SOFEMA AVIATION SERVICES

EASA Certification Hazard Analysis Considerations

Sofema Aviation Services (SAS) www.sassofia.com reviews the use of the term discusses the fundamentals and considers the various activities associated with the following terms:

- Preliminary Hazard Analysis (PHA)
- Subsystem Hazard Analysis (SSHA)
- System Hazard Analysis (SHA)

Introduction - The PHA, SHA, and SSHA processes are crucial components of the aircraft initial certification and development process.

- By systematically identifying and analyzing potential hazards at various levels (preliminary, system and subsystem), these analyses contribute to the design of safe aircraft systems and help mitigate risks before the aircraft enters service.
- They play an important role in ensuring that the aircraft meets the necessary safety requirements and that appropriate measures are in place to demonstrate full compliance with all certification specifications

Preliminary Hazard Analysis (PHA):

Preliminary Hazard Analysis (PHA) is a fundamental part of system safety engineering and risk management processes, used early in the development of a new system or product such as an aircraft. Its main goal is to identify possible hazards, their causes and effects, and the methods to mitigate these hazards in the subsequent design stages.

During a PHA, a multidisciplinary team of experts examines the aircraft and its subsystems to identify potential hazards that could arise from various factors, such as design flaws, human errors, environmental conditions, or operational procedures. The team evaluates each hazard in terms of its severity, likelihood of occurrence, and detectability.

- The purpose of PHA is to identify and assess potential hazards associated with the aircraft design, subsystems, and operations.
- It is typically performed before detailed design work begins and helps to identify critical safety requirements and design constraints.

Here are the basic steps and prerequisites for performing a PHA for aircraft initial certification and development:

- The first step in the PHA process is to accurately describe the system, which includes the aircraft's purpose, physical and functional characteristics, and operating environment. This step is crucial as it helps define the system's boundaries and understand how the system interacts with other systems, operators, and the environment.
- Using the system description, the team then identifies potential hazards that could occur during normal and abnormal conditions. This can be done through brainstorming sessions, past experience, similar system analysis, and other risk identification techniques.

- Once potential hazards are identified, the team determines possible causes for each hazard and the potential effects should the hazard occur.
    - This involves identifying system failures, human errors, and external events that could lead to each hazard.
    - This step also involves assessing the severity and likelihood of each hazard.
- Based on the risk assessment, the team then identifies ways to mitigate the identified risks.
    - This could involve design changes, use of safety equipment, procedures, training, etc.

Finally, all the information from the PHA process is documented in a PHA report. This report includes the system description, identified hazards, their causes and effects, risk assessment, and mitigation strategies.

The PHA should be performed against criteria set forth by EASA / FAA or relevant Industry Standard for example FAR / CS 25

Subsystem Hazard Analysis (SSHA)

Subsystem Hazard Analysis (SSHA) is a crucial part of the overall system safety assessment (SSA) process in the certification of an aircraft. It is used to determine the potential hazards that can arise from the subsystems of an aircraft and to evaluate their impact on the entire system and its operation.

Important Considerations

- These are complex and extensive regulations that require a deep understanding of aviation safety principles and practices. Misinterpretation or misunderstanding of the regulations can lead to non-compliance.
- The safety requirements stipulated by the regulations can place significant constraints on the design of the aircraft subsystems. Designers must find a balance between achieving the desired performance and functionality, and complying with the safety regulations.
- The SSHA process requires a deep understanding of aircraft subsystems and safety principles. This requires a strong background in aviation engineering and safety.
- Conducting SSHA involves analyzing potential hazards and risks, and devising measures to reduce them. This requires strong analytical skills, including the ability to think critically and systematically.
- The need for extensive documentation - The SSHA must be documented and communicated effectively to various stakeholders, including designers, operators, maintenance staff, and regulatory bodies.

Here are the primary steps in carrying out a Subsystem Hazard Analysis:

- The first step involves the identification of all the subsystems of the aircraft. These can include flight control systems, power systems, avionics, propulsion systems, hydraulic systems, and more.

- Next, a detailed functional description of each subsystem is provided. This should include the operations performed by the subsystem, its inputs and outputs, and its interactions with other subsystems.

- Once the subsystems and their functionalities have been detailed, the potential hazards that can arise from their operation or malfunction are identified.
    - This involves using methods such as fault tree analysis (FTA) or failure modes and effects analysis (FMEA).

- The potential impact of each hazard is then assessed and classified based on severity. This is often done using a severity classification matrix.

- The probability of each hazard occurring is also assessed. This involves a detailed analysis of the likelihood of various failures and malfunctions. The probability is often classified as frequent, probable, occasional, remote, extremely unlikely, based on the likelihood of the hazard occurring during the operational life of the aircraft.

- The risk associated with each hazard is evaluated by combining its severity and probability. This allows for the identification of unacceptable risks that need to be mitigated. Risk Mitigation measures may include design changes, redundancy, warning systems, training, and procedures.

- The results of the SSHA are documented in a report that includes all the identified hazards, their severity and probability, the associated risks, and the proposed mitigation measures.

System Hazard Analysis (SHA)

System Hazard Analysis (SHA) is an integral part of the aircraft initial certification and development process. It builds upon the findings of PHA and SSHA to assess the overall safety of the aircraft system and to identify hazards that may arise from system-level interactions.

It involves identifying and analyzing potential hazards associated with aircraft systems to ensure the safety of the aircraft and its occupants. SHA is typically conducted in accordance with regulatory requirements and industry standards.

System Hazard Analysis (SHA) is a comprehensive analysis that considers the entire aircraft system as a whole, including all subsystems and their interactions. The analysis should be conducted by a knowledgeable team against specific criteria, ensuring compliance with regulations and safety objectives.

During SHA, the team evaluates the combined effects of subsystem failures, human errors, and external factors to assess the potential hazards at the system level.

The analysis includes the identification of hazards caused by the integration of subsystems, the evaluation of the system's ability to handle failures and malfunctions, and the assessment of the effectiveness of safety mitigations and procedures. SHA helps ensure that the overall aircraft system meets the required safety standards and that potential risks are adequately addressed.

Prerequisites for Conducting a System Hazard Analysis:

- Sufficient system design information should be available, including system architecture, interface specifications, and operating principles.
- Clear and complete system requirements should be established, including functional requirements, performance criteria, and safety objectives.
- The FHA is typically conducted prior to the SHA and helps identify hazards associated with the overall aircraft design. The results of the FHA may guide the subsequent SHA process.
- The analysis team should possess the necessary knowledge, expertise, and experience in the specific system being analyzed, as well as hazard analysis techniques and industry standards.
- The System Hazard Analysis should be performed against specific criteria, which may vary depending on the applicable regulations and standards. However, some common criteria include:
    - Compliance with Regulations:
    - The analysis should address the safety objectives defined for the system or aircraft, ensuring that hazards are appropriately identified, analyzed, and mitigated.
    - The analysis should include a comprehensive risk assessment, considering the severity, likelihood, and exposure of each identified hazard.
    - The analysis should establish clear and concise safety requirements that can be traced back to the identified hazards. (These requirements should be verifiable and validated during the subsequent verification and validation processes.)

The Steps to Consider the SHA are as follows:

- The first step is to clearly define the scope of the analysis.
    - This involves identifying the specific system or subsystem that will be analyzed and determining its boundaries and interfaces with other systems.

- The analysis team identifies potentially hazardous conditions associated with the system. This can include failures, malfunctions, operating errors, or external events that could lead to an unsafe situation.

- Once the hazardous conditions are identified, the analysis team conducts a thorough analysis of each hazard.
    - This includes examining the causes, consequences, and contributing factors associated with each hazard.

- The team assesses the level of risk associated with each hazard. Risk is typically evaluated based on the severity of the consequences, the likelihood of occurrence, and the exposure of occupants or the environment to the hazard.

- Based on the risk assessment, safety requirements are established to mitigate or eliminate the identified hazards.
    - These requirements define the necessary design features, system behavior, operational procedures, or other measures to ensure the system operates safely.

- The safety requirements are then verified and validated through various means, such as analysis, testing, and simulation. This step ensures that the implemented mitigations effectively address the identified hazards.

- Throughout the process, all findings, analyses, and decisions are documented. The analysis results are compiled into a formal report, which is reviewed internally and may be subject to external regulatory scrutiny.

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

Online can support your company's specific objectives.