

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



Table of Contents

We Don't Compete on Safety	2
The DevSafe Five Laws of System Safety	3
System Safety Approaches	5
Disambiguating the "S" Word.....	6
System Safety in a Nutshell.....	8
Reliability and Safety - Fraternal Twins	10
The Unintended Competition - Engineering vs System Safety	12
How long are you planning to stay in System Safety?	14
Eyes Wide Open to Safety	16
"You get the Safety effort you pay for"	17
10 Commandments of System Safety.....	18

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



We Don't Compete on Safety



Competition is a very important aspect of a free market economy. It drives capabilities up and costs down. As a consumer, what's not to love? But there are times and places where competition takes a back seat to human compassion and concern. I believe such is the case when it comes to System Safety.

Before my retirement, I had submitted invention disclosures on software I had created to manage new product development safety programs compliant with MIL-STD-882 Task 106 Hazard Tracking Systems (HTS). Our IP department reviewed my disclosures and eventually denied processing the patent applications on the basis of an edict I had heard from our Communications Director previously; "We don't compete on safety".

While the ego aspects of adding a software patent to my list of accomplishments was a big potential plus, especially for a tool I developed from scratch and spent the better part of 17 years using and refining, I was impressed by the fact that I now had a first hand example of how my employer "walked the talk" for safety. Further, they fully supported my participation (and other employees) in teaching safety related courses at the University of Southern California. Even to students who represented competing organizations. Knowing I had my employers support to share my knowledge and experience was inspiring.

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



I was reminded of this by the recent Boston Marathon, where one participant reached 26.1 out of 26.2 miles and his body began to shut down. He hit the ground in view of the finish line. Out of compassion, 2 fellow runners scooped him to his feet and helped him finish the last 0.1 miles. As a five-time finisher of the Boston Marathon, I know participation here is a "Mt. Everest" scale lifetime achievement for most people. The bib numbers of the helpers (less than 3000) told you they were fast competitive runners. But at that moment, they were no longer competitors but fellow humans who fully understood their common goal and stopped to help this runner to achieve his. Together. I get emotional viewing the photos.

It takes an enlightened view of progress to recognize and support areas where we compete and don't compete. The benefit of System Safety cooperation between organizations, even competing ones, should be acknowledged and supported by every organization.

Because at the end of the day, we're all in this together.

The DevSafe Five Laws of System Safety



0th Law - The consequence of violating any of the System Safety laws defaults to a reactive (after the fact) System Safety Management approach to the degree of the deviation.

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



1st Law - 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 (before the fact) Safety Management approach.

2nd Law - 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.

3rd Law - The fundamental skillset of a System Safety expert is the ability to conduct safety analysis of products/processes in order to establish hazards and risk causal scenarios which allows safety risk to be assessed relative to established system safety risk acceptance criteria.

4th Law - The fundamental capability 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.

5th Law - 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.

Other LinkedIn Articles

TJ Candy – DevSafe Consulting

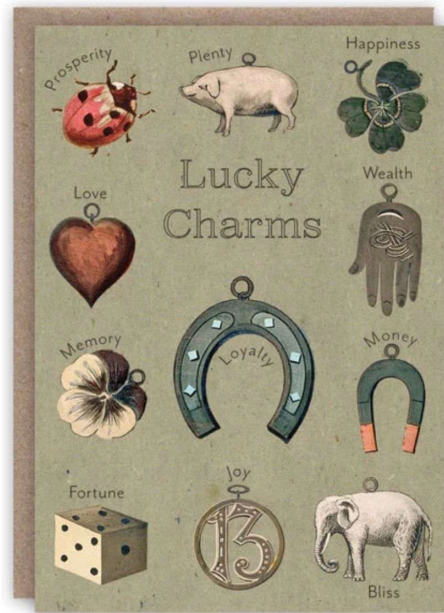


System Safety Approaches

Prior to the formation of the modern (post-WWII) system safety discipline, safety risk management relied primarily on three things;

- 1) Avoiding past mistakes (reactive "after the fact" risk management approach)
- 2) The competence of the engineering staff
- 3) Luck

The primary goal of modern system safety discipline is to prevent mishaps before they occur



(proactive/predictive risk management approach).

To the extent defects exist in either the content or execution of the system safety process and/or the capabilities of the safety practitioner(s) providing its oversight is the extent to which product safety performance returns to the earlier era.

It's as simple as that.

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



Disambiguating the "S" Word



Safety

A word with great power. At its mention, one can get people's attention, bring sweeping change, or even stop things in their tracks. Wielding the "s" word can be like swinging a "sword" (word play intended). Bringing great power to the bearer. And with great power comes great responsibility. The truth is that safety is more like a Swiss Army Knife than Excalibur.

In the hands of a true safety expert, this word can cut through bias, posturing and even inexperience to support a more focused and informed decision-making process. In the wrong hands, it can be abused for nefarious purposes, create inefficiencies or even mislead the decision-making process.

Understanding the many facets and domains of safety helps interpret what is heard from safety experts (including myself!) speaking to the world. This can help determine what to accept and know when they have departed from their "swim lane". Potentially start clashing with safety experts swimming in the other direction.

For this reason, there is a need to be keenly aware of these differences in the context of any safety discussion. For example, I have heard organizations including both System Safety and Environmental Safety (EHS) without sufficient disambiguation in high level safety discussions leading people to bring System Safety issues to EHS and vice-versa.

They have similar but distinct processes, standards, training and acronyms. And if these safety experts aren't sufficiently trained/experienced and take on cross-tasking, serious problems can

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



result. Anyone who has taken on home electrical or plumbing jobs instead of calling in a pro can attest to the quality and confidence difference.

Some general descriptions of the "blades" in the Safety knife;

- System Safety - Structured approach to hazard identification, risk assessment and corrective action verification
- Functional Safety - System safety concepts applied to sub-systems or subfunctions
- 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
- Operational Safety - Compliance to established safety guidance

Some disciplines which are distinct but have ties to System Safety;

- Human Factors
- Reliability
- Cybersecurity
- Survivability

Each of these "blades" and disciplines are best undertaken by experts specifically trained and experienced in the distinct forms of analysis needed, sometimes unique to the product and/or lifecycle phase. Use of the wrong "blade" can potentially create more harm than good.

So, when you hear some expert (including me!) speaking on the subject of safety, it is good to have some context or some band-aids close by.

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



System Safety in a Nutshell



The historical foundational principle of the System Safety discipline is to provide independent oversight of critical product design decisions and processes as early in the product lifecycle as possible to eliminate or reduce exposure to undesirable loss events.

The primary discipline of System Safety is the oversight of the conduct of a System Safety process created using established best safety practices and industry standards tailored to the specific product.

The System Safety process should engage all levels of management and all subject matter experts and support teams as appropriate.

The scope of System Safety is safety risk management throughout the operation and intended functioning of the product throughout all stages of the product lifecycle; from initial concept, design, regulatory approval and use through product termination.

There are three fundamental approaches to safety risk management:

1. Predictive - The identification of safety hazards through analysis, their cause(s) and risk reduction actions prior to a loss event occurring.
2. Proactive - The examination of product usage information to identify risk reduction actions prior to a loss event occurring.
3. Reactive - The examination of a loss event and help identify action(s) necessary to preclude a recurrence (default safety management approach).

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



The core activities of the System Safety process are:

1. Identification of risk reduction action(s) necessary to meet established product safety goals.
2. Conduct safety assessments as needed to support product decision making process.
3. Providing documentation verifying implementation of any necessary hardware and software action(s) to a regulatory function.
4. Conducting periodic audits as needed to assure effectiveness and ongoing compliance to established safety actions.

The System Safety Practitioner must be knowledgeable and skilled in all appropriate safety analysis techniques commensurate with the application, intended operation and lifecycle phase of the product. This is best accomplished by engaging trained, experienced and certified System Safety Professionals who operate organizationally independent of the product engineering function. The practitioner should maintain professional currency through ongoing training and regular interaction with fellow safety professionals.

The degree to which the above system safety process/actions are not engaged is the degree of reliance on a reactive system safety risk management approach.

Do you agree? Or am I off my nut?

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



Reliability and Safety - Fraternal Twins



My wife has a fraternal twin sister that is 2" shorter and has different hair color. My wife's father had an identical twin. So much so that the minister had to warn everyone at the start of his funeral service that his twin brother and not the deceased was about to walk into the church. There was still a large gasp when he walked in!

Many people regard System Safety and Reliability as identical twins. But in actuality, they're more like fraternal twins - a lot of similarities, but the core skillsets are distinct (but closely related).

For example, System Safety doesn't mind redundancy while Reliability favors a more reliable part for a lower part count. While it varies from company to company, many organizations issue FMECAs from Reliability while System Safety tackles FHA, SHA, etc. This delineation allows Reliability to focus on individual parts while System Safety looks from the systems perspective. Which makes sense as the modern System Safety process was initially carved out from the Systems Engineering function.

Many organizations even put them in the same department, but if no distinction in expectations is made between System Safety and Reliability personnel, then inefficiencies and serious risk management problems can result.

I've always maintained that a poor reliability effort can undermine even the most robust safety

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



process. Conversely, a poorly executed safety process can dull the most meticulous reliability effort.

Returning from one of my early System Safety classes at USC with this perspective, I met with my Reliability lead for our program and told him I needed to bring him flowers and chocolates every day. I told him Reliability was the "wind beneath my safety wings". I didn't want to do the things he was doing and he didn't want to do what I was doing. A happy family!

It's understood that they're closely related. Reliability issues can impact safety, but so can Quality and Manufacturing issues. Same with Human Factors, Cybersecurity, Survivability and even AI. But all these areas should have distinct intrinsic processes to stop these types of issues from becoming safety issues.

Software reliability and safety have parallels with hardware, but the industry is still struggling to make the distinctions. As with hardware, System Safety handles critical function definition, safety requirement and testing rigor establishment. The effort to assure the hardware or software reliably does what safety requires it to do should fall to the reliability realm.

As products and processes become more complex and difficult to risk manage, proper alignment of oversight resources is key. Knowing the distinction between skillsets and tasking personnel accordingly may create turf wars and animosity between different program departments, but in the end, it's All in Family.

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



The Unintended Competition - Engineering vs System Safety



Having multiple decades of experience in both aerospace engineering and system safety, as well as training hundreds of safety professionals as a System Safety certification instructor, I feel I'm in a unique position to make a generalized industry-wide observation that I've had from sitting in both corners.

The competition between Engineering and System Safety.

While conflict is part and parcel to working in the high-stakes technical product development arena, I've experienced and heard everything from gentle smiling jabs to out-and-out verbal haymakers being thrown by engineering and safety people in meeting rooms, classrooms and video screens. Not what the founders of the modern system safety approach intended.

It's not a mean-spirited competition but what I maintain is a slowly evolving difference of interpretation of what system safety is and is supposed to be doing. This difference has resulted in a divergence from what I believe was the original intent, program decision oversight by independent safety professionals early in the design process.

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



Looking back on history, it's not hard to see how a rift could occur. The adage "nobody is happy to see Safety" comes from the part of human nature that doesn't like people looking over their shoulders or being judged. But the post-WWII ICBM development found it to be essential in assuring adequate safety consideration in critical design decisions.

Today, the most common place this battle is fought is when engineering decides "when do we bring in the safety team?". While every good organization has a safety policy which directs when the safety team is engaged, it's usually left to engineering/project discretion on when to bring the safety team in. The decision can be based on many valid factors, program scale and funding, program or data security, and even bad past safety team experiences or an inexperienced or untrusted safety team.

The high technical competence and self-reliance of most engineers often leads to the conclusion they can do safety work on par with a safety professional. I know that's how I felt in my engineering career phase. I even came into my first safety review of my hardware with a strong defensive posture. I felt I understood safety intrinsically and my superior technical qualifications were being challenged and judged. I didn't fully appreciate the "help" of objective oversight at that time.

Turning competition into co-existence is going to take role calibration and enlightened leadership that accepts the foundational truths of the origins of system safety. Assuring that the safety team is a cadre of suitably trained and experienced safety professionals ready to take on today's challenges as well as the even larger challenges on the immediate horizon.

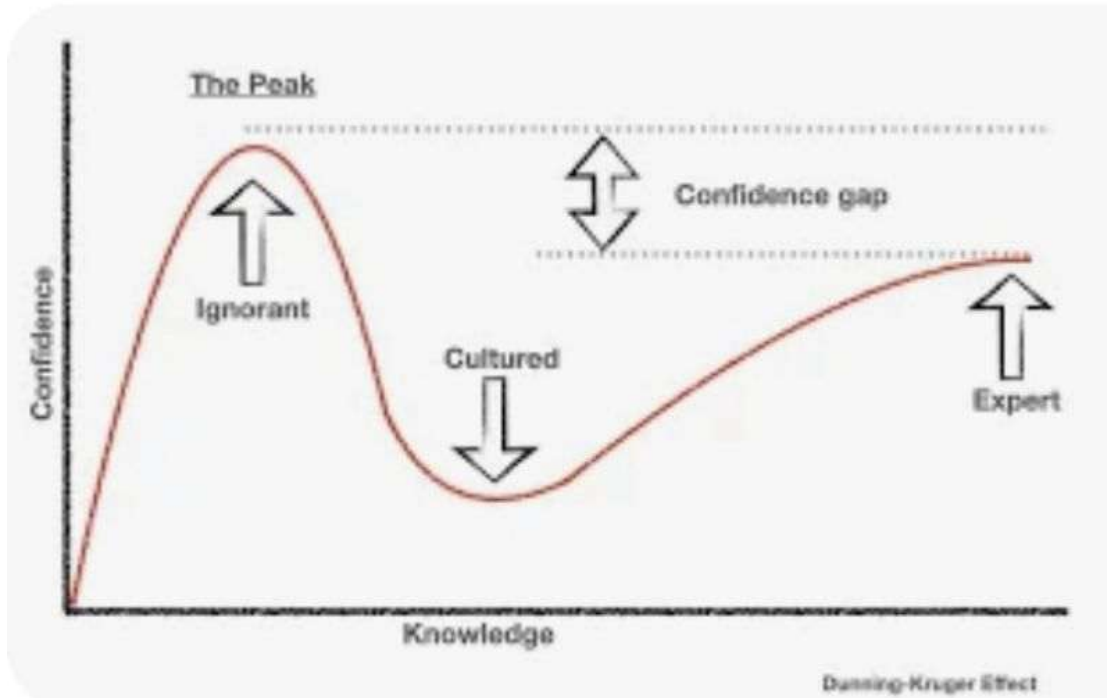
And leaving the boxing ring behind.

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



How long are you planning to stay in System Safety?



About halfway through my 43 year aerospace engineering career, I decided to act on my interest and apply for an opening in the Flight Safety Office.

One of my interviewers was someone who eventually became Vice President of Engineering at the large aerospace company I worked for. She even put the phrase "every engineer is a safety engineer" on posters throughout the plant.

During the interview, she asked, "How long are you planning on staying in safety?". "The rest of my career", I sincerely replied. Her response was fast and blunt. "Good, because it's going to take 10 years to get what we need out of you".

She was clearly not looking for a "3 and out" person to join the safety team. She must have known Dunning-Kruger effect is real and applies to Safety. And for the record, I did eventually join the FSO and retire from there nearly 20 years later.

But that blunt interview statement stayed with me for the rest of my career and into my time as system safety certification instructor at the University of Southern California. The fundamental truth of the "10 year pipeline" has been underscored time and again as I get

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



exposed to a wider and wider range of organizations and individuals from around the world taking the class.

Safety is different from other technical disciplines. It requires a higher level of commitment on the part of both the individual and the organization to achieve the needed competency than in other technical disciplines.

Not enough training or experience and the associated safety effort is vulnerable to leaving risk "on the table", particularly during the product development phase. Risk that can make it into the marketplace and potentially cause mishaps.

As industry grapples today with a myriad of safety issues, time and again, post-accident investigations uncover root causes that are fundamentally failures to follow historically validated safety processes and practices.

Could it be that the loss of oversight (which is a fundamental tasking of the safety profession) by suitably trained and experienced safety professionals is a factor in any of these events?

In world looking for fast and cheap answers, it might be time for all of industry to recognize that creating safety experts is neither.

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



Eyes Wide Open to Safety



Before my retirement, I was sitting in an "all hands" leadership status meeting for a large military product development effort. All associated engineering and technical teams were represented.

When the time came to talk about Safety (as all good companies do), the Engineering Manager included in his comments that he wanted the entire team to be "eyes wide open" to safety.

Wow. As the safety lead for the program, I was immediately struck by the profound clarity provided by this short statement. It clearly captured an attitude of focus and intention that I believe should be the vision for any system safety effort.

The primary lesson learned from the post-WWII ICBM development effort of the 50's and 60's was that independent safety oversight was needed on all critical product development decisions. As early in the design process as possible. The actions that followed led to the modern approach to system safety that is captured in MIL-STD-882 as well as other safety standards and practices.

The Engineering Manager's short statement cast a vision for an honest "no squinting, no shading, no ignoring" view of the safety story in every product decision.

This vision, combined with a thorough and prudent safety process designed and overseen by a capable product safety team that is organizationally independent of product leadership, helps to provide a light to where that eagle-eyed vision should be applied.

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



I believe the founding members of the modern system safety profession would applaud that vision.

I also believe that the key to addressing many of the safety challenges facing industry today is to recognize where we have deviated from the system safety lessons learned in the past. This includes fidelity to the safety process that brought incredible improvements in aviation safety in the 70's and early 80's.

Put it all together and the results can be, well, eye-opening.

"You get the Safety effort you pay for"



A while back I did a LinkedIn series of posts on some of the great quotes that influenced my career in system safety.

This particular quote came from my friend and system safety mentor, KC Wilson, when we were talking about product safety performance and how one fielded product line maintained a mishap rate very close to the target rate threshold. The bottom line was that adequate funding was being provided to analyze options and implement safety corrective actions as they were needed.

The cost of implementing safety corrective actions on a fielded product can vary greatly. Actions can be as simple as an inspection or as complex as introducing a redesigned part to an active fleet. For the latter, if cost considerations cause delays or the changes aren't fully implemented, the accident rate will most likely go up. Simple as that.

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



On product development programs, depending on when in the design cycle corrective actions are determined, even complex design changes may be implemented relatively easily and affordably. This is especially true if actions are identified before the design is finalized.

But the task of analyzing complex systems for safety during product development; reviewing data, determining hazards and establishing corrective actions can be a significant cost in terms of time and money. The later in the product development cycle, the greater the potential complexity and subsequent cost of implementing these actions.

It takes an organization with an enlightened senior leadership that fully accepts KC's statement as true to assure that the system safety effort is adequately staffed and funded to do its job from the very start.

The cost of funding a robust and thorough development system safety effort is significant. But the cost of funding an operational product safety effort that has to deal with issues that weren't found during the development phase is greater. Not to mention the potentially high cost of loss events.

A corollary to KC's quote could be "Paying for safety earlier is better than paying more for safety later".

10 Commandments of System Safety

- 1) Thou shall have a Safety Department, separate and distinct from Engineering and Program Management
- 2) Thou shall have no false Safety experts before thee
- 3) Thou shall abide regular Safety Working Group meetings and keep them wholly functioning on all program levels
- 4) Thou shall bid thy Safety Department to construct a safety program in its earliest stages to raise the product in the path of righteous safety specifications
- 5) Thou shall honor thy lessons learned and do not constrain thy Safety Department from keeping vigilance over current events
- 6) Thou shall not murder Safety Department input to trade studies nor ask them while walking into

Other LinkedIn Articles

TJ Candy – DevSafe Consulting



the change decision meeting

7) Engineering shall not covet thy Safety Department budget nor steal from the Safety Team to feed other departments

8) Thou shall encourage thy Safety Department to commune with all thy systems neighbors Safety Departments that all may prosper in the lands

9) Thou shall place qualitative probabilities over quantitative probability in the early stages of thy Safety Department assessments

10) Thou shall faithfully engage thy Safety Department through all stages of thy products lifecycle

Do this and it will be well with you. From a safety perspective, anyway.