their level of expertise incorrectly.

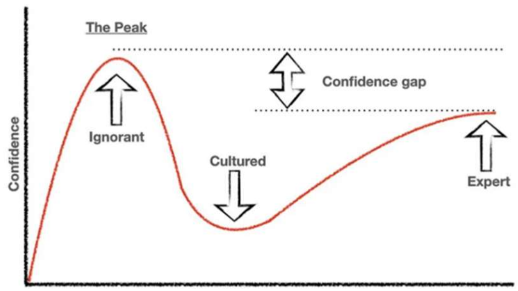

Figure 9 – Dunning-Kruger Effect

It can be problematic in two ways;

- Overestimation of competence based on limited skillset
- Underestimation of competence of highly skilled

In terms of "dueling Systems Safety experts", many times the basis of disagreement can be based simply on a newly christened safety expert being unaware or untampered by their lack of knowledge.

Awareness that expertise is strongly influenced by exposure underscores why experience must be combined with training to have better knowledge. It doesn't help that assertiveness is a required trait for many safety professionals in execution of the oversight function.

One of the hallmarks in discerning an expert's placement on the Dunning-Kruger chart is how they approach the safety tasking. Blind bureaucratic compliance to safety specifications and practices can be positive (especially in the operational phase), but it can also be a sign of a lack of understanding of system safety foundations.

Anytime safety experts disagree, no matter what the reason, it can place the teams looking for safety input in a quandary. Likewise, an insufficiently qualified safety expert can potentially undermine and/or create inefficiencies in the safety process without being aware.

The result can be confusion and/or distrust of the safety process. If the teams opt to withdraw and move towards self-reliance outside the safety team, the independent oversight function is compromised.

6) Summary

Based on the observations of over 40 years in the aerospace industry with nearly 20 years in the system safety profession, it is clear to the author there is a crisis in the system safety profession that needs to be addressed as soon as possible.

The central point of this paper is that in many cases I've observed, the System Safety function, which was originally pulled from the Systems Engineering function, has eroded back into the Engineering function, compromising independent oversight and relegating industry back to a reactive "break/fix" cycle observed in the early ICBM era.

The key reason for this erosion is the loss of system safety expertise has allowed misinterpretation and mis-application of safety standards and practices further eroding industry confidence and reliance on the foundational system safety processes and safety experts.

7) Conclusions

There needs to be a greater understanding outside the safety profession of the importance of the independent oversight function as well as engagement at the executive level to ensure the vitality and proper functioning of the safety team.

By far the biggest need is for more System Safety professionals in industry with adequate training and experience to create, conduct and oversee robust and effective safety processes which are grounded in the foundations of system safety established in the ICBM era and incorporating the lessons learned from recent events that include assessments of fidelity to the safety process established for that product.

Secondly, there needs to be consensus at a very high level on what the foundations of the system safety discipline is and some type of industry-wide recognized credentialing to provide some assurance to the industry that the fundamentals of system safety are being observed.