SOFEMA
AVIATION SERVICES

Understanding Safety Assurance in an EASA Part 21 J Design Organisation, Monitoring, Measurement, and Management of Change

Sofema Online (SOL) www.sassofia.com considers the key aspects of the EASA Part 21J Safety Management System – Safety Assurance element.

Introduction

For EASA Part 21 J design organisations, safety assurance through monitoring, measurement, and management of change is fundamental to maintaining airworthiness and regulatory compliance.

- By embedding robust safety management practices into everyday activities, organisations can proactively manage risks, ensure the effectiveness of safety controls, and promote a strong safety culture.

- The regulatory framework set by EASA provides a structured approach to achieving these goals, ensuring that design organisations can safely manage changes and continuously improve their safety performance.

Safety assurance within a EASA Part 21 J design organisation includes elements of monitoring, measurement, and management of change.

- The overarching aim is to ensure that safety objectives are met, hazards are identified, and risks are mitigated in line with regulatory requirements.

- For a design organisation, this means managing the safety of design changes and ensuring continued compliance with airworthiness standards.

Here we consider monitoring, measurement, and change management, within the context of EASA's regulatory framework.

Monitoring Safety Performance

Monitoring safety performance is a key component of the Safety Management System (SMS).

- The objective is to ensure that safety objectives are consistently achieved, emerging risks are identified, and potential hazards are effectively managed to maintain airworthiness and regulatory compliance.
- As stipulated in AMC1 21.A.239(c), design organisations must establish a structured and systematic process for monitoring safety performance, which plays a crucial role in sustaining the integrity of the design and its airworthiness throughout its lifecycle.

Purpose of Safety Monitoring in Part 21J Organisations - The primary purpose of monitoring safety performance is to:

- Ensure compliance with safety and regulatory requirements
    - **Monitoring** - ensures that the design management system is functioning in accordance with EASA regulations, particularly the requirements under Part 21 Subpart J.
    - **Identify deviations from safety objectives** - Continuous monitoring helps detect any deviation from predefined safety objectives, allowing timely interventions to mitigate risks.
    - **Detect emerging hazards** - Monitoring systems are designed to capture and analyse data to identify hazards that may not have been apparent during initial design stages, particularly as the product is deployed in varied operational environments.
    - **Assess the effectiveness of safety controls:** Monitoring is crucial for assessing whether safety controls implemented during the design process remain effective throughout the product's lifecycle.

Structured Safety Monitoring Process (Per AMC1 21.A.239(c))

According to AMC1 21.A.239(c), a Part 21J design organisation must implement a structured and formalised monitoring process. The design of this system should integrate the following elements:

Establishment of Safety Indicators

- Safety Performance Indicators (SPIs) are essential metrics that quantify the organisation’s safety performance.
- These indicators can include data points such as
    - The frequency of safety occurrences,
    - Non-compliance with airworthiness standards, or
    - Deviations during audits.
- SPIs should be measurable, relevant, and aligned with the organisation’s safety objectives. Examples of SPIs include:
    - Rate of design errors or inconsistencies found during compliance verifications.
    - Number of safety-related design changes.
    - Frequency of safety incidents during testing or product certification.

Data Collection and Analysis

- The collection of safety data is fundamental to the monitoring process.
    - This data can be gathered from various sources, including incident reports, airworthiness directives, safety audits, design reviews, and feedback from operators and users.

- Data collection methods should be both quantitative and qualitative, allowing the organisation to build a comprehensive view of its safety performance.
- Data points might include:
  - Error reports,
  - System failures, or
  - Deviations from expected performance during flight testing.

Analysis of safety data should focus on identifying trends, patterns, and potential hazards. Statistical methods and safety risk management tools like Fault Tree Analysis (FTA) and Failure Mode Effects Analysis (FMEA) are commonly used in the aviation industry to understand the root causes of safety issues.

Audits and Inspections

- Internal audits and inspections are an essential part of safety monitoring in a Part 21J organisation.
- These audits are conducted to assess the integrity of the design process and the effectiveness of the safety management system.
- Audits should:
  - Review compliance with design standards and airworthiness requirements.
  - Assess the effectiveness of safety procedures, particularly those related to hazard identification and risk management.
  - Identify any gaps or weaknesses in the safety controls or design practices.
  - External audits by EASA or other aviation authorities also play a role in ensuring that the organisation adheres to regulatory requirements.

Monitoring of Subcontractors and Suppliers

In a design organisation, it is common to subcontract certain design or testing activities to external suppliers. According to AMC1 21.A.239(c), the design organisation remains responsible for the monitoring of safety performance in these activities.

- Supplier performance should be monitored to ensure that subcontracted work complies with safety and design requirements. Audits, performance reports, and safety feedback mechanisms should be used to verify the adequacy of external contributions to the design process.

Key Considerations for Effective Monitoring

Real-time monitoring tools enable quicker responses to emerging risks, reducing the time between hazard identification and mitigation.

- **Real-Time Monitoring Tools**

- Systems such as Flight Data Monitoring (FDM) and Aircraft Condition Monitoring Systems (ACMS) are used to capture and analyse operational data, which can provide insights into the performance of the design under real-world conditions.

- **Trend Analysis and Predictive Monitoring**
  - Trend analysis is a proactive monitoring technique that allows organisations to detect early signs of potential issues.
  - By reviewing data over time, design organisations can identify patterns that indicate safety risks before they escalate into incidents.
  - Predictive monitoring uses data analysis to forecast possible safety concerns based on historical trends.
    - This is particularly useful for identifying risks that might arise as the design interacts with different operational environments or as the product ages.

- **Feedback Loops and Continuous Improvement**
  - An effective monitoring system must include feedback loops that allow information to flow from the operational environment back to the design team.
  - This feedback helps in assessing the performance of the design and in identifying areas where improvements are necessary.

- Organisations should establish processes for continuously improving the design management system based on the feedback received during safety monitoring.
  - This could involve updating design procedures, refining safety objectives, or improving communication with stakeholders.

Risk-Based Monitoring

A risk-based approach to monitoring ensures that the focus is placed on areas of the design with the highest safety impact. High-risk areas, such as critical systems or components that could affect airworthiness, should receive more attention in the monitoring process.

- Risk-based monitoring helps allocate resources efficiently, ensuring that the most significant safety concerns are addressed without overburdening the system with unnecessary checks.

Challenges in Monitoring Safety Performance

- **Data Overload -** One of the challenges in monitoring safety performance is managing the sheer volume of data that can be collected.

- Organisations must have the systems and processes in place to filter, prioritise, and analyse large datasets without losing sight of key safety indicators.
    - Automated systems and data analytics tools can help streamline this process, but human oversight is essential to ensure that the right conclusions are drawn from the data.

Human Factors

- Human factors play a significant role in the effectiveness of safety monitoring.
- Monitoring systems must consider human performance, including the potential for human error in both the design process and in the monitoring activities themselves.

Note - It is also important to ensure that employees are fully trained in safety monitoring procedures and are aware of their role in maintaining safety performance.

Resistance to Reporting

- A non-punitive safety reporting culture is vital for effective safety monitoring.
- Employees must feel confident that reporting errors, incidents, or near misses will not result in negative consequences.
    - This ensures that all relevant safety data is captured and used for risk management.

Integration with the Safety Management System (SMS)

Monitoring safety performance should not be viewed in isolation but as an integral part of the overall Safety Management System (SMS).

- It should be closely linked with other SMS components such as risk management, safety assurance, and safety promotion.
- Information gathered during monitoring activities should feed into risk assessments and decision-making processes across the organisation.
- **Safety Risk Management:** Monitoring activities identify emerging risks and provide the data needed to conduct detailed risk assessments.
- **Safety Assurance:** The results of monitoring activities are used to evaluate the effectiveness of safety controls and identify areas where improvements are necessary.
- **Safety Promotion:** Monitoring outcomes should be communicated throughout the organisation to promote safety awareness and encourage continuous improvement.

Management of Change

Changes in the design organisation—whether they involve personnel, processes, technology, or regulations—can pose new safety risks. The management of change

(MoC) process ensures that any modifications within the organisation are evaluated for their safety implications before implementation

MoC Process:

- **Risk Assessment:** Any proposed changes should be subjected to a rigorous risk assessment to determine their impact on safety. This includes evaluating both the likelihood and severity of potential hazards introduced by the change.
- **Human Factors Consideration:** MoC processes should also consider the impact of changes on human performance. For instance, changes in technology, workflow, or staffing can introduce human factors that affect the overall safety of the design
- **Safety Culture:** Engaging personnel at all levels ensures that the organisation maintains a strong safety culture, even during periods of significant change. Open communication and continuous safety promotion activities support this

Regulatory Requirements: EASA Part 21 J Compliance

Under EASA Part 21 J, design organisations must maintain a Design Management System (DMS) that integrates safety management elements into their core activities.

- The safety management system (SMS) must focus on proactive hazard identification, risk assessment, and the mitigation of risks to an acceptable level.
- The regulations mandate the continuous monitoring of all design activities to ensure that safety risks are effectively managed.
    - Importantly, the management of change must be a documented process that aligns with the organisation’s hazard identification and risk management practices

Best Practices for Effective Safety Assurance

- **Proactive Hazard Identification:** Organisations should employ both reactive and proactive methods for hazard identification. Proactive methods include design reviews and audits that anticipate potential failures, while reactive methods involve investigating past incidents
- **Clear Communication Channels:** Safety-related information must be effectively communicated throughout the organisation to ensure that all stakeholders understand safety objectives, risks, and the actions taken to mitigate those risks
- **Ongoing Training and Competency Management:** Safety assurance relies on competent personnel who are continuously trained in the organisation's safety policies, objectives, and procedures

Next Steps

For more information, visit the following training course: EASA Part 21 Subpart J Safety Management System Implementation – 2 Days or contact us at team@sassofia.com.