System Safety – A Profession in Crisis

TJ Candy
DevSafe Consulting, LLC

“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 I. Stieglitz
“Engineering for Safety”
September 17, 1947

System Safety – A Profession in Crisis

Observations based on 43 years in the Aerospace industry as both a design engineer and safety professional and 4 years teaching System Safety Certification Course at University of Southern California

Commonality noted across companies, industries, countries, and product types which indicate an erosion in the System Safety Profession from its origins in the ballistic missile era.

Are current safety issues evidence of erosion from these origins?

Who/What/Where/How questions with explanations

Agenda

Who is TJ Candy?

What crisis?

Where we started

How did we get here?

Summary/Conclusions

Who is TJ Candy?

- Bachelors in Mechanical Engineering – Michigan State University – 1981
- 43-year career in Aerospace engineering
  - GE Aerospace – 34 years
  - Ex-Cell-O (now Woodward) – 6 years
  - Bendix (now Honeywell) – 3 years
- Primary engagement in military gas turbine industry
  - Design/Systems Engineer – 20 years (1 patent!)
  - Information Technology – 4 years
  - System Safety – 19 years
- System Safety Certificate – USC Aviation Safety & Security Program – April 2016
- USC Safety Certification Instructor since October 2021
- Retired System Safety Controlled Title Holder - April 2024
- Manager of DevSafe Consulting, LLC since 2024

Who is TJ Candy? - Explanation #1

System Safety Exposure

- Joined GE Aerospace FSO in 2003
- Gas turbine product development and support
  - F110 Product Support
  - JSF/XA100 (F-35) development
  - T901 (Blackhawk/Apache)
  - Advised numerous advanced engine development programs
  - Wrote military system safety design practice currently in use
- USC Certification Instructor
  - System Safety Course (SSC)
  - Advanced System Safety (ADVSS) – new assignment

USC Student Breakdown *

Student Breakdown	
US	68%
Non-US	32%

	Country
1	Australia
2	Brazil
3	Canada
4	Germany
5	Hungary
6	Italy
7	Mexico
8	Netherlands
9	Nigeria
10	Singapore
11	South Korea
12	USA

	Company
1	Australian Submarine Agency
2	Boeing
3	Brazilian Air Force
4	Certified Aviation Services
5	Embraer
6	FAA
7	GE Aerospace
8	General Atomics Aerotec Systems
9	Honeywell
10	Hungary Ministry of Defence
11	Italian Air Force
12	Lockheed Martin Aeronautics Co.
13	Martin Solutions, LLC
14	NASA
15	Nigerian Civil Aviation Authority
16	Northrop Grumman
17	Republic of Korea Air Force
18	Republic of Singapore Air Force
19	Royal Netherlands Air Force
20	RTX (Raytheon, Collins, Pratt & Whitney)
21	Singapore Ministry of Defence
22	US Air Force
23	US Army
24	US Navy
25	US Space Force

** 156 students to date*

Who is TJ Candy? - Explanation #2

- Combination of training and experiences has provided a unique insight into the System Safety profession – primarily in product development phase
- Extended assignment duration in development safety (~17 years) led to clearer understanding of MIL-STD-882 safety process/intent
- Common positive response from people exposed to system and USC students
- Wrote GE Aerospace standard practice for military development safety process prior to retirement – used on multiple advanced development programs
- Background in IT allowed for creation of robust software tool also used on multiple advanced development programs
- Experience, news stories and student interactions seem to show common global thread in how System Safety is functioning

What Crisis?

High-profile events

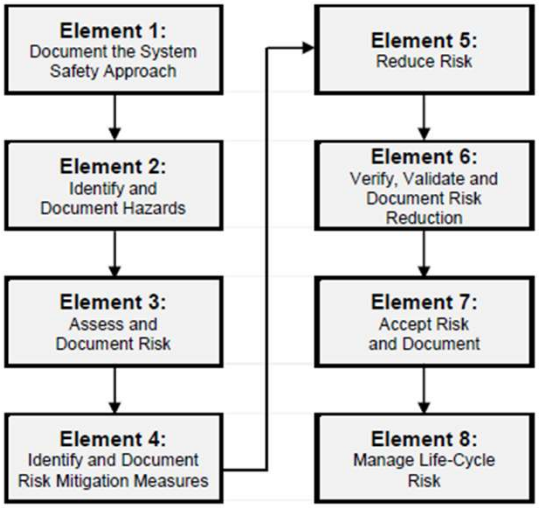
- Shuttle accidents
- 737 Max
- Oceangate Titan Submersible
- Spacex “RUD” events
- Self-driving vehicles
- Boeing CEO before Congress
- More….

What Crisis? – Explanation #1

- “Accidents will happen”, but are established safety processes being followed?
- System Safety team often engaged later in design process
- “10-year rule” – training + experience (poaching problem)
- “The great thing about safety standards is that there’s so many to choose from”
- Higher reliance on bureaucratic/regulatory compliance than observing “the fundamentals” of system safety
- Software/Safety open questions (LOR harmonization)
- Role of C-Suite in System Safety
- “Safety Expert” definition
- Safety discipline being subsumed back into engineering at the expense of “independent oversight” – higher residual risk

What Crisis? – Explanation #2

- "Deep diving" MIL-STD-882 uncovered "physics of system safety"
  - The how's and why's of the 100-400 series tasks – 200 series is not exhaustive!
  - Process "tailoring" to the specific product is required
  - The central role the hazard tracking tool plays in facilitating the safety process
- Discussions with fellow safety experts
  - Credentials of safety team members varied – severely understaffed/undertrained
  - Safety engagement subject to engineering direction/funding
  - Safety team brought in late to issues – options limited
- Review of publicly available resources of mishap events led to questions
  - How was the safety team engaged?
  - Was the safety process followed rigorously?
- Cases presented by USC students



Eight elements of the system safety process
MIL-STD-882 Figure 1

What Crisis – Explanation #3

- Current safety-related events regularly indicating known field safety practices not being followed
- Many investigations do not look at failures in the safety process itself after root cause hardware/software failures identified
- Reduced visibility to safety process malfunction during the product development process
- Safety teams constantly operating in “triage” mode – little/no time for training/collaboration

Open Questions

- What is a “safety expert”?
- What is minimum training/experience to create and oversee safety processes?
- What should a CEO know about System Safety and engage with the safety team?

If we can’t answer these questions, we have a crisis

Where we started

- Modern system safety process emanates from learnings of the ICBM development of the 1950's and 60's
  - Basis in emerging General Systems Theory of 1940's
  - Independent safety oversight of critical design decisions needed as early in the design process as possible
  - Need for systematic proactive/predictive approach to safety rather than reactive
- Led to creation of MIL-STD-882 which focused on planning and executing a structured, robust and thorough system safety process as early in the design process as possible

Where we started – Explanation #2

- Vast improvements in safety beginning in the 1960's
- Leveling off in more recent decades

How did we get here?

- System Safety as an approach and profession has eroded slowly over the past few decades
- Loss of oversight - the Safety function is being subsumed back into the Engineering function
  - Engineering directed engagement and funding of safety team
  - Heavier reliance on compliance to existing standards/procedures – vulnerable to new
- Decreased dependence on trained and experienced System Safety professionals
  - Less proactive/predictive hazard detection
  - Lack of centralized certification for System Safety professionals
  - Lack of understanding of “10-year rule” in establishing training pipeline
  - Safety professional in-fighting (“dueling safety experts”)

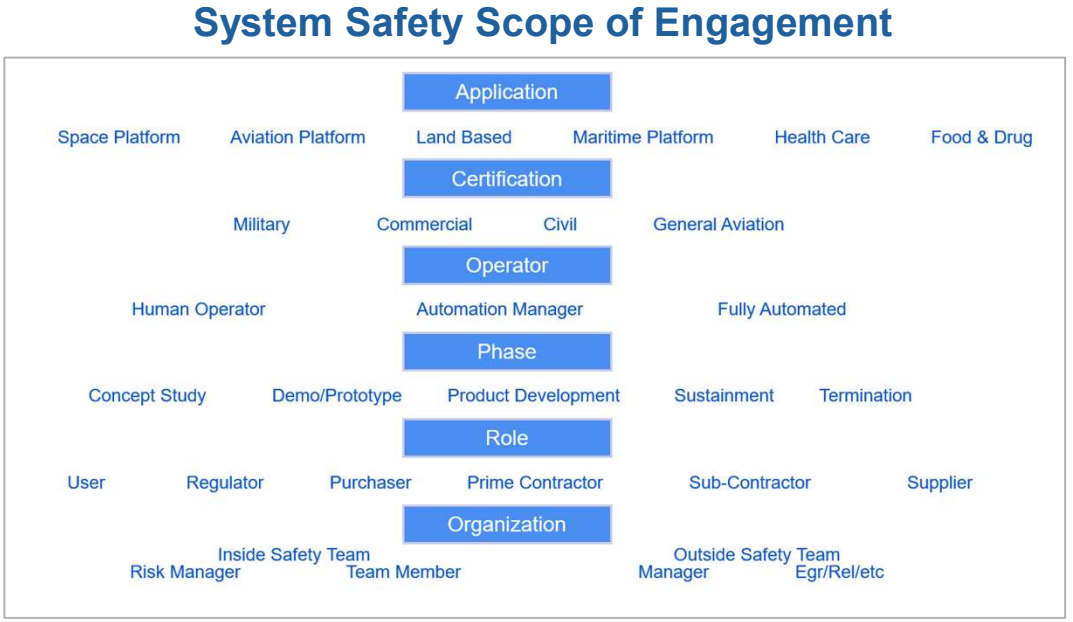
How did we get here? – Explanation #1

- Exodus of “founding” System Safety experts
- Erosion of understanding of system safety fundamentals/oversight
- Insufficiently trained and/or experienced safety representation can be grossly inefficient (“fad” approaches) and result in high residual product safety risk
- Cost is King
  - System Safety seen as duplication of Systems Engineering
  - Engineering can do Safety as well as the Safety team
  - Cost avoidance is not allowed as substantiation for Safety Team engagement/staffing
  - 30%-50% of safety effort is unplanned reaction – Staffing to plan is understaffing
- Difficult to prove accidents prevented/cost avoided

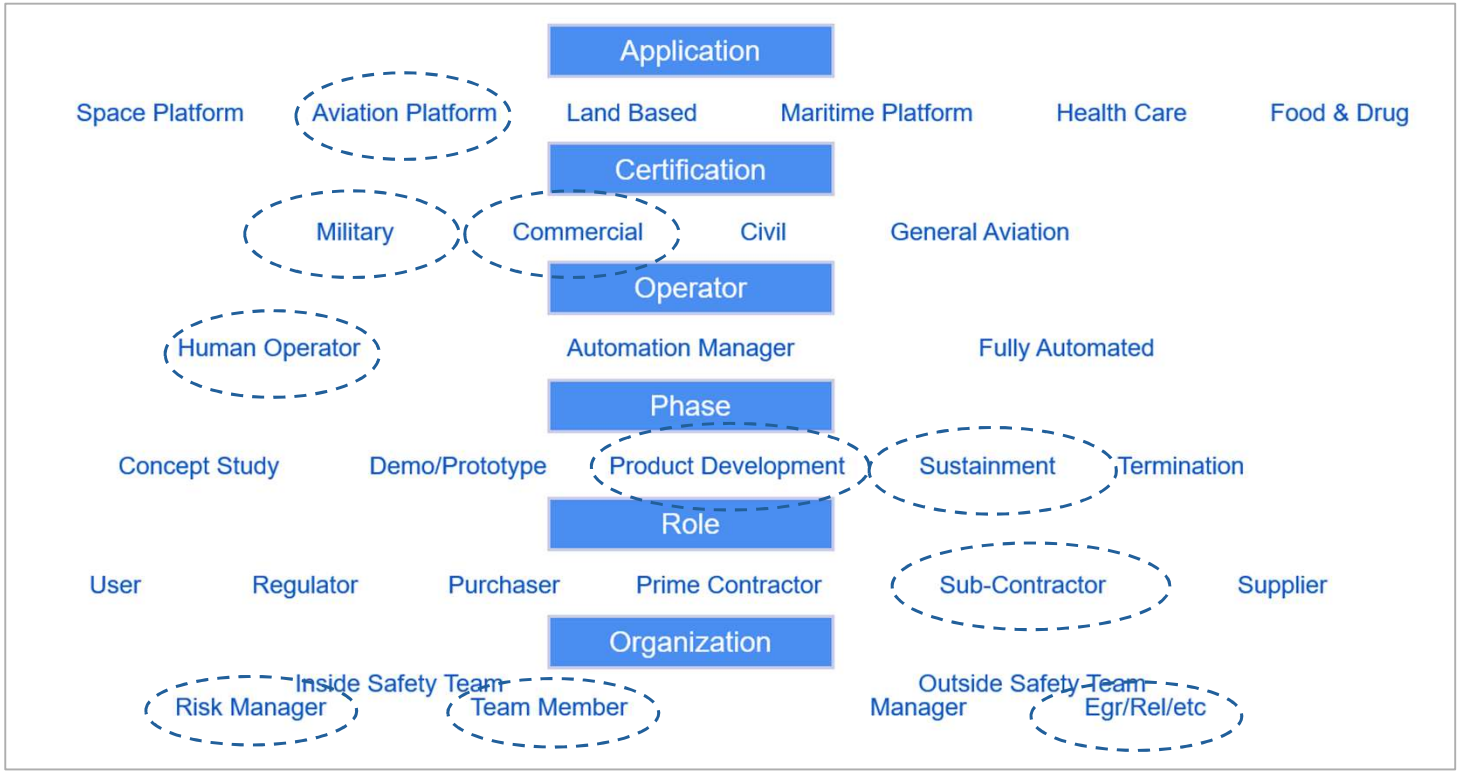
  If leadership sincerely believed that the System Safety process works and avoids loss events, then funding the System Safety team would never be an issue
- Safety professionals can be their own worst enemy

How did we get here? – Explanation #2

- Safety expertise strongly influenced by their experience/exposure
- Very similar high-level safety process
- Each “path” can have unique definitions, acronyms, standards, specialized sub-processes and skillsets for system safety
- Can be source of perceived disagreement/infighting between “experts”



TJ Candy – Scope of Engagement (Bonus Feature)



How did we get here? – Explanation #3

- System Safety required skillsets vary within product lifecycle phases
- Each phase requires unique training and proficiencies
- Generally not recognized in industry

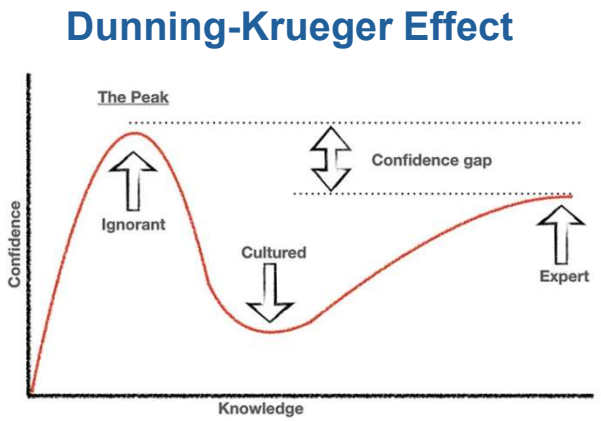
Phase	Concept	Development	Sustainment/Ops	Termination
Project Scope	R&D/B&P	Product Design	Manufacturing and Fleet Support	Deactivation / Destruction
Safety Team Scope	Test Facility Safety	Hazard Analysis / Product Readiness	Fleet Risk Management	Material Handling
Required Skillsets	• Facility Safety • Safety effort initiation	• System modeling and analysis tools • Full development team engagement	• Fleet risk management • Incident Investigation	• Logistics / Transportation • EHS

System Safety Skillset Comparison

Development and Operation/Sustainment Comparison

How did we get here? – Explanation #4

- High-level misinterpretation of system safety
  - Bureaucratic “check the box” approach
  - System Safety skillset intrinsic within Engineering discipline
  - System Safety and EHS are alike
- “Safety Expert” as a relative term
  - Dunning-Krueger Effect
    - Cognitive Bias
      - Overestimation of competence based on limited skillset
      - Underestimation of competence of highly skilled
    - Hard to distinguish difference
  - “Swim Lanes” of expertise (previous chart)



Who/What/Where/How Summary

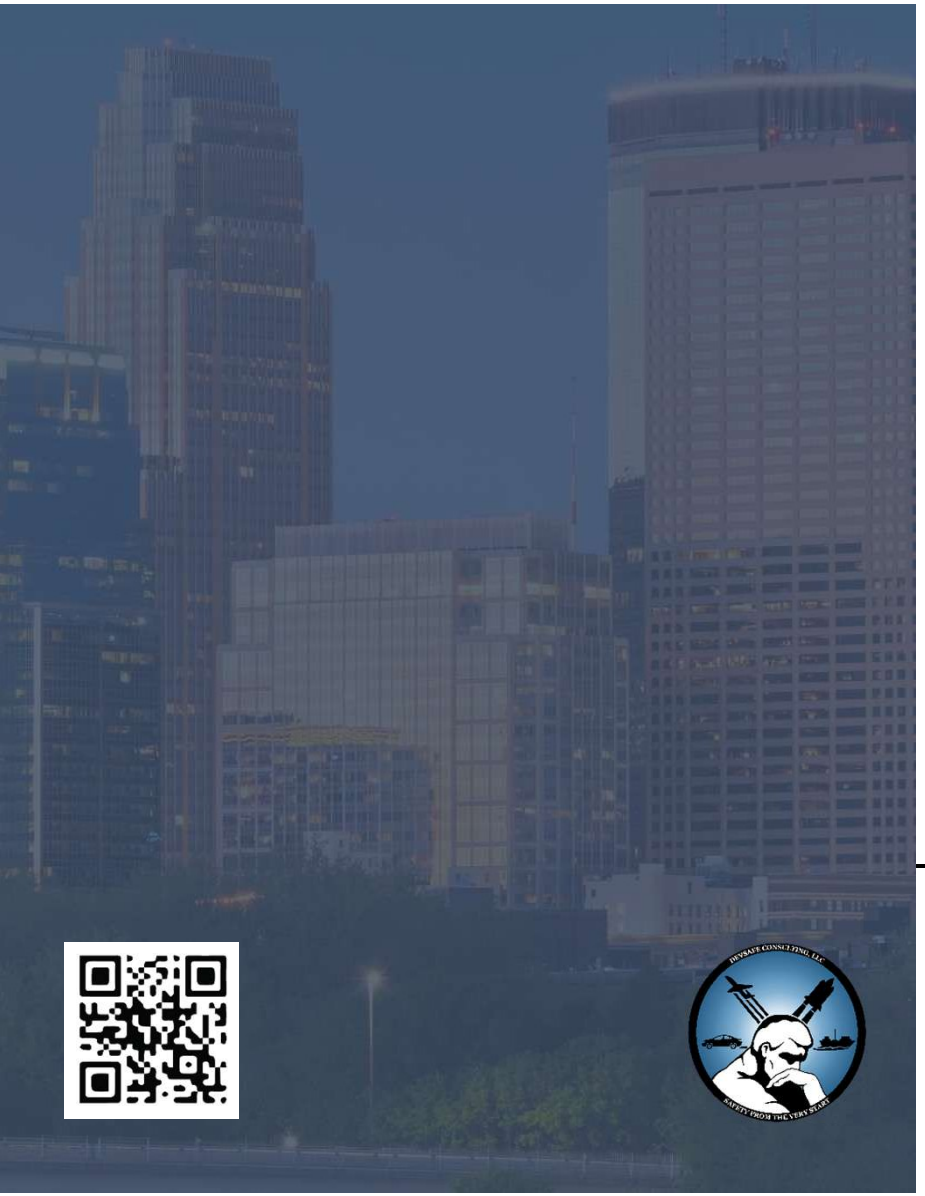
- Events since 1980's indicate an ongoing erosion of fidelity to the System Safety process formulated post WWII and implemented in the 1960's and 70's
- System safety function less independent of Engineering function
  - Lack of accepted and common required safety standards and credentialing for safety professionals
  - Blind compliance to safety standards and processes
  - Safety team engaged "as needed" – often later in design process
  - Reduction in Safety experts with fundamental system safety understanding

Conclusions

- The System Safety profession is in a crisis mode
- Needed within the system safety profession
  - Concurrence needed on system safety fundamentals, establishing centralized credentialing for safety professionals
  - Career progression based on Training + Experience
  - “Convince yourself it’s safe first” approach – not blind compliance
  - Quit fighting with one another
- Needed from industry leaders
  - Independent oversight is chartered and being dutifully conducted by safety team
  - Assure Safety teams are being engaged early in the design process
  - Health/vitality monitoring of their safety team (experience/training/tasking)

“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....”

William I. Stieglitz
“Engineering for Safety”
September 17, 1947



Summary Conclusion

The System Safety profession is operating in a crisis mode globally.

The path ahead requires both concurrence and action both within the System Safety profession as well as industry leaders

Until then, the industry will continue to see “knowable” safety hazards released to the marketplace

Contact

TJ Candy

Tj.candy@devsafeconsulting.com

https://devsafeconsulting.com

LinkedIn (Anthony Candy)

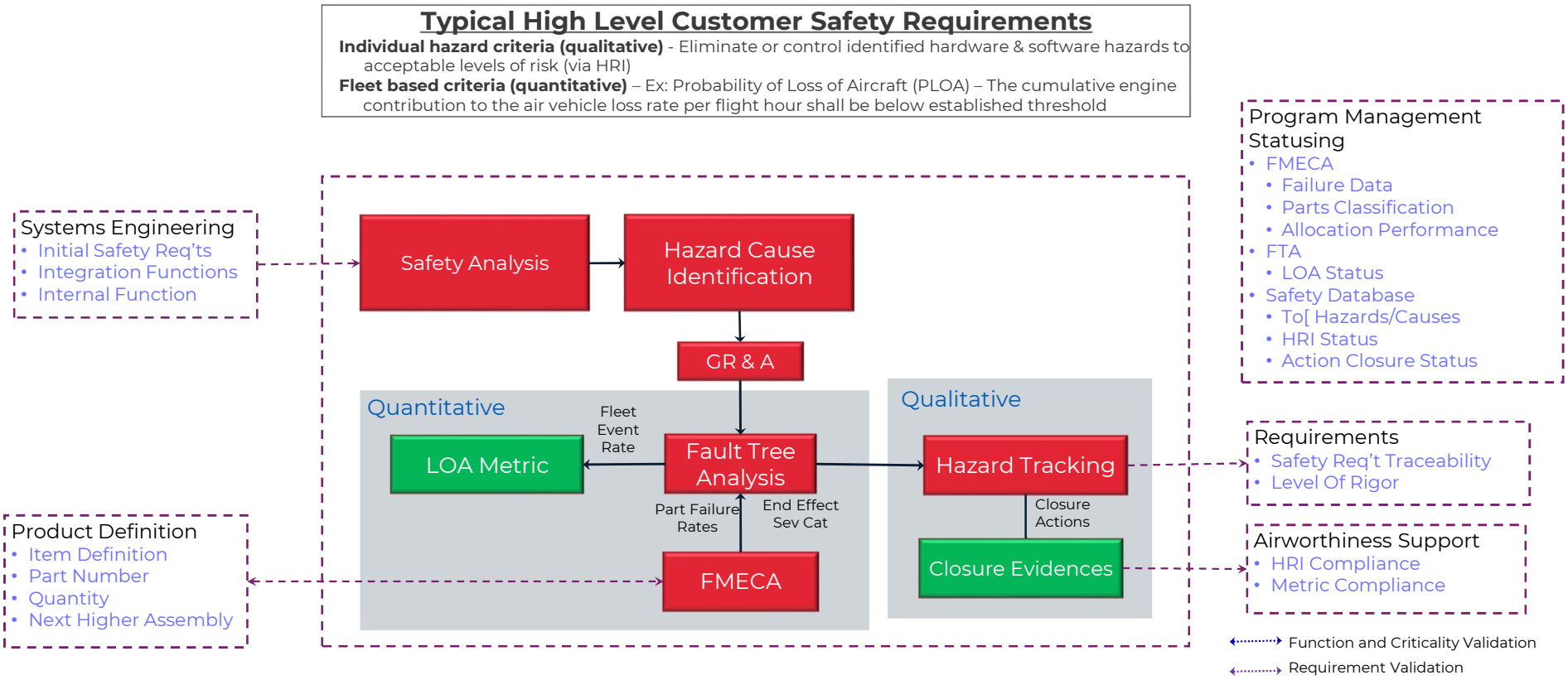
Backup Slides

Hazard Identification Methods

Hazard Existence	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), SME engagement, open reporting
Unknown	Unknowable	Opportunistic Inspection (Fleet Leader), Analytics, Trial & Error (break/fix)

The System Safety process focuses on assuring all “knowable” hazards are identified and subjected to the safety process

Sample Development Safety Process Overview



System Safety Ugly Truths

- Very few people are truly happy to see a safety professional
- A well organized and funded safety effort can have the same outcome as a lucky program
- When safety works right… nothing happens
- 30-50% of Safety team activities are unplanned responses to events
- All safety meetings are working group meetings