EASA Aircraft Certification CS-25 - Considerations Related to the Role of a Functional Hazard Assessment (FHA)

Sofema Online (SOL) www.sofemaonline.com considers the role of a Functional Hazard Assessment as part of the Aircraft Type Certificate Certification Process.

Introduction

A Functional Hazard Assessment (FHA) is a systematic evaluation conducted to identify and assess potential hazards associated with the functions and behavior of a system or process. It is commonly to ensure safety and mitigate risks.

The FHA focuses on analyzing the functional aspects of a system to identify potential hazards and their potential consequences.

An FHA is typically performed during the early stages of system development, such as during the design phase or when significant changes are made to an existing system. It is essential to conduct the FHA early on to identify potential hazards before they become more difficult and costly to address during later stages.

FHA provides insights into potential hazards, by understanding the potential hazards and their consequences, organizations can implement measures to reduce the risks associated with the system.

Note - Conducting an FHA can be a complex process, especially for large and intricate systems. Analyzing all potential functional hazards requires expertise and a thorough understanding of the system.

What is the difference between Failure Modes and Effects Analysis FMEA and FHA?

- The Functional Hazard Assessment FHA looks at what major failures of function can occur, the effects of those failures, the risk associated with them, and the safety criteria we must meet to make that risk acceptable.
- The Failure Modes and Effects Analysis FMEA looks at what happens when each component of the system fails in various ways.

Note regarding Preliminary Hazard Analysis (PHA)

A PHA is conducted at the early stages of system development to identify hazards and their potential causes. It provides a high-level overview of the hazards, whereas an FHA delves deeper into the functional aspects of the system.

Note Regarding Fault Tree Analysis (FTA)

FTA is an analysis technique used to identify the causes of an undesired event or hazard. It focuses on identifying specific failure modes and their combinations that could lead to hazards.

- In contrast, an FHA concentrates on the functional behavior and potential hazards associated with the system.

What is a Functional Hazard Analysis (FHA)?

Functional Hazard Assessment (FHA) is a top-down iterative process, initiated at the beginning of the development or modification of a System.

- The objective of the FHA process is to determine: how safe does the system need to be. The process identifies potential failures modes and hazards.
- The process identifies potential failures modes and hazards. It assesses the consequences of their occurrences on the safety of operations, including aircraft operations, within a specified operational environment.
- The FHA process specifies overall Safety Objectives of the system, i.e. specifies the safety level to be achieved by the system.

General Notes Conducting an FHA

- The essential pre-requisite for conducting an FHA is a description of the high level functions of the system – such as would typically be specified in an operational concept document.
- FHA is therefore first conducted during the System Definition phase of the system life cycle.
    - The purposes of the System Definition phase are to establish basic operational objectives for the system within its specified operational environment, to identify the functions required to achieve these objectives, and to specify system and interfaces (between functions and with the environment) requirements.

- FHA is typically performed before the functions have been allocated to equipment, procedures or people elements
    - It considers what the proposed system will do, rather than how these elements should implement the functions.
    - FHA results will be used to support the process of function allocation.

Note - In practice, however, development and assessment usually proceed in parallel, and some allocation of functions may already have been determined by practical constraints – especially where an existing system is being modified.

FHA Initiation

Develop a level of understanding of the system, its operational environment and, if appropriate, its regulatory framework, sufficient to enable the safety assessment activities to be satisfactorily carried out.

- System Description
- Operational Environment Description
- Regulatory Framework
- Applicable Standards
- Other Inputs (e.g., other FHA results, hazard database, incident investigation reports, lessons learned, etc.)
- Gather all necessary information describing the system.
- Review this information to establish that it is sufficient to carry out the FHA.
    - If not available, describe the operational environment of the system.
- Identify and record assumptions made.
- Formally place the input information under configuration management.

FHA Planning

- Define the objectives and scope of the FHA, the activities to be carried out, their deliverables, their schedule and the required resources.
- Initial Safety Plan
- Identify and describe the more specific activities for each FHA step.
- Submit the FHA plan to review to provide assurance of its suitability.
- Formally place the FHA plan under configuration management.

FHA Safety Objectives

- To identify all potential hazards associated with the system;
- To identify hazard effects on operations, including the effect on aircraft operations;
- To assess the severity of each hazard effect;
- To specify Safety Objectives, i.e. to determine the maximum frequency of hazard's occurrence;
- To assess the overall foreseen (future) risk associated to introducing the change or new system.

Notes Concerning Information gathered or derived in the FHA Initiation step

- Severity Classification Scheme
- Organisation Risk Classification Scheme
- Safety Objective Classification Scheme
- For each system function and combination of functions:
    - Identify potential hazards
    - Identify hazard effects
    - Assess the severity of hazard effects.
    - Specify Safety Objectives.
    - Assess intended aggregated risk.
    - List of hazards, with the rationale for the severity classification of their effects

FHA Verification

- To demonstrate that the set of Safety Objectives meet the Organisation Safety Target, i.e. the overall acceptable level of risk.
    - Information gathered or derived during the FHA steps;
    - Initial Safety Plan and FHA Plan;
    - Intermediate and final outputs of the FHA process.
    - Review and analyse the results of the FHA process.

FHA Validation

- Review and analyse the Safety Objectives to ensure their completeness and correctness;
- Review and analyse the description of the operational environment to ensure its completeness and correctness;
- Review, analyse, justify and document safety-related assumptions about the system, its operational environment and its regulatory framework to ensure their completeness and correctness.
- Review and analyse traceability between functions, failures, hazards, hazard's effects and Safety Objectives.
- Review and analyse the credibility and sensitivity of derived Safety Objectives to assumptions and risk.

FHA Assurance Process

- To provide assurance and evidence that all FHA activities (including FHA Verification and FHA Validation) have been conducted according to the plan;
- To ensure that the FHA process as described in the FHA Plan is correct and complete.
    - Information gathered or derived during the FHA steps;
    - Initial Safety Plan and FHA Plan;
    - Intermediate and final outputs of the FHA process.
    - Ensure that FHA steps are applied;
    - Ensure that assessment approaches are applied;
    - Ensure that all outputs of the FHA steps, including FHA Verification, FHA Validation and FHA Process Assurance are formally placed under configuration management;
    - Ensure that any deficiencies detected during FHA Verification or FHA Validation activities have been resolved;
    - Ensure that the FHA process would be repeatable by personnel other than the original analyst(s);

- Ensure that the findings have been disseminated to interested parties;
- Ensure that the outputs of the FHA process are not incorrect and/or incomplete due to deficiencies in the FHA process itself.

Documentation

Document the results of the FHA process (including the results of FHA Verification, FHA Validation and FHA Process Assurance activities);

- Formally place the FHA documentation under configuration management;
- Disseminate the FHA documentation to all interested parties.

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