Flight Control System Certification Discussion Exercise

- Functional Hazard Analysis FHA,
- Fault Tree Analysis,
- Dependence Diagrams,
- Common Cause Analysis
- FMEA

Functional Hazard Analysis (FHA) for Flight Control System:

- The main objective of Functional Hazard Assessment (FHA) is to identify and evaluate the functions of a system that could cause or contribute to a hazard.
- In the context of a flight control system, FHA would consider different functional failures and their effects on the overall system and the aircraft. The assessment considers various modes of failure, how they might occur, and the consequences of such failures.

Before an applicant proceeds with a detailed safety assessment, an FHA of the airplane and system functions to determine the need for and the scope of subsequent analysis should be prepared.

- This assessment may be conducted using service experience, engineering and operational judgment, or service experience and a top-down deductive qualitative examination of each function.
- An FHA is a systematic, comprehensive examination of airplane and system functions to identify potential no safety effect, minor, major, hazardous, and catastrophic failure conditions that 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.
- The FHA concerns the operational vulnerabilities of systems rather than a detailed analysis of the actual implementation.

Each system function should be examined regarding the other functions performed by the system because the loss or malfunction of all functions performed by the system may result in a more severe failure condition than the loss of a single function.

In addition, each system function should be examined regarding functions performed by other airplane systems because the loss or malfunction of different but related functions, provided by separate systems, may affect the severity of failure conditions postulated for a particular system.

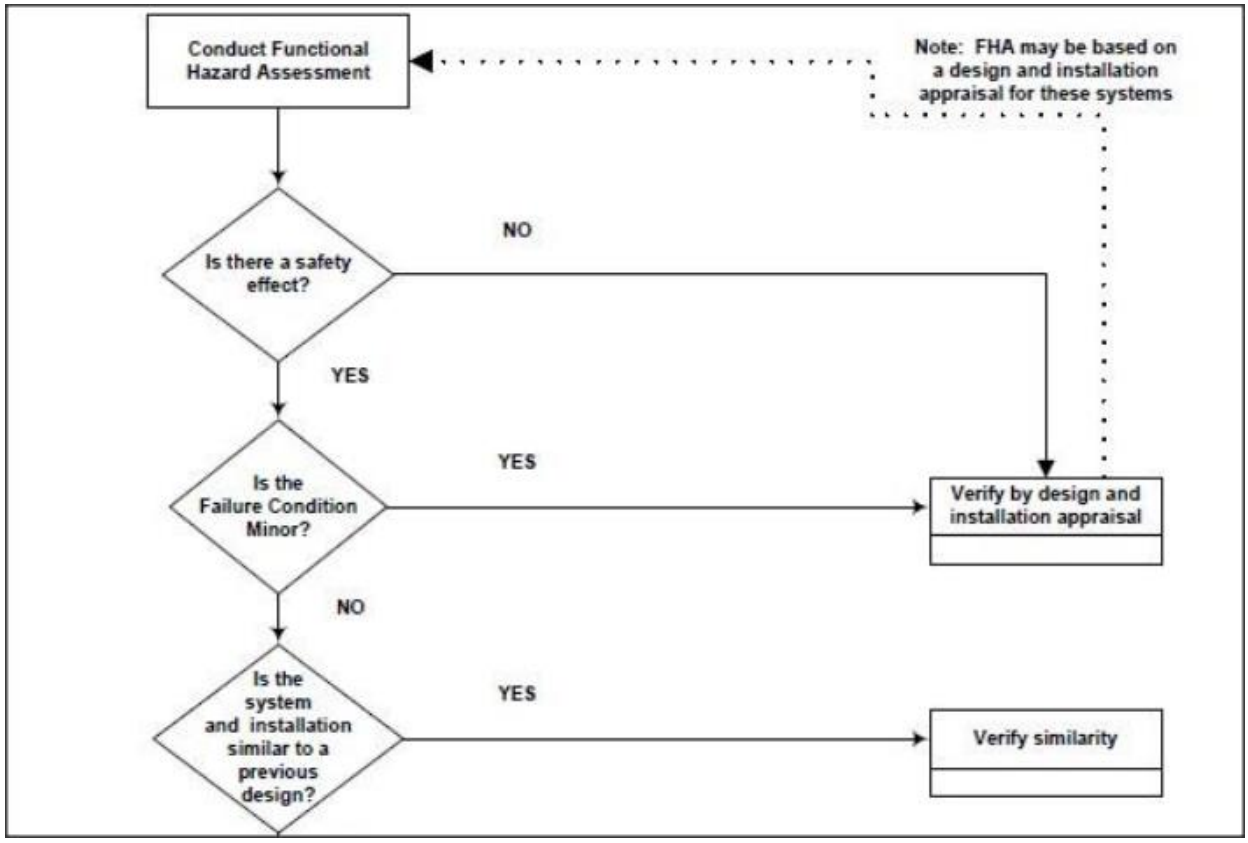
Note - The FHA is an engineering tool that should be performed early in the design and updated as necessary.

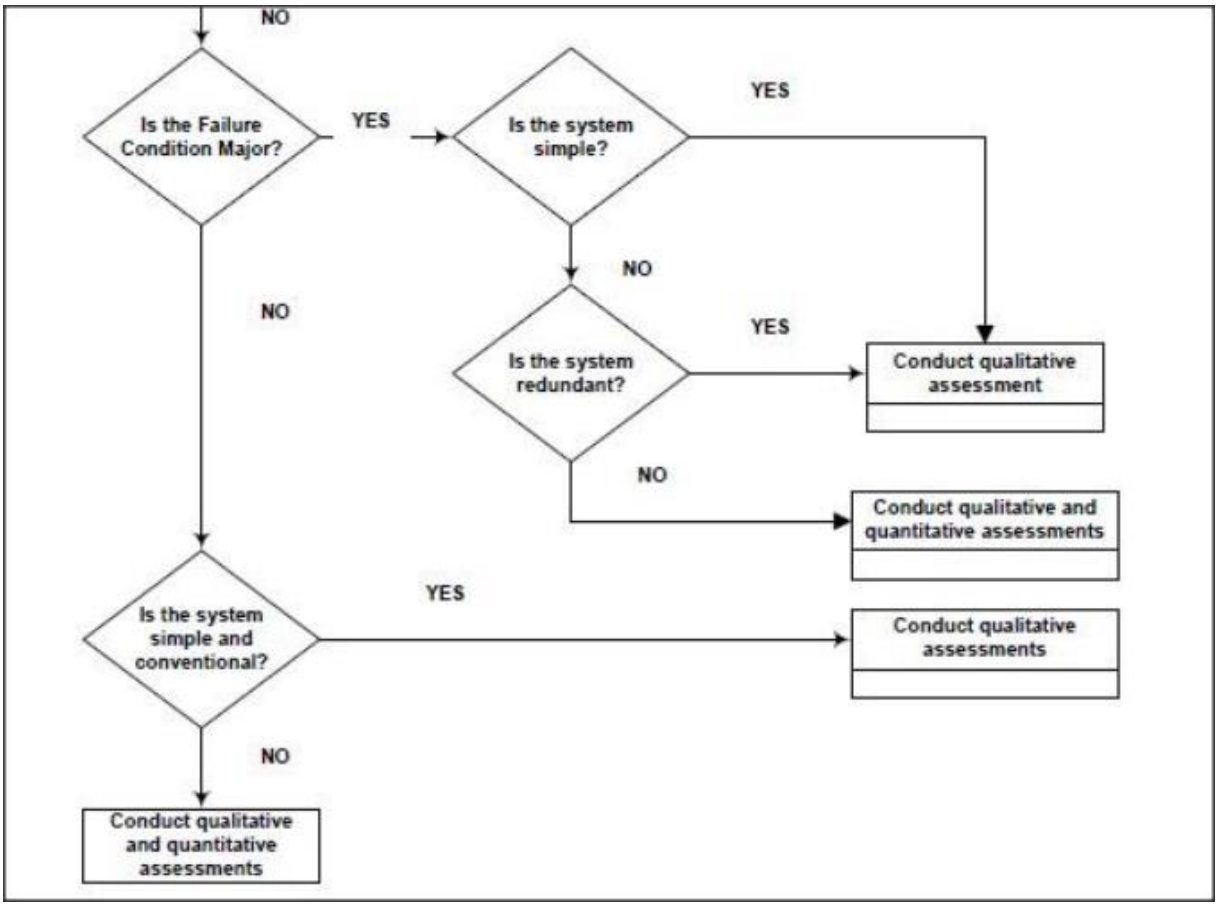
- It is used to define the high-level airplane or system safety objectives that should be considered in the proposed system architectures. Also, it should be used to assist in determining the DALs for the systems. Many systems may need only a simple review of the system design by the applicant to determine the hazard classification. An FHA requires experienced engineering judgment and early coordination between the applicant and EASA.

Depending on the extent of functions to be examined and the relationship between functions and systems, different approaches to FHA may be taken.

- Where there is a clear correlation between functions and systems, and where system and function interrelationships are relatively simple, it may be feasible to conduct separate FHA's for each system.

- However, this is conditional providing any interface aspects are properly considered and easily understood. However, a top-down approach from an airplane level perspective should be taken in planning and conducting an FHA where system and function interrelationships are more complex.





Time Line & Competence Considerations - How long does it take to perform a FHA?

Overall, a high-level FHA could take around 3 to 6 months depending on the complexity of the system, the experience of the team, and the specific requirements of the project. This timeline can expand if the system is particularly complex or if unexpected issues arise during the assessment.

A Functional Hazard Assessment (FHA) for an aircraft flight control system is a comprehensive and critical task.

- This activity involves assessing the functional hazards and risks of an aerospace system and determining the required safety measures to manage these risks.
- **Preliminary Planning (1 to 2 weeks):** This step involves the development of a detailed work plan which includes assembling the team, defining roles and responsibilities, and determining the scope of the FHA.
    - Manpower: A team leader, safety engineer(s), system engineer(s), flight control specialists, and possibly a project manager.
    - Competence: Knowledge of flight control systems, risk management, safety engineering principles, and familiarity with regulatory standards (like DO-178C, DO-254, ARP4761, etc.) is required.

- **System Familiarization (2 to 4 weeks):** This step involves reviewing the system design, understanding the function of each component, and how they integrate together.
    - Manpower: System engineer(s), safety engineer(s), and flight control specialists.
    - Competence: Technical understanding of flight control systems, ability to understand system design documents, schematics, and design analysis.

- **Risk Identification and Assessment (4 to 8 weeks):** This phase involves identifying potential functional hazards and failure conditions, analyzing their potential effects and causes, and assessing their associated risks.
    - Manpower: Safety engineer(s), system engineer(s), and flight control specialists.
    - Competence: Deep understanding of safety analysis techniques (like FMEA, FTA, etc.), risk assessment methodologies, and flight control systems.

- **Risk Mitigation and Safety Requirement Identification (2 to 4 weeks):** In this phase, the team develops strategies to mitigate identified risks and establishes safety requirements.
    - Manpower: Safety engineer(s), system engineer(s), and flight control specialists.
    - Competence: Proficiency in risk management, ability to devise mitigation strategies, and define safety requirements based on risk levels.

- **Documentation and Reporting (2 to 3 weeks):** This last step involves documenting the FHA process, results, and the risk mitigation plan, and producing a final report.
    - Manpower: Safety engineer(s), system engineer(s), technical writer(s).
    - Competence: Strong technical writing skills, ability to communicate complex concepts clearly, and a deep understanding of the system and its associated risks.

Classification of Failures

The classification of failure conditions does not depend on whether a system or function is required by any specific regulation.

- Some systems required by specific regulations, such as transponders, position lights, and public address systems, may have the potential for only minor failure conditions.
- Conversely, other systems not required by any specific regulation, such as flight management systems and automatic landing systems, may have the potential for major, hazardous, or catastrophic failure conditions.

The classification of failure conditions should consider all relevant factors.

- Examples of factors include the nature of the failure modes, which includes:
    - common mode faults,
    - system degradation resulting from failures,
    - flight crew actions,
    - flight crew workload,
    - performance degradation,
    - reduced operational capability,
    - effects on airframe, etc.

- It is particularly important to consider factors that would alleviate or intensify the severity of a failure condition.
    - An example of an alleviating factor would be the continued performance of identical or operationally similar functions by other systems not affected by a failure condition.
    - Examples of intensifying factors would include unrelated conditions that would reduce the ability of the crew to cope with a failure condition, such as weather or other adverse operational or environmental conditions.
- The ability of a system to inform the pilot of potential or real failure conditions so that timely corrective action can be taken to reduce the effects of the combination of events is desirable.
    - This approach may reduce the severity of the failure condition.
- Because of the large number of combinations of failures, various mitigating factors, airplane characteristic effects, and similar factors, a specific FHA and the related safety assessments may be significantly different for each evaluated airplane type and configuration.
- These factors preclude providing a concrete example of a FHA that applies across the board to every installation.
- It is critical to understand that significant engineering judgment and common sense are necessary to provide a practical and acceptable evaluation of the airplane and its systems.

Failure Conditions Criteria

Failure conditions. A condition having an effect on either the airplane or its occupants, or both, 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.

Failure conditions may be classified according to the severity of their effects as follows:

- **No safety effect**. Failure conditions that would have no effect on safety (that is, failure conditions that would not affect the operational capability of the airplane or increase crew workload).
- **Minor.** Failure conditions that would not significantly reduce airplane safety and involve crew actions that are within their capabilities.
    - Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in crew workload (such as routine flight plan changes), or some physical discomfort to passengers or cabin crew.

- **Major.** Failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be a significant` reduction in safety margins or functional capabilities.

    - In addition, the failure condition has a significant increase in crew workload or in conditions impairing crew efficiency; or a discomfort to the flight crew or physical distress to passengers or cabin crew, possibly including injuries.

- **Hazardous.** Failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be the following:

    - A large reduction in safety margins or functional capabilities;
    - Physical distress or higher workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or
    - Serious or fatal injury to an occupant other than the flight crew.

- **Catastrophic.** Failure conditions that are expected to result in multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crewmember normally with the loss of the airplane.

Notes:

The phrase “are expected to result” is not intended to require 100 percent certainty that the effects will always be catastrophic. Conversely, just because the effects of a given failure, or combination of failures, could conceivably be catastrophic in extreme circumstances, it is not intended to imply that the failure condition will necessarily be considered catastrophic.

- The term “catastrophic” was defined in previous versions of advisory materials as a failure condition that would prevent continued safe flight and landing.

- Failure conditions with no safety effect.

- An FHA with a design and installation appraisal to establish independence from other functions is necessary for the safety assessment of these failure conditions.

In general, common design practice provides physical and functional isolation from related components, which are essential to safe operation.

- If the applicant chooses not to do a detailed FHA, the safety effects may be derived from the design and installation appraisal performed by the applicant.

Analysis of Minor Failure Conditions.

An analysis should consider the effects of system failures on other systems or their functions.

- An FHA with a design and installation appraisal to establish independence from other functions is necessary for the safety assessment of these failure conditions. In general, common design practice provides physical and functional isolation from components that are essential to safe operation.

- If the applicant chooses not to do a detailed FHA, the safety effects may be derived from the design and installation appraisal performed by the applicant.

Analysis of Major Failure Conditions.

- An assessment based on engineering judgment is a qualitative assessment, as are several of the methods described below:

- Similarity allows validation of a requirement by comparison to the requirements of similar certified systems.
- The similarity argument gains strength as the period of experience with the system increases. If the system is similar in its relevant attributes to those used in other aeroplanes and if the functions and effects of failure would be the same, then a design and installation appraisal and satisfactory service history of either the equipment being analysed or of a similar design is usually acceptable for showing compliance.
- It is the applicant's responsibility to provide data that is accepted, approved, or both, and that supports any claims of similarity to a previous installation.

Non Complex Systems

- For systems that are not complex and where similarity cannot be used as the basis for compliance, then compliance may be shown by means of a qualitative assessment that shows that the major failure conditions of the system, as installed, are consistent with the FHA (for example, redundant systems).

- To show that malfunctions are indeed remote in systems of high complexity without redundancy (for example, a system with a self-monitoring microprocessor), it is necessary to conduct a qualitative functional FTA or FMEA supported by failure rate data and fault detection coverage analysis.

Considering Redundancy

An analysis of a redundant system in the airplane is usually complete if it shows isolation between redundant system channels and satisfactory reliability for each channel.

- For complex systems, where functional redundancy is required, a qualitative FMEA or FTA may be necessary to determine that redundancy actually exists (for example, no single failure affects all functional channels).

Fault Tree Analysis

Fault Tree Analysis (FTA): Fault Tree Analysis is a top-down approach used to identify the root causes of a system failure. It uses a tree-like model of system failures to determine the probability of top-level failures from the probabilities of lower level failures. This allows for a quantitative evaluation of system reliability and safety. In the context of flight control systems, FTA would map out the different failure paths that could lead to a major malfunction or accident.

Consider the following steps involved in the Fault Tree Analysis (FTA)

Define the System and Failure Criteria - 1-2 Weeks

- Manpower: Systems Engineer, Certification Specialist
- Systems Engineer and Certification Specialist work together to define the system, its intended functions, and the failure criteria.
    - The output is a clear definition of the system and its intended behavior under normal and abnormal conditions.

Construct Preliminary Fault Tree - 2-3 Weeks

- Manpower: Systems Engineer, Reliability Engineer
- Using the system definition and failure criteria, the systems and reliability engineers construct a preliminary fault tree.
    - This is a top-down, deductive analysis where the undesired state of the system (i.e., the top event in the fault tree) is identified, and the conditions and events that could cause this are identified and arranged in a logical, tree-like diagram.
    - The output is the preliminary fault tree.

Detailed Fault Tree Analysis - 4-6 Weeks

- Manpower: Systems Engineer, Reliability Engineer, Design Engineer
- Performa a Detailed FTA identifying and adding all potential root causes of the failure to the fault tree and analyzing their probability and impact.
- This will typically require a detailed understanding of the design of the system.
    - The output is the completed fault tree.

Validate Fault Tree - 2-3 Weeks

- Manpower: Systems Engineer, Test Engineer
- Validate the Fault Tree through a combination of theoretical analysis and empirical testing.
- The system may need to be tested under different conditions to confirm the potential failure modes identified in the fault tree.
    - The output is a validated fault tree.

Mitigate Identified Risks – Several Weeks (or more)

- Manpower: Systems Engineer, Design Engineer
- Based on the validated fault tree, the design of the System may need to be modified to mitigate identified risks.
    - The output is a system design that has been modified to address potential failure modes.

Document Findings and Submit for Certification – 2 – 3 Weeks

- Manpower: Systems Engineer, Certification Specialist
- The findings from the FTA, including the fault tree itself, the identified failure modes, and the steps taken to mitigate these, are documented and submitted to the relevant certification authority (e.g., FAA in the USA, EASA in Europe).
    - The output is the completed Certification Documentation

Respond to Certification Authority Feedback (Potentially Several Weeks)

- Manpower: Systems Engineer, Certification Specialist
- The certification authority may have questions or require additional information or testing.

- The systems engineer and certification specialist work together to respond to this feedback.
    - The output is a certified flight control actuator.

Dependence Diagrams

These diagrams help in visualizing the interdependencies among different system components or functions.

- They are beneficial in assessing the effects of multiple failures or changes within the system. In a flight control system, this could help to identify how a failure in one subsystem (e.g., autopilot, navigation, control surfaces) might affect other subsystems or the overall operation of the aircraft.
- Dependence diagrams play an essential role in ensuring the safety and functionality of aircraft systems, but creating and maintaining them can be a complex and challenging process.
- Various parties are typically involved in the creation and maintenance of dependence diagrams including Aircraft Design Engineers, Certification Engineers & System Safety Engineers and Regulatory Authorities, review the dependence diagrams as part of the certification process.

These Diagrams Serve a Dual Role.

- Firstly, they assist in the identification and understanding of how the failure of one component or system could potentially affect others.
    - This helps in defining safety requirements, as well as in the development of safety and redundancy measures.
- Secondly, dependence diagrams help in understanding the interplay between different systems during normal operation.
    - This knowledge is critical when designing and implementing new components or systems, or when performing upgrades or changes.

Dependence Diagrams Development Process

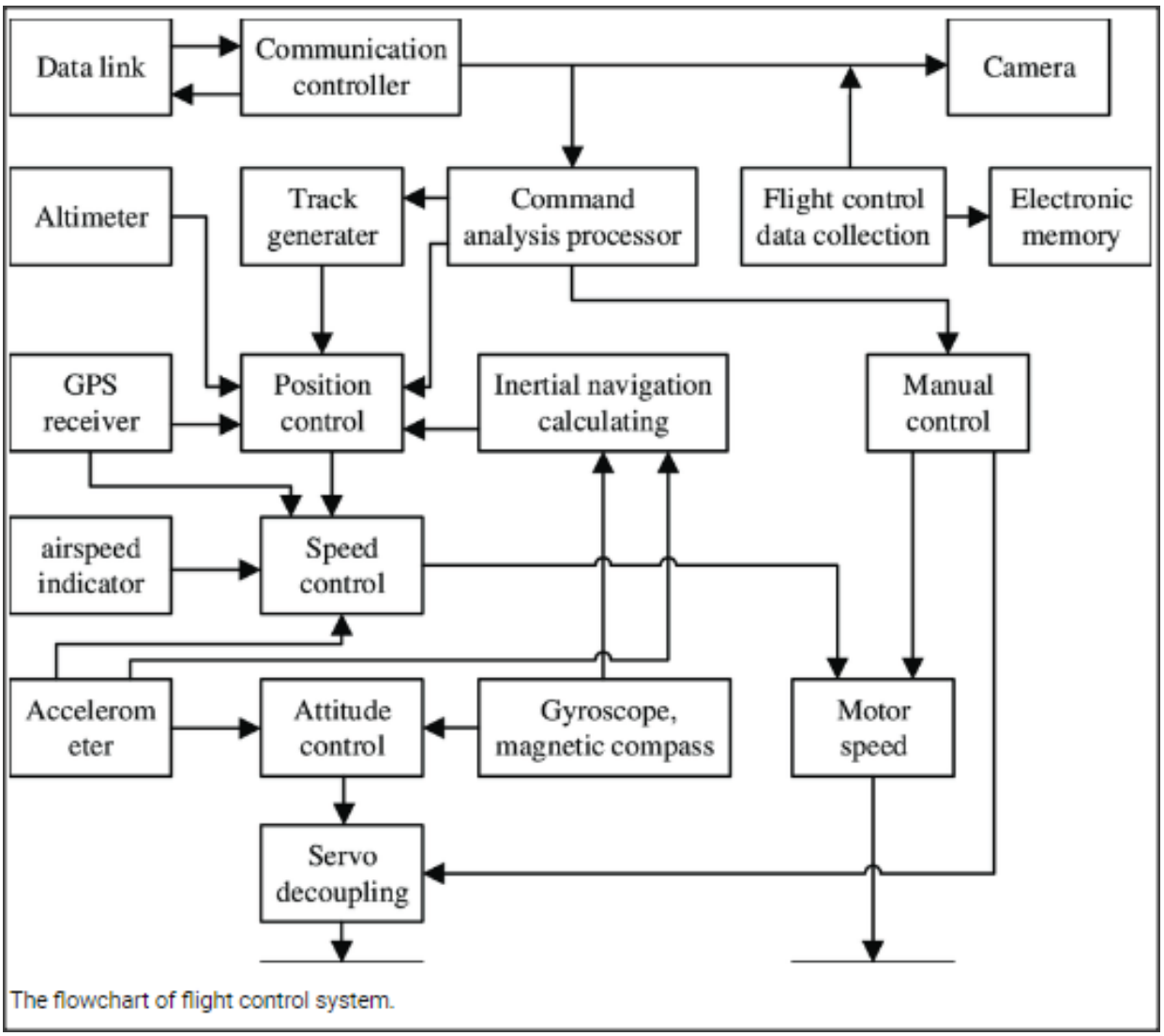
- The creation and review of a dependence diagram can be a time-consuming process, typically taking place over many weeks or months.
- Initial design concepts are developed into a preliminary dependence diagram.
- The diagram is iteratively reviewed and refined by engineers and safety experts to ensure accuracy and completeness.
- The finalized diagram is tested and verified against the actual aircraft systems.
- The diagram is then submitted to the relevant regulatory authority as part of the certification documentation.
- Any changes or upgrades to the aircraft systems must be reflected in updates to the dependence diagram, which may require additional certification.

Challenges to Creating an Effective Dependence Diagram

- Modern aircraft systems are incredibly complex, with hundreds of interrelated components. Representing these accurately and understandably can be a significant challenge.

- As designs evolve during the development process, the dependence diagram must be updated to reflect these changes, which can be resource-intensive.
- Different regulatory authorities may have different standards or requirements for dependence diagrams, which can complicate the certification process.
- With the increasing reliance on software in modern aircraft, understanding and representing software dependencies can be particularly challenging.

Example Contents of a Dependence Diagram for an Aircraft Flight Control System



The flowchart of flight control system.

- A dependence diagram would illustrate the relationships and dependencies between different components and subsystems involved in controlling the flight of an aircraft.
- Here are the typical elements that might be contained within a dependence diagram for an aircraft flight control system:

- Flight Control Computer (FCC): The central computing unit responsible for processing control inputs and providing commands to actuators and control surfaces.
- Control Surfaces such as ailerons, elevators, rudders, flaps, and spoilers, which are responsible for controlling the aircraft's motion.
- Various sensors on the aircraft, such as airspeed sensors, altitude sensors, gyros, accelerometers, and angle-of-attack sensors, provide data to the flight control system.
- Actuators are responsible for physically moving the control surfaces based on the commands received from the Flight Control Computer.
- Different control modes that the flight control system can operate in, such as manual control, autopilot, fly-by-wire, and different flight envelope protections.
- The algorithms and logic used by the Flight Control Computer to process sensor data and determine appropriate control surface commands.
- In redundant flight control systems, there might be multiple control laws to handle failures or ensure graceful degradation.
- The communication pathways through which different components exchange data and commands.
- The power distribution and supply system that provides electrical power to the flight control system.
- The interface through which pilots interact with the flight control system, such as control yokes, pedals, and displays. (human -machine interface HMI)
- The software components and programs responsible for the control logic and coordination of the flight control system.
- Safety features and interlocks that prevent conflicting commands or actions that could jeopardize the aircraft's safety.
- Sensors that provide data on environmental conditions like temperature, humidity, and air pressure, which may influence control decisions.
- The navigation system, which may have dependencies on the flight control system, especially during automatic navigation modes.

Common Cause Analysis

Common Cause Analysis (CCA) describes the method used to identify the potential for common-cause failures (CCFs) within a system, where multiple components fail simultaneously due to a single event or shared cause.

In the context of certification, a comprehensive CCA is crucial. Regulatory bodies require a systematic approach to identifying and mitigating safety risks, including CCFs. Therefore, demonstrating a rigorous CCA is often a requirement for certification of an aviation flight control system

In an aircraft flight control system, this could be due to design faults, human errors, or external events that could impact multiple components at once.

- The results of a CCA are often used to inform design changes, preventive measures, or redundancy measures to mitigate the risk of CCFs.
- For example, in a flight control system, a power supply issue might simultaneously affect multiple subsystems.

- By identifying and mitigating these common-cause failures, the overall reliability of the system can be improved.

A multidisciplinary team usually carries out CCA involving system engineers, reliability engineers, safety engineers, and often software and hardware engineers.

Common Cause Analysis Timeline

- The CCA should be initiated during the conceptual design stage and continually updated throughout the lifecycle of the system until its decommissioning.
- This ongoing process should align with the main design reviews, and it must accommodate any design changes or system modifications.

Common Cause Analysis Significant Challenges

- Identification of CCFs can be a complex process due to the high interdependency of modern aircraft systems.
- Challenging to balance the costs and benefits of implementing redundancies or changes to mitigate CCFs.
- Requires a significant time and resource for a comprehensive CCA

Conducting a CCA

- Use of proven CCA methodologies such as Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), or Event Tree Analysis (ETA).
- Conduct a thorough and systemic CCA at each major design phase and update it as the design matures.
    - Ensure adequate diversity and redundancy in the system design to mitigate CCFs.
    - Regularly review and update the CCA as the system evolves and as more data becomes available about system reliability and failure modes.

Initiate the Common Cause Analysis (CCA) – 1 to 2 Weeks

- Define the system or process that will be the subject of the analysis.
    - This should include understanding the various components of the system and how they interact.
- Assemble the team which could include system engineers, operations staff, maintenance personnel, etc.

Gather Data – 1 to 2 Weeks

- Investigate the system or process to identify any failures that could potentially be caused by a common cause.
    - This could involve reviewing previous failure data, conducting interviews with staff, and observing the system or process in operation.

Analyze Data – 1 to 2 Weeks

- Analyze the identified potential common cause failures:
    - Use appropriate statistical techniques to determine the likelihood of each identified potential common cause failure.

- This might involve looking for trends or patterns in the data, using techniques such as root cause analysis or fault tree analysis.

Identify Mitigation Strategies – 1 to 2 Weeks

- For each identified potential common cause failure, identify potential strategies to mitigate the risk of that failure occurring.
  - This could involve changes to the system or process, enhanced monitoring, additional training for staff, etc.

Develop and Implement Action Plan – Several Weeks

- Develop a detailed action plan for implementing the identified mitigation strategies.
  - This plan should include specific actions, responsibilities, timelines, and required resources.
- Carry out the actions identified in the action plan.
  - This could involve making changes to the system or process, providing additional training to staff, implementing new monitoring procedures, etc.

Review and Monitor – Continuous As Required

- Once the mitigation strategies have been implemented, it's important to monitor their effectiveness.
  - This could involve gathering and analyzing data to determine whether the likelihood of the identified potential common cause failures has been reduced.
- Regularly review and update the CCA to ensure it remains accurate and relevant.
  - This should involve repeating the above steps at regular intervals, for example, annually, or when significant changes are made to the system or process.

Failure Modes and Effects Analysis (FMEA)

Example FMEA worksheet

FMEA Ref.	Item	Potential failure mode	Potential cause(s) / mechanism	Mission Phase	Local effects of failure	Next higher level effect	System Level End Effect	(P) Probability (estimate)	(S) Severity	Detection (Indications to Operator, Maintainer)	(D) Detection Dormancy Period	Risk Level P*S (+D)	Actions for further Investigation / evidence	Mitigation / Requirements
1.1.1	Brake Manifold Ref. Designator 2b, channel A, O-ring	Internal Leakage from Channel A to B	a) O-ring Compression Set (Creep) failure b) surface damage during assembly	Landing	Decreased pressure to main brake hose	No Left Wheel Braking	Severely Reduced Aircraft deceleration on ground and side drift. Partial loss of runway position control. Risk of collision	(C) Moderate	(VI) Catastrophic (this is the worst case)	(1) Flight Computer and Maintenance Computer will indicate "Left Main Brake, Pressure Low"	Built-In Test interval is 1 minute	Unacceptable	Check Dormancy Period and probability of failure	Require redundant independent brake hydraulic channels and/or Require redundant sealing and Classify O-ring as Critical Part Class 1

Failure Modes and Effects Analysis (FMEA): This is a systematic method for identifying potential failure modes within a system, determining the effects of those failures, and prioritizing the failure modes based on their impact on system operation and safety.

An FMEA of a flight control system would consider all the possible ways that various components of the system could fail, the effects of those failures, and the level of risk associated with each failure mode.

All these methods play a crucial role in ensuring the reliability, safety, and performance of complex systems such as a flight control system. They provide a structured way of identifying, analyzing, and mitigating potential system failures

Considerations Related to EASA Certification Failure Modes and Effects Analysis (FMEA)

Introduction

The final step before beginning to perform the analysis is to obtain the following information which may be necessary to complete the analysis, or may simplify the analysis activity.

- FMEA requirements including safety related and requested failure effects and specific operating modes of interest
- Specifications
- Current drawings or schematics
- Parts lists for each system or item
- Functional block diagrams
- Explanatory materials including the theory of operation
- An applicable list of failure rates
- The FMEA on the previous generation or similar function
- Any design changes and revisions that have not yet been included on the schematic.
- Preliminary list of component failure modes from previous FMEAs, if applicable

(NOTE: Designs may change frequently and having the most up to date material will reduce FMEA updates.)

Performing the Analysis:

- The analyst needs to review and understand the information gathered during the preparation stage previously described.
- The analyst will also find it useful to understand the functions that the design being analyzed performs within the next higher level.
    - After the analyst has gained sufficient knowledge, failure modes are identified.
    - Every feasible hardware failure mode is postulated at the level of the design being analyzed.
    - Consideration is given to failure modes of the components or functions that make up the given level.
- Every identified failure mode is analyzed to determine its effect on the given level and usually on higher levels as well.
- Failure effect categories are created for each different type of effect and a code may be assigned to each effect category.
    - Defining these codes simplifies the FMEA worksheet by moving the description of each effect from the worksheet to the body of the report.

    - The FMEA worksheet provides a list of failure modes, effects and rates.
    - Each effect category must have only one higher level effect, otherwise the effect categories must be defined in more detail.
        - For example, if the effect category is originally defined as "causes signal xyz to be out of specification" but an out of specification high condition causes a different effect from an out of specification low condition, then the effect category should be split to "... out of specification high" and "... out of specification low".
        - Similarly if the failure mode is found to cause two higher level effects (e.g., "Loss of signal A" and "Loss of signal B") then these two should be combined to form a new effect category "Loss of both signal A and B".
- The means by which the failure is detected is usually determined and documented within the FMEA worksheets.
    - Examples of detection methods include detection by hardware or software monitors, flight crew detection, power up tests, and maintenance checks.
- For a quantitative FMEA, a failure rate is assigned to each failure mode.
    - Whenever possible, failure rates should be determined from failure data of similar equipment already in field use.

There are two basic types of FMEAs, functional and piece-part.

- Functional FMEAs are typically performed to support the safety analysis effort with piece-part FMEAs performed as necessary to provide further refinement of the failure rate.

Piece Part FMEA

- Piece-part FMEAs are typically done when the more conservative failure rates from a functional FMEA will not allow the system or item to meet the FTA probability of failure budget.
- A piece-part FMEA may also be useful for systems that rely on redundancy, since a functional FMEA may not reveal single component failures affecting more than one redundant element. Piece-part FMEAs are also useful for safety analysis of mechanical items and assemblies.

Functional FMEA

- A functional FMEA may be performed at any indenture level.
    - The appropriate level of subdivision is determined by the complexity of the system and the objectives of the analysis.
    - If the required analysis is on a section of circuitry or mechanical devices larger than a particular function, it should be broken down into functional blocks.
    - From an aircraft or system level, this may mean defining each LRU or item as a functional block. From the system or lower levels it may involve breaking down an item into many blocks.
    - The FMEA task is simplified if each block has as few outputs as possible.
    - Once the functional blocks have been determined, a functional block diagram should be created and each block labeled with its functional name. For each

functional block, internal and interface functions should be analyzed relative to system operation.

The next step is postulating the failure modes for each functional block. Determine the failure modes by thinking about the intent of the functional block and trying to determine how that function might fail regardless of the specific parts used.

- The analyst must know the operation of the functional block well enough to be positive that no significant failure modes have been overlooked, including single component failures that could affect more than one redundant functional block. Often, given a clear description of the block's function, many of the failure modes will become apparent.

Note There may be other failure modes based on circuit implementation.

- The effect of each failure mode is determined by considering how the function fits into the overall design.
    - Failure effect categories are generally created for each effect type and a failure effect category code is assigned.
    - All failure modes that cause this identical effect are assigned to the effect category.
    - The effect category code can then be entered into the FMEA worksheet for each failure.
    - Software and fault monitoring must be considered when determining failure effects and means of detection.
- As part of this analysis, the analyst must also verify that the monitoring can indeed detect the failure mode.
- In order to properly perform this analysis, the analyst must have detailed knowledge of the system requirements and software design including internal fault management techniques as applicable.
- If a quantitative analysis is being performed, a failure rate is assigned to each failure mode.
    - One technique is to perform a failure rate prediction for each block and apportion the failure rate across the various failure modes based on past experience of similar functions or other sources allowing determination of probability of occurrence.

Documentation

The results of the functional FMEA are recorded in a worksheet

Different requirements may result in addition or deletion of some of the information. The analyst should ensure that the FMEA form and content meets the specific needs of the requester before beginning the analysis.

As the analysis progresses, the following should be informally recorded for future maintenance of the FMEAs and to assist in resolving questions regarding the FMEA.

- Justification of each failure mode
- Rationale for the assigned failure rate
- Rationale assigning a particular failure to a failure effect category

- Documentation of any assumptions made

This documentation is typically not included in the FMEA report but is retained for reference.

Practical Considerations

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....'

Note 'misleading' hazards are avoided by addressing 'integrity' of components / data paths

- 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
- 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),

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

- 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
    - Network Architectures and protocols that contribute to availability
    - Transport protocols and Application design (resilience to loss, etc)

Next Steps

Sofema Aviation Services (www.sassofia.com) offers training to cover CS 25 System Safety Assessments – please see the following link https://sassofia.com/course/type-certification-system-safety-assessment-5-days/

For additional questions or comments – please email team@sassofia.com