MEETING RELIABILITY REQUIREMENTS FOR ROTOR ICE PROTECTION SYSTEM DESIGN

Paweł GOLEC, Józef BRZĘCZEK

PZL Mielec Sp. z o.o., ul. Wojska Polskiego 3, 39-300 Mielec
e-mail: p_golec@pzlmielec.com.pl, j_brzeczek@pzlmielec.com.pl

Abstract

Increasing cost of rotorcraft maintenance forces transport companies to utilize their rotorcraft fleet to the fullest. This means that the most successful rotorcraft production company is the one that can provide rotorcraft that can operate in wider range of weather conditions than competition.

Air transport authorities define requirements for both rotorcraft performance during flight in icing conditions and reliability of ice accretion protection systems. At the same time production company management requires that production, and development costs are as low as possible.

This paper will focus on problems of meeting requirements of rotorcraft ice protection systems reliability using various types of reliability analyses that will help keep the system as simple and inexpensive as possible and are required in certification process of ice protection system.

Key words: rotorcraft reliability, system safety assessment, CCA, FHA, SSA, FMEA, FTA

PROJEKTOWANIE UKŁADU OCHRONY WIRNIKA PRZED OBLODZENIEM ZGODNIE Z WYMAGANIAMI NIEZAWODNOŚIOWYMI

Streszczenie

Ciągłe zwiększanie się kosztów utrzymania wiropłatów wymusza na firmach transportowych maksymalne wykorzystanie możliwości posiadanej floty. Oznacza to, że producent wiropłatów, aby osiągnąć sukces musi dostarczać produkt, który będzie w stanie operować w szerszym zakresie warunków pogodowych, niż firmy konkurencyjne.

Organy nadzoru lotniczego określają zarówno wymagania dla własności lotnych wiropłatów w czasie lotu w warunkach oblodzenia oraz wymagania niezawodnościowe układu ochrony przed oblodzeniem. Jednocześnie zarządzający firmami produkującymi, wymagają, aby koszty produkcji i opracowania projektu były możliwie jak najniższe.

Niniejsze opracowanie skupia się na problematyce sprostania wymaganiom niezawodnościowym przy wykorzystaniu różnych typów analiz niezawodnościowych, które pozwolą na zaprojektowanie możliwie najprostszych i najtańszych układów, i które są wymagane w procesie certyfikacyjnym układu ochrony wiropłata przed oblodzeniem.

Słowa kluczowe: niezawodność wiropłatów, ocena ryzyka systemów, CCA, FHA, SSA, FMEA, FTA

1. AVIATION AUTHORITIES REQUIREMENTS REGARDING RELIABILITY

Certification Specifications (CS) issued by European Aviation Safety Agency (EASA) define reliability requirements in Certification Specifications for Small Rotorcraft paragraph CS-27.1309 and Certification Specifications for Large Rotorcraft paragraph CS-29.1309. The process of performing reliability analyses is often called system safety analysis or assessment, so to avoid confusing this process with System Safety Assessment analysis in this paper "reliability analysis" term will be used.

2. DEFINING CERTIFICATION BASIS

First thing that needs to be done is to define certification basis, that is which CS paragraphs rotorcraft must comply with.

Small rotorcaft is defined by maximum takeoff weight (MTOW) of 3 175 kg or less and nine or less passanger seats. Single engine, small rotorcraft is certified as Category B, multiengine can be certified as Category A, if some additional requirements are met, including CS-29.1309.

Large rotorcraft (MTOW greater than 3 175 kg) can be certified as Category A or B depending on MTOW and number of passanger seats. Rotorcraft with MTOW greater than 9072 kg and 10 or more passanger seats

must be certified as Category A. Any other multiengine rototcraft may be certified as Category B.

Any rotorcraft certified as Categoty B is allowed to fly in conditions of weather and light, and over such routes, which may permit a safe forced landing at any time of the mission, so if the goal is to aquire certification to fly into known icing (FIKI) the rotorcraft should be certified as Category A.

3. RELIABILITY REQUIREMENTS

According to subparagraph CS-29.1309 (b)(2) and CS-29.1309 (c) Category A rotorcraft must be designed that: *"(b)(2) For Category A rotorcraft: (i) The occurrence of any failure condition which would prevent the continued safe flight and landing of the rotorcraft is extremely improbable; and (ii) The occurrence of any other failure conditions which would reduce the capability of the rotorcraft or the ability of the crew to cope with adverse operating conditions is improbable. (c) Warning information must be provided to alert the crew to unsafe system operating conditions and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimise crew errors which could create additional hazards."* [1].

This requires, apart from conforming to good engineering practices, installation of failure warning devices and implementing special procedures; performing complex qualitative and quantitative analyses, and even ground, flight or simulation tests. Factors that needs to be taken into account are clearly defined in CS-29.1309 (d) *" (1) Possible modes of failure, including malfunctions and damage from external sources; (2) The probability of multiple failures and undetected failures; (3) The resulting effects on the rotorcraft and occupants, considering the stage of flight and operating conditions; and (4) The crew warning cues, corrective action required, and the capability of detecting faults."* [1]

Following analyses must be performed to show compliance with CS-29.1309 (b)(2), CS-29.1309 (c) and CS-29.1309 (d): rotorcraft level FHA, PSSA, FMEA, FTA, CCA and as a summary SSA.

4. BRIEF DESCRIPTION OF DIFFERENT TYPES OF RELIABILITY ANALYSES

4.1. Functional Hazard Assessment (FHA)

FHA is qualitative, high level assessment of rotorcraft or system functions and should be conducted at the beginning of rotorcraft development process as soon as basic functions or principles of operations of rotorcraft are defined. It identifies and classifies hazards associated with rotorcraft functions and combination of these functions whether it is complete or partial loss of function, or erroneous functionality and if crew is able to detect failure. Identified hazards are then classified according to the effect on the safety of the rotorcraft, its crew and passengers. This type of analysis can be performed at rotorcraft or system level and its output is the starting point for allocation of safety requirements.

4.2. Preliminary System Safety Assessment (PSSA)

Preliminary System Safety Assessment is a tool used to gather rotorcraft functional requirements, hazards descriptions associated with loss of each rotorcraft function, failures that contribute to loss of a particular function and reliability and design requirements for systems responsible for performing those functions.

Main purpose of PSSA is to serve as a design/certification process guidance. Based on FHA results PSSA defines hardware and software requirements for the designed system e.g. built in test, dissimilarity, monitoring, Flight Manual procedures, etc.

PSSA also include strategies for reliability analysis or certification process, such as what type of reliability analysis is must be performed for given system and what kind of tests must be done to confirm rotorcraft/system performance or analysis results.

4.3. System Safely Assessment (SSA)

SSA is a tool used for evaluation of the implemented design solution. It summarizes results of all reliability analyses, ground, flight or simulation test required to show satisfactory reliability levels of designed rotorcraft. It is not uncommon for PSSA that matured over time during design process to turn into SSA by simply stating that all rotorcraft/system performance, design, and reliability goals set by PSSA have been met.

4.4. Failure Modes and Effects Analysis (FMEA)

FMEA can be performed at system or item level depending on application and system complexity. Basic objective of FMEA is to identify possible elementary failures and effect of this failures on the higher level functions and rotorcraft; failure detection means; corrective actions to mitigate failure effects; situation in which failure can occur or take effect. There are two basic assumptions when performing FMEA; human error is not taken into consideration and only one failure occurs at a time.

FMEA has few variations;

Quantitative variation of FMEA is called Failure Modes, Effects and Criticality Analysis (FMECA). Apart from providing the same information as FMEA it also contains information about failure criticality and probability of failure occurrence.

Failure Modes and Effects Summary (FMES) groups all failures, identified in FMEA, that contribute to loss of particular function. FMECA and FMES outputs are used as inputs for FTA.

4.5. Fault Tree Analysis (FTA)

FTA is "top-down" process that gathers all failure modes that contribute to loss of particular function identified in FHA. Failure modes are then combined together into logic structure that shows combinations of elementary failures that are required, to produce top event. Analysis proceeds down the tree structure until Primary Events are identified. Primary Event is defined as an event that does not need to be broken down into finer detail to show compliance with reliability requirements.

FTA can be either qualitative and quantitative. Qualitative FTA simply shows dependences between system or failures, while quantitative FTA is used to determine probability of loss of examined function using Boolean logic. In most cases inputs for FTA are outputs of FMEA, FMES or FMECA for quantitative FTA.

4.6. Common Cause Analysis (CCA)

To satisfy reliability requirements independency between systems and failures must be shown. To identify factors that can contribute to loss of independency, or to show that risk associated with dependencies is acceptable a Common Cause Analysis (CCA) must be performed. CCA can be divided into three different types on analyses.

Zonal Safety Analysis (ZSA) takes into consideration place in the rotorcraft (zone) where elements of systems are installed. The objective is to ensure that the equipment pieces within each zone are installed with respect to design and installation, interference between systems, and maintenance error reduction standards.

Particular Risk Analysis (PRA) considers factors that might have influence on system, but originate outside the system and may influence several zones. Typical PRA would consider items like fire, failure of high energy devices (engine, APU, fans), high pressure bottles, duct rupture, high temperature air duct leakage, leaking fluids (fuel, water, battery acid, hydraulic), bird strike, lighting strike, flailing shafts, HIRF, hail, snow, etc.

Common Mode Analysis (CMA) show that faults identified in FTA and assumed to be independent are independent in reality. CMA takes into consideration the effects of specification, design, implementation, installation, maintenance, and manufacturing errors and environmental factors other than those already considered in the PRA.

5. RELIABILITY ANALYSES DURING DESIGN AND CERTIFICATION PROCESS

To meet all reliability requirements stated in paragraph 1309 save both time and money designated to rotorcraft development process reliability analyses must be started in correct order and at proper design advancement points. Since most of reliability analyses are iterative by nature it might be assumed, from reliability engineer point of view, that particular development stage is finished when all required analyses are completed.

Figure 1 shows when particular type of reliability analysis should be started as rotorcraft design matures over time. It is a based on SAE ARP 4761, January 12, 1996 *Figure 1 – Overview of Safety Assessment Process*.

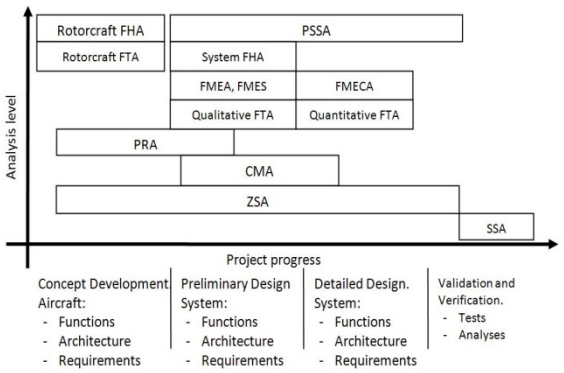

Figure 1. Reliability analyses in design process

6. RELIABILITY ANALYSIS IN THE RIPS DESIGNING PROCESS

To show how reliability analysis fits into actual development process, let us use Rotor Ice Protection System (RIPS) as an example.

Every reliability engineer must remember that the objective of reliability analysis is not to design system or device that would never fail , but to develop device that would fail in a safe way, by introducing hardware or software solutions, redundancy in critical areas or emergency procedures.

To make the description of process of performing clear let us divide it into steps.

6.1. Step 1

First step after adding additional system and function to the existing rotorcraft is system level FHA. Outputs of system FHA are then used to update rotorcraft level FHA and FTA.

It takes a lot of time and interdisciplinary knowledge, a lot of "what if?" questions, to prepare good FHA.

Since management decided that our rotorcraft should be able to fly in icing, designers must know what is the effect of ice accumulation on elements of our rotorcraft. This is done using engineering experience, ice accumulation and effect simulations and test. It will show us which parts of rotorcraft needs to be ice protected and how they need to be protected.

There are two types of ice protection systems: anti-icing – prevents ice accumulation, and de-icing – allows certain amount of ice to accumulate and then sheds this ice.

One of rotorcraft elements that will need ice protection is main rotor. The most effective and practical

rotor ice protection can be achieved using electrically heated mats attached to the rotor blades. Since heating all blades simultaneously would require tremendous amount of electrical power (assuming four blade rotor, 15 meters in diameter, would require about 140 kW of power) anti-icing system becomes impractical and we must divide rotor into zones that are heated in sequence. Another problem is rotor unbalance due to added mass of ice. Ice accumulated on one blade causes rotor unbalance. This means that we must de-ice two opposite rotor blades at the same time and in case of one blade heater failure we must make sure that opposite is disabled. This way electrical power that might be allocated to one blade is halved and we must divide blade into zones to keep de-icing effective and reconsider heating sequence to keep rotor balanced. We must also consider situation in which heater operates on power levels greater than required or cannot be switched off at all. Rotor will lose mechanical properties, if overheated, so this is potentially catastrophic situation and only overall rotorcraft characteristics can mitigate this hazard (rotor blade integrity loss warning devices, etc.).

At this point PRA does not make much impact on the system requirements, because factors that could affect de-icing mats would also affect the rotor itself, so these should have already been considered in original rotorcraft PRA and ZSA.

Having considered all possible threats to rotorcraft associated with rotor ice protection, we must classify those threats to allocate minimum failure rate requirements to elements responsible for providing rotor ice protection. This can be done using Table 1 based on SAE ARP 4761, January 12, 1996 *Table 1* that classifies failures into four categories depending on how failure affects aircraft, crew or passengers. Failure that leads to death or severe injury of crewmember or passengers is classified as Catastrophic. Failure monitoring systems are classified the same as monitored system. It also translates terms "extremely improbable" and "improbable" used in 1309 (b)(2)(i) and (ii) into minimal "per flight hour failure probability" value needed in quantitative FTA. An example of rotor blades ice protection FHA contains table 2.

Table 1. Failure Conditions Severity as related to Probability Objectives and Assurance Levels

Probability (Descriptive)	Probable	Improbable		Extremly Improbable
Probability (Quantitative)	$< 1.0x10^{-3}$	$< 1.0x10^{-5}$	$< 1.0x10^{-7}$	$< 1.0x10^{-9}$
Failure Severity Classification	Minor	Major	Hazardous	Catastrophic
Failure Condition Effect	- slight reduction in safety margins - slight increase in crew workload - some inconveniance to occupants	- significant reduction in safety margins or functional capabilities - significan increase in crew workload or in conditions impairing crew efficiency - some discomfort to occupants	- large reduction in safety margins or functional capabilities - higher workload or physical distress such that crew could not be relied upon to perform tasks accurately or completely - adverse effect on occupants	- all failure conditions which prevent continous safe flight and landing

Table 2. RIPS Functional Hazard Assessment

Failure Condition	Phase	Failure Effect	Classification
Inability to turn off main rotor RIPS –not annunciated	Flight	Possible main rotor damage due to overheating if incorrect heating mode is selected. Large reduction of safety margins. Advise crew to monitor cues that would indicate rotor damage.	Hazardous
Inability to turn off main rotor RIPS –annunciated	Flight	Possible main rotor damage due to overheating if incorrect heating mode is selected. Small reduction of safety margins. RIPS is disengaged by on/off switch, pulling out circuit breaker or OAT switch (OAT > 5°C)	Minor

6.2. Step 2

As soon as FHA is completed the Preliminary System Safety Assessment should begin. PSSA takes the output of FHA and expands it by items such as verification methods of failure classification and analyses required to prove that system meets minimum failure rate requirement, and hardware, software and procedure requirements.

Since PSSA serves as certification plan it should be agreed with Certification Authority to address all Authority's reservations regarding FHA failure classification and necessary tests and analyses. Another consequence of poorly prepared PSSA could be lack of safety essential piece of hardware, flight manual procedure or the opposite; situation with minor effect on flight safety would have complicated emergency procedure that only increase hazard level. It must be noted that all Catastrophic and Hazardous failures requires quantitative FTA to be done, but sometimes such analysis is required for Major failures if system has complex design.

Example of PSSA is shown below:

Table 3. RIPS Preliminary System Safety Assessment

Failure Condition	Phase	Failure Effect	Classification	Failure Rate	Verification	Design Requirements
Inability to turn off main rotor RIPS – annunciated	Flight	Possible main rotor damage due to overheating if incorrect heating mode is selected. Small reduction of safety margins.	Minor	$<1x10^{-3}$	RFM and RIPS FHA	- RIPS circuit breaker within pilots reach, - warning based on OAT and RIPS operation - RFM procedures associated with above

6.3. Step 3

This step takes the longest as it requires few iterative, mutually dependant analyses to be done. As system design matures and more details are available FMEA, FTA and CCA must be done. FMEA serves as design validation tool, taking into consideration failure modes such connector contact failure, contactor coil failure, jammed switch, etc. Knowledge on effects of such failures on system and rotorcraft gives useful feedback regarding system design, ensures that no single failure has Catastrophic effect and indicate areas that are susceptible to human errors. To make it easier to prepare FMEA it is possible to use FHA output as rotorcraft level effect of single item failure. This way both system FHA and FMEA can be verified for completion.

Qualitative FTA will provide information regarding system elements independency requirements and assigns failure rate budget.

CCA must be carried out to make sure that required system independency exists. Redundant system should be installed in different zones of the rotorcraft, but sometimes it is impossible, e.g. slip rings that connect blade heater with power source, are located on main rotor shaft. If this kind of situation is discovered and described in ZSA then PRA and CMA must be verified to find any factors that could affect both elements and establish requirements that will eliminate or mitigate hazard. Few examples: primary and stand-by systems, that are located in one junction box, must have separate connectors of different type or clearly marked to avoid assembly or maintenance error; ZSA indicates that components are located in zone with increased temperature, and cooling fans are needed.

6.4. Step 4

In this step FMEA is expanded to FMECA. Failure rates needed can be obtained by using accepted failure rate data sources, such as famous MIL handbooks e.g. MIL-HDBK 217F; flight and maintenance history; laboratory tests. This kind of data can be derived from similar systems on other aircrafts, but acceptable similarity level must be proven. Another information that is needed is failure mode ratio. Some items may fail in more than one way (mode) and we must determine the proportional probability of the item failing in that mode. Note that summarized probability of item failing in all modes should equal one.

FTA uses tree structure to show dependency levels between failures (FMECA output) and uses Boolean logic to calculate top event (FHA output) probability of occurrence. If FTA indicates that system does not meet reliability requirements there might be three reasons for this: deeper level FMECA must be conducted (e.g. from junction box level to junction box elements); dependency levels must be changed. Element common to primary and stand-by system greatly reduce total failure probability; system design must be simplified to reduce number of basic events contributing to top event, or redundant or monitoring system must be added.

6.5. Step 5

After all analyses, tests and simulations are finished it is time to verify the rotorcraft or system safety. This process is called System Safety Assessment. A very good starting material is Preliminary System Safety Assessment that's been updated as system development progressed. Primary difference between PSSA and SSA is that PSSA describes what needs to be done in order to develop reliable and safe system or rotorcraft, while SSA describes what have been done in order to develop reliable and safe system.

7. CONCLUSION

Tight cooperation of design and reliability engineers produces a design that might be complicated, with unusual technical solutions or have special requirements regarding production process but keeps development and certification process time and cost efficient and produces rotorcraft that is safe, reliable, easy to operate and maintain.

8. REFERENCES

[1] European Aviation Safety Agency: CS-29 Certification Specifications for Large Rotorcraft, Amendment 3, December 11, 2012.

[2] Society of Automotive Engineers: ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, January 12, 1996.