Introduction to Aerospace Network Certification §/JAR25.1309 / CS25

Jamie Zaehring
Associate Technical Fellow – SME in Deterministic Networks and Integrated Modular Avionics
Boeing Commercial Airplanes
10 March, 2021

Agenda

- List of Significant Certification Guidance Documents
- 25.1309
  - History,
  - Hazard classification levels, and
  - Relevant excerpts from 25.1309
- Functional Hazard Assessment examples
- Examples of compliant System Design and Fault Tree
- Summary/Conclusion

Aerospace Certification Documents are many…

- Design Assurance
  - DO-178C (Software)
  - DO-254B (Hardware)
- Development Assurance
  - ARP4754A – Guidelines for Development of Civil Aircraft and Systems
- DO-297 – Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations
- DO-330 – Software Tool Qualification Considerations
- Safety
  - ARP4761 – Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems…
  - AC25.13091A – FAA Advisory Circular - System Design and Analysis

Today let's delve into the safety regulations of FAA §/JAR25.1309 and EASA CS-25, and the guidance provided by AC25.1309 Arsenal.

AC25.1309 History

- FAA AC25.1309-1A current guidance was released in 1988, and provides compliance suggestions for showing an airplane and system design is safe.
- In 1996, a Systems design and analysis working group submitted an updated draft referred to as the ‘Arsenal Draft’ that has since been the defacto working standard (despite being a draft).
- European Union Aviation Safety Agency (EASA) has an equivalent (non-conflicting) regulation CS25, which is regularly updated through amendments.
- In 2020, CS25 Amendment 24 was released (heavily reviewed and contributed to by aerospace industry and regulators (including FAA))
- This presentation uses the Arsenal Draft to introduce aerospace safety certification guidance. It can be found here:
- https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/TAEsdaT2-5241996.pdf

Terms and Definitions

- a. Analysis. The terms "analysis" and "assessment" are used throughout. Each has a broad definition and the two terms are to some extent interchangeable. However, the term analysis generally implies a more specific, more detailed evaluation, while the term assessment may be a more general or broader evaluation but may include one or more types of analysis. In practice, the meaning comes from the specific application, e.g., fault tree analysis, Markov analysis, Preliminary System Safety Assessment, etc.

- b. Assessment. See the definition of analysis above.

- c. Average Probability Per Flight Hour. for the purpose of this AC/AMJ, is a representation of the number of times the subject Failure Condition is predicted to occur during the entire operating life of all airplanes of the type divided by the anticipated total operating hours of all airplanes of that type (Note: The Average Probability Per Flight Hour is normally calculated as the probability of a failure condition occurring during a typical flight of mean duration divided by that mean duration).

- d. Candidate Certification Maintenance Requirements (CCMR). A periodic maintenance or flight crew check may be used in a safety analysis to help demonstrate compliance with §/JAR 25.1309(b) for Hazardous and Catastrophic Failure Conditions. Where such checks cannot be accepted as basic servicing or airmanship they become Candidate Certification Maintenance Requirements (CCMRs). AC/AMJ 25-19 defines a method by which Certification Maintenance Requirements (CMRs) are identified from the candidates. A CMR becomes a required periodic maintenance check identified as an operating limitation of the type certificate for the airplane.

Terms and Definitions

- e. Check. An examination (e.g., an inspection or test) to determine the physical integrity and/or functional capability of an item.
- f. Complex. A system is Complex when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods.
- g. Conventional. A system is considered to be Conventional if its functionality, the technological means used to implement its functionality, and its intended usage are all the same as, or closely similar to, that of previously approved systems that are commonly-used.
- h. Design Appraisal. This is a qualitative appraisal of the integrity and safety of the system design.
- i. Development Assurance. All those planned and systematic actions used to substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis.
- j. Error. An omission or incorrect action by a crew member or maintenance personnel, or a mistake in requirements, design, or implementation.

Terms and Definitions

- k. Event. An occurrence which has its origin distinct from the airplane, such as atmospheric conditions (e.g. gusts, temperature variations, icing and lightning strikes), runway conditions, conditions of communication, navigation, and surveillance services, bird-strike, cabin and baggage fires. The term is not intended to cover sabotage.

- l. Failure. An occurrence which affects the operation of a component, part, or element such that it can no longer function as intended (this includes both loss of function and malfunction). Note: Errors may cause Failures, but are not considered to be Failures.

- m. Failure Condition. A condition having an effect on the airplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.

- n. Installation Appraisal. This is a qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry-accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into service.

- o. Latent Failure. A failure is latent until it is made known to the flight crew or maintenance personnel. A significant latent failure is one which would in combination with one or more specific failures or events result in a Hazardous or Catastrophic Failure Condition.

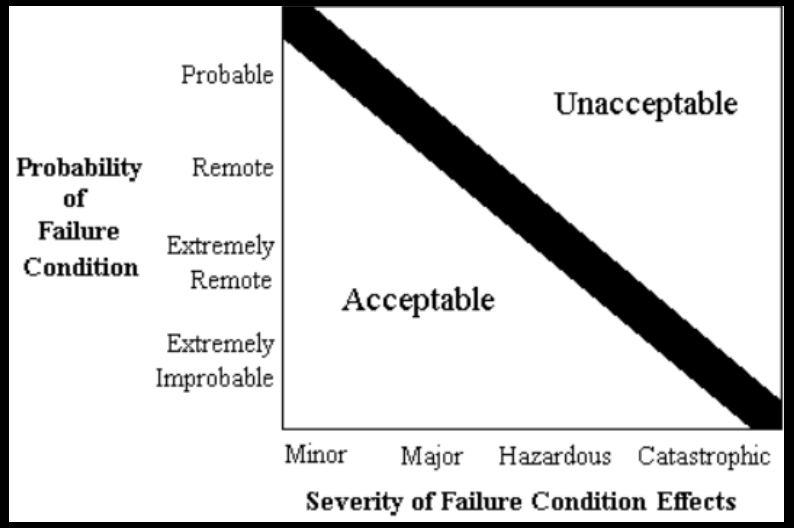
Terms and Definitions

- p. Qualitative. Those analytical processes that assess system and airplane safety in an objective, non-numerical manner.
- q. Quantitative. Those analytical processes that apply mathematical methods to assess system and airplane safety.
- r. Redundancy. The presence of more than one independent means for accomplishing a given function or flight operation.
- s. System. A combination of components, parts, and elements which are inter-connected to perform one or more functions.

AC25.1309 Safety Objective

- a. The objective of §/JAR 25.1309 is to ensure an acceptable safety level for equipment and systems as installed on the airplane. A logical and acceptable inverse relationship must exist between the Average Probability per Flight Hour and the severity of Failure Condition effects, as shown in Figure 1, such that:
    1. Failure Conditions with No Safety Effect have no probability requirement.
    2. Minor Failure Conditions may be Probable.
    3. Major Failure Conditions must be no more frequent than Remote.
    4. Hazardous Failure Conditions must be no more frequent than Extremely Remote.
    5. Catastrophic Failure Conditions must be Extremely Improbable.

Figure 1: Relationship between Probability and Severity of Failure Condition Effects



AC25.1309 Arsenal

- Figure 2:Relationship Between Probability and Severity of Failure Condition.

Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Allowable Qualitative Probability	No Probability Requirement	<---Probable---->	<----Remote----->	Extremely <----------> Remote	Extremely Improbable
Allowable Quantitative Probability: Average Probability per Flight Hour on the Order of:	No Probability Requirement	<----------> $<10^{-3}$ Note 1	<----------> $<10^{-5}$	<----------> $<10^{-7}$	$<10^{-9}$
Classification of Failure Conditions	No Safety Effect	<-----Minor------>	<-----Major------>	<--Hazardous--->	Catastrophic
Note 1: A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category airplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.					

AC25.1309

- 25.1309B – Arsenal Draft
- The airplane systems and associated components, considered separately and in relation to other systems, must be designed ***and installed*** so that:
  - (1) ***Each*** catastrophic failure condition
    - (i) is **extremely improbable**; and
    - **(ii) does not result from a single failure**; and
  - (2) ***Each*** hazardous failure condition is **extremely remote**; and
  - (3) ***Each*** major failure condition is **remote**.

Quantitative:
P=<1E-9 / pfh

Quantitative:
P=<1E-7 / pfh

Quantitative:
P=<1E-5 / pfh

AC25.1309 - 10. IDENTIFICATION OF FAILURE CONDITIONS AND CONSIDERATIONS WHEN ASSESSING THEIR EFFECTS

- a. Identification of Failure Conditions. Failure Conditions should be identified by considering the potential effects of failures on the airplane and occupants. These should be considered from two perspectives:

1. by considering failures of airplane level functions - Failure Conditions identified at this level are not dependent on the way the functions are implemented and the systems' architecture.

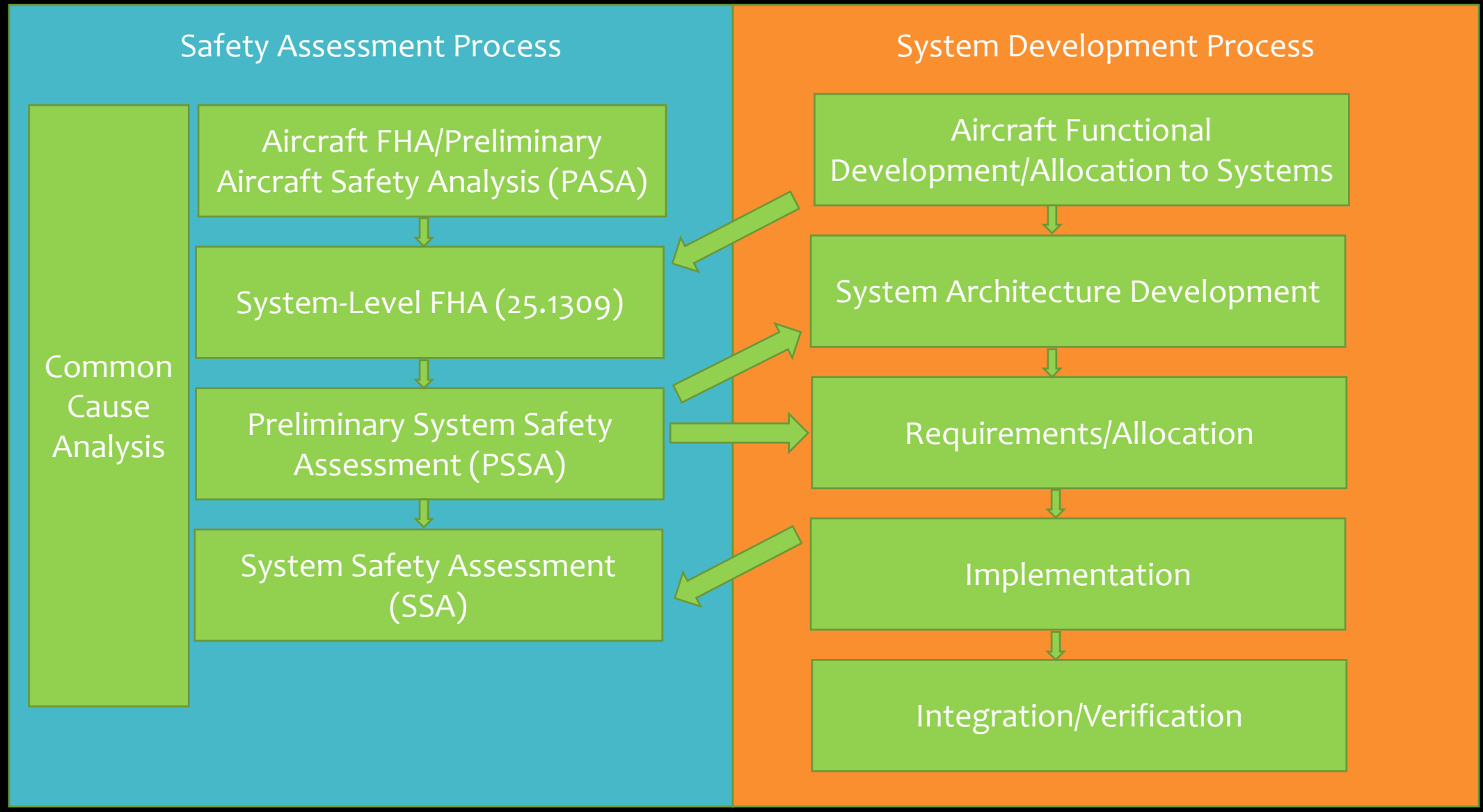
2. by considering failures of functions at the system level - these Failure Conditions are identified through examination of the way that functions are implemented and the systems' architectures.

It should be noted that a Failure Condition may result from a combination of lower level Failure Conditions. This requires that the analysis of complex, highly integrated systems, in particular, should be conducted in a highly methodical and structured manner to ensure that all significant Failure Conditions which arise from multiple failures and combinations of lower level Failure Conditions are properly identified and accounted for. The relevant combinations of failures and Failure Conditions should be determined by the whole safety assessment process that encompasses the aircraft and system level functional hazard assessments and common cause analyses. The overall effect on the airplane of a combination of individual system Failure Conditions occurring as a result of a common or cascade failure, may be more severe than the individual system effect. For example, Failure Conditions classified as minor or major by themselves may have hazardous effects at an airplane level, when considered in combination.

AC25.1309 – Functional Hazard Assessment (FHA)

- b. Identification of Failure Conditions Using a Functional Hazard Assessment.
- (1) Before an applicant proceeds with a detailed safety assessment, a Functional Hazard Assessment (FHA) of the airplane and system functions to determine the need for and scope of subsequent analysis should be prepared. This assessment may be conducted using service experience, engineering and operational judgment, and/or a top-down deductive qualitative examination of each function. A Functional Hazard Assessment is a systematic, comprehensive examination of airplane and system functions to identify potential Minor, Major, Hazardous, and Catastrophic Failure Conditions which may arise, not only as a result of malfunctions or failure to function, but also as a result of normal responses to unusual or abnormal external factors. It is concerned with the operational vulnerabilities of systems rather than with a detailed analysis of the actual implementation.
- The level of hazard also dictates development assurance methods critical to compliance. (these are in addition to quantitative probability and no single failure compliance)
- ARP4754A – Summarized: Catastrophic = DAL A, Hazardous >DAL B, Major > DAL C, Minor > DAL D, No Safety Effect = DAL E.
  - Generally, most things that interface to Avionics require DAL D or better.

Aerospace Safety and System Development Process



What are ‘misleading’ functional hazards?

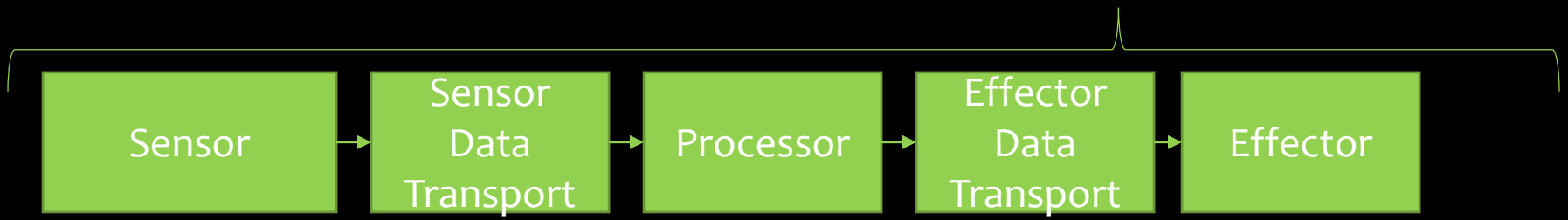
- Misleading functional hazards are aircraft hazards resulting from a function operating erroneously (including incorrect crew response acting on inaccurate information)
  - In Systems and Networks the causing failure condition is often referred to as: ‘undetected erroneous data’ or ‘undetected corruption’, in that the receiving system/function has no ability to detect the errors within the data (and thus it will result in misleading functional behavior).
- Example: ‘Misleading attitude display to both sides of the cockpit….’
- ‘misleading’ hazards are avoided by addressing ‘integrity’ of components / data paths
  - Numerous architectures can be used to meet 25.1309 probability guidance
    - Considerations:
      - Redundant sources for purposes of availability or integrity
      - Stringent requirements on data transport integrity are more critical in some architectures
      - Bandwidth impacts to support many copies of the same information should be considered
      - Voting can be used to boost integrity
      - Corner conditions around voting, transitions, temporal relationships of input signals can be difficult to verify.
      - Fully duplicate, redundant systems drive weight, cost, power
      - Some architectures more easily allow for dissimilarity
      - Etc…
- Integrity of network data for a system can include many aspects: bit integrity, frame integrity, packet integrity, datagram integrity, temporal integrity, ordinal integrity, source integrity (some assurance of authenticity of sender), etc

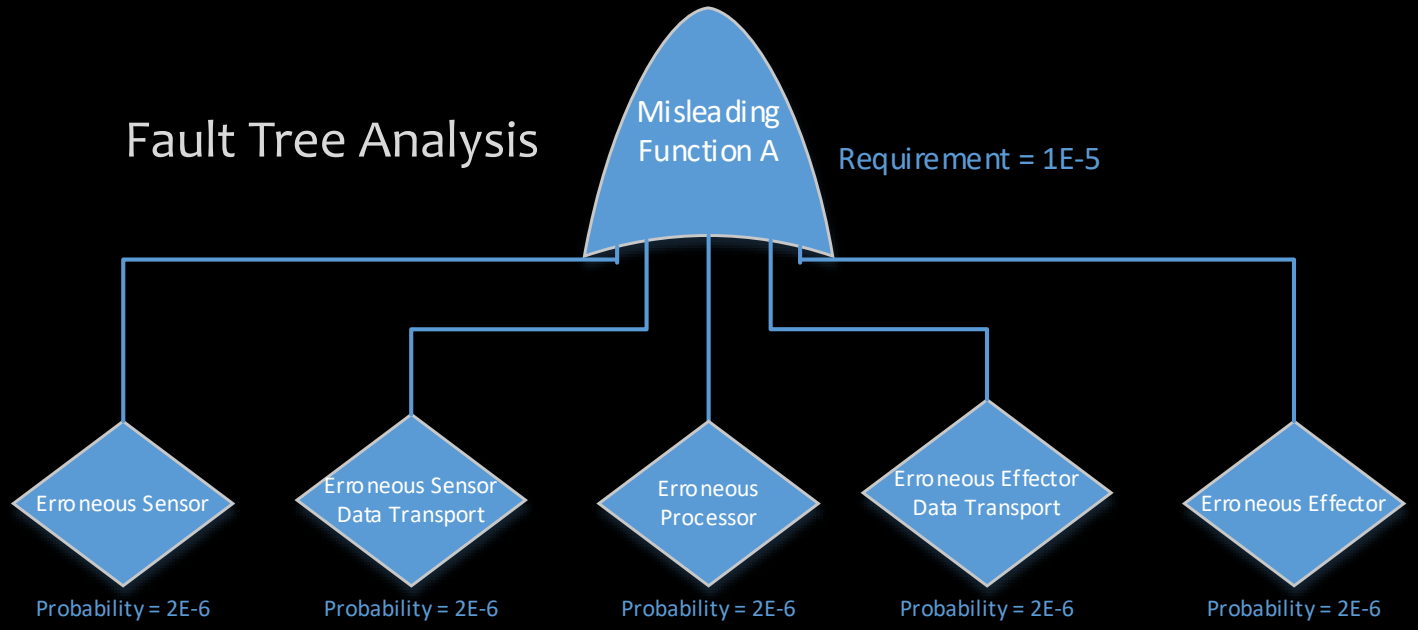
What are ‘loss’ functional hazards?

- ‘Loss’ functional hazards are aircraft hazards resulting from the loss of a system/function.
- ‘loss hazards’ are avoided by addressing ‘availability’ of components / data paths
  - Impacted by reliability / redundancy
- Ex: “Loss of XYZ Function can cause Hazardous aircraft condition”
- More specific example: “Loss of all flight control” resulting in catastrophic aircraft hazard
  - This Functional Hazard Assessment item then drives safety requirements on the redundant flight control systems, both for independence (recall “no single failure”)adding up all of the contributing probabilities using fault tree analysis to show that the top event of ‘loss of all flight control’ will occur less than 1E-09, per the 25.1309 regulation.
  - Catastrophic hazards have an extra expectation, reflected in requirements, of compliance to 25.1309-1B, “No single failure regardless of probability”

Application Example 1

<1E-5 pfh for 'Major' Aircraft Hazards

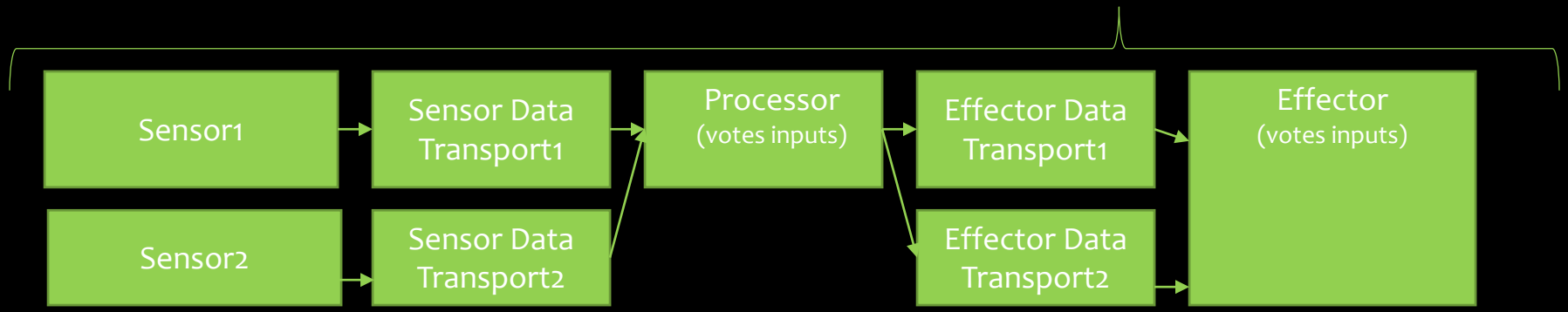




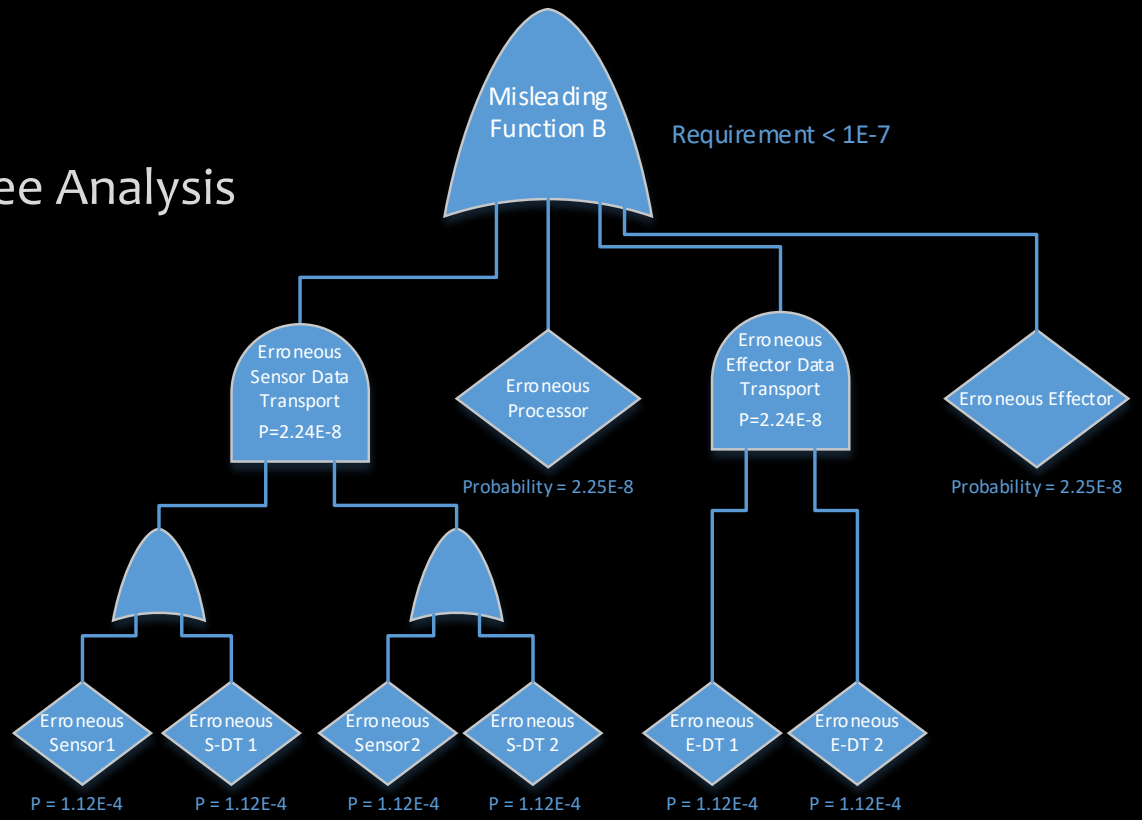
- Balancing impacts of Size, Weight, Power, and Cost (SWaP-C) is a key driver in aerospace systems architecture.

Application Example 2

<1E-7 pfh for 'Hazardous' Aircraft Hazards

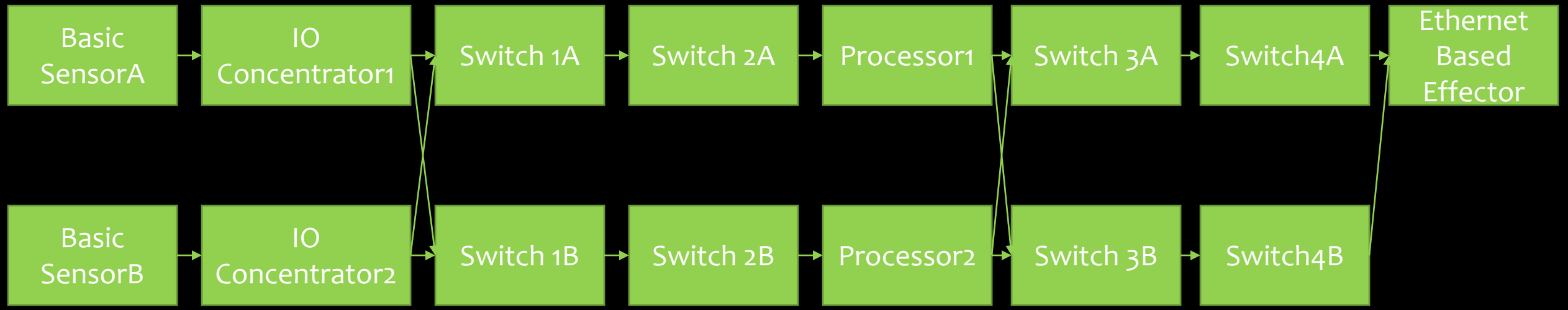


Fault Tree Analysis



- Sometimes SWaP-C might drive architecture
- Two Sensors with easier requirements, better fault tolerance
- Two Network Switches with easier requirements, better fault tolerance
- In allocation & design, margin often added to requirements to reduce impact of late discoveries.
- Many, many possible permutations, but all have the same goals
  - Meet 25.1309/CS25

Application Example 3 – Complexity grows



- Failure Modes become more complex, especially when including multiple/latent failures
- Common Mode Analysis (CMA) / Common Cause Analysis (CCA) grow more challenging, especially with catastrophic hazards with ‘no single fault, regardless of probability’ requirements.
- Fault Tree Analysis (FTA) increases in complexity
- Regulation compliance is still expected

Conclusion

- In support of certification, Aerospace Systems and Networks are especially sensitive to:
  - Fault Tolerance
    - Fail Safe and Fail Active Architectures
      - Fail Safe (detect error and disable function)
      - Fail Active (detect error and outvote/use alternate means to continue operating function safely)
    - Single Point Failures that could cause loss or misleading data
  - 25.1309 Quantitative Probability and ‘No Single Failure’ guidance requires detailed failure mode analysis of:
    - Systems
    - Components
    - Network Architectures and protocols that contribute to integrity
      - 802.1AS, 802.1Qbv, 802.1Qci, 802.1Qcr, etc.
    - Network Architectures and protocols that contribute to availability
      - 802.1CB, etc.
    - Transport protocols and Application design (resilience to loss, etc)