SOFEMA
AVIATION SERVICES

General Introduction to Probability Determination Methods

Sofema Aviation Services (SAS) www.sassofia.com considers the primary techniques to analyze the potential risk of a system, product or process.

Introduction

Determining safety during certifications often involves assessing the potential risks associated with the use or operation of a particular system, product, or process.

A number of methods are available to quantify the risk associated with the particular system or product undergoing certification, allowing certifying authorities and organizations to make informed decisions about its safety.

At its core, Probability Methods is the study and application of mathematical methods that deal with the quantification and management of uncertainty. These methods allow us to assess the likelihood of a specific event occurring, given a set of initial conditions or states. In the realm of safety assessment, this could be anything from the probability of an accident during manufacture, to the likelihood of a system failure during in service operation or a latent software error.

Probabilistic methods are extensively used to estimate these risks and make informed decisions. Consider the following examples

Probabilistic Risk Assessment (PRA):

- This is a systematic and comprehensive methodology to evaluate risks associated with a complex system.
- The aim is to answer three fundamental questions:
  - What can go wrong,
  - How likely is it, and
  - What are the consequences?
- In the context of safety certification, PRA is used to identify potential failure modes, their causes and effects, their probabilities, and their potential impacts.

Positive Benefits of PRA:

- PRA offers a systematic way to quantify risks, determining both the probability and consequences of adverse events. This can provide vital information for decision-making and risk management processes.

- PRA can help in identifying which elements or events contribute the most to the overall risk. This can allow organizations to focus on mitigating these high-risk components to improve safety.
- The outputs of a PRA can be valuable in supporting risk-informed decisions about design changes, operational procedures, safety measures, or maintenance strategies.
- Conducting a PRA can support the compliance requirements for demonstrating safety system conformity.
- By identifying the areas of highest risk, PRA can help organizations to allocate their resources more effectively and efficiently, focusing on areas that will have the most impact on risk reduction.

Potential Issues with PRA:

- PRA models can become extremely complex, especially for large systems with many interacting elements.
    - This can make the PRA difficult to develop, understand, and communicate.
- PRA relies on a number of assumptions, and there is often significant uncertainty in the input data (such as failure rates).
    - This can limit the accuracy of the PRA results.
- Human errors can have a major impact on system risk, but they are difficult to quantify and can often be underestimated in PRA models.
- The probabilistic nature of PRA can give a false sense of precision or certainty. While PRA can indicate which events are more likely to occur, it can't predict specific future events.
- There's a risk that a successful PRA might lead to complacency, with a belief that all risks have been identified and are being managed. However, there will always be unknown risks that haven't been included in the PRA.

Fault Tree Analysis (FTA):

- This is a top-down, deductive failure analysis in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events.
- This method explores various combinations of system failures using probabilities to calculate the likelihood of the top event (i.e., the main failure being analyzed).

Positive Benefits of Fault Tree Analysis (FTA):

- FTA allows for systematic identification and analysis of various potential failure modes in a system.
    - This approach promotes a comprehensive understanding of the system's structure and interactions.
- By identifying potential points of failure, FTA can help organizations avoid costly system failures.
    - This analysis also provides insight into how multiple failures could interact, which can help prioritize prevention efforts.
    - Once the fault tree is built, it can be used repeatedly for similar systems or adapted for other systems. (This can save time in the analysis of new systems or in re-analysis if a system is modified.)
- Fault trees can provide both a qualitative understanding of failure mechanisms and, with sufficient data, a quantitative estimate of system reliability.

Potential Issues of Fault Tree Analysis (FTA):

- Building a fault tree requires a detailed understanding of the system being analyzed.
    - Incorrect assumptions about the system's operation can lead to incorrect conclusions about the risks of failure.
- The fault tree can become extremely complex for large systems.
    - This can make the tree difficult to understand or manage, and increases the risk of errors in the analysis.
- Quantitative analysis requires failure data that is often difficult to obtain, particularly for new or unique systems.
    - This limits the ability to predict the absolute likelihood of system failures.
- While FTA can analyze hardware and software failures, it may not fully account for human errors, which can also cause system failures.
- Creating and maintaining a fault tree can be time-consuming and expensive, especially for large or complex systems.

Event Tree Analysis (ETA):

- Event tree analysis is a forward, bottom-up, logical modeling technique for both success and failure events.
- It's used to evaluate the impact of the failure of individual system components or operations.
- Each branch of the tree represents a possible event or decision outcome and each node on the tree represents the outcome of a test.

Benefits of Event Tree Analysis:

- ETA provides a systematic method to predict the possible outcomes of an initiating event. It can help visualize the course of actions, enabling a comprehensive prediction.
- By using statistical data, ETA allows the assignment of probabilities to each branch of the tree. This helps in assessing the overall risk or reliability of a system.
- By analyzing the branches of an event tree, critical sequences leading to undesired outcomes can be identified.
    - This aids in risk management and mitigation strategies.
- ETA helps in understanding the interrelation between different events, offering a comprehensive view of complex systems.
- It helps in optimizing safety measures by visualizing the effectiveness of various preventative and mitigative measures.

Issues with Event Tree Analysis:

- ETA requires significant, reliable data to estimate probabilities accurately. In certain situations, sufficient or accurate data may not be available, leading to potential inaccuracies.
- For complex systems with numerous potential initiating events and outcomes, the event tree can become very large and complex, making it difficult to create and interpret.
- The results of an ETA are dependent on the quality and reliability of the input data.
    - Uncertainty in input data can lead to uncertainty in the output.
- ETA can sometimes oversimplify complex processes due to its high-level nature. It may not capture intricate details of specific processes.
- ETA is subject to the biases of those creating the tree, as they select which events to include and how to estimate probabilities.
- Creating a detailed and accurate event tree can be a time-consuming process, especially for complex systems with numerous potential events and outcomes.

Reliability Analysis:

- This involves estimating the likelihood that a system or component will perform its intended function without failure over a specified period of time under certain conditions.
    - Metrics such as Mean Time Between Failures (MTBF), Mean Time to Failure (MTTF), and Failure Rate (λ) are calculated to represent reliability.

- The associated probabilities of these metrics are used in the safety certification process.

Benefits of Reliability Analysis:

- Reliability analysis provides insights into potential points of failure, enabling designers and engineers to improve system design to increase overall reliability.
- It allows organizations to assess and manage the risks associated with system or component failure, thereby reducing potential losses.
- It can identify problems early in the design or production process, reducing the costs associated with rework, recalls, or repairs.
- Within Aviation, enhancing system reliability can significantly improve safety, protecting human lives and the environment.
- Reliable products mean fewer failures and less downtime, leading to improved customer satisfaction and trust.

Issues with Reliability Analysis:

- Reliability analysis can become complex when dealing with intricate systems with many interacting components.
- The complexity increases further when considering different failure modes and their interdependencies.
- The analysis often depends on the availability and accuracy of failure data. In many cases, this data is either unavailable or unreliable, leading to uncertainty in the analysis.
- Reliability analysis, especially for complex systems, can be resource-intensive. It may require significant amounts of time, skilled personnel, and sophisticated software tools.
- In order to make the analysis feasible, certain assumptions and simplifications might be made, which can lead to inaccurate results if these assumptions do not hold.
- If not conducted properly or if results are misinterpreted, reliability analysis could give a false sense of security, potentially leading to unanticipated failures.

Monte Carlo Simulation:

- This is a computerized mathematical technique that allows people to account for risk in quantitative analysis and decision making.
- It provides a range of possible outcomes and the probabilities they will occur for any choice of action.

Benefits of Monte Carlo Analysis:

- Monte Carlo analysis provides a probabilistic assessment of system or component performance. It helps quantify the likelihood of failure and provides valuable insights into the reliability and performance characteristics of the system.
- Monte Carlo analysis considers uncertainty in the input parameters by using probability distributions instead of deterministic values.
    - This allows for a more realistic representation of the system's behavior and a better understanding of the potential outcomes.
- The technique allows for a comprehensive analysis of the system's performance over a specified period of time and under various conditions.
    - It can incorporate complex relationships between variables, enabling a thorough examination of potential failure scenarios.
- Monte Carlo analysis facilitates sensitivity analysis by identifying the most critical parameters or variables that affect the system's performance.
    - This information helps focus efforts on improving the reliability of those components or reducing uncertainty in key inputs.
- Monte Carlo analysis provides decision-makers with valuable information for risk management and decision support.
    - By quantifying the likelihood of failure and the associated uncertainties, it enables informed decision-making, such as identifying areas for improvement or selecting optimal designs.

Issues with Monte Carlo Analysis:

- Monte Carlo analysis involves running a large number of simulations, which can be computationally intensive and time-consuming, especially for complex systems or when evaluating numerous variables.
- Adequate computational resources are required to perform the analysis efficiently.
- Monte Carlo analysis relies on assumptions and simplifications to model the system accurately.
    - The accuracy of the results depends on the quality of these assumptions, and any inaccuracies or oversights in the model can introduce bias or errors into the analysis.
- The reliability of Monte Carlo analysis heavily relies on the availability and quality of data used to define input parameters and their probability distributions.
    - Insufficient or inaccurate data can lead to unreliable results and inaccurate estimations of system performance.
- Developing an accurate and comprehensive model for Monte Carlo analysis can be challenging, especially when dealing with complex systems with numerous interdependencies.

- Defining appropriate probability distributions, establishing relationships between variables, and accounting for all relevant factors require expertise and careful consideration.

- Interpreting the results of Monte Carlo analysis requires a thorough understanding of statistical concepts and their implications.
  - Misinterpretation or misunderstanding of the output can lead to incorrect conclusions or improper decision-making.

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