SAFETY ASSESSMENT OF AERO ENGINE THRUST REVERSER ACTUATION SYSTEMS

Dipl.-Ing. David Grasselt, Prof. Dr.-Ing. Klaus Höschler
Chair of Aero Engine Design
Traffic Engineering Institute
Brandenburg University of Technology Cottbus - Senftenberg
Siemens-Halske-Ring 14, 03046 Cottbus
Germany

Abstract

This paper deals with the safety assessment methods for an under-wing aero engine electrical thrust reverser actuation system (ETRAS). Different methods are addressed and compared. A short introduction to the technical system of a thrust reverser is provided; potential problems and their consequences are given. The huge effort spent on improving this kind of system's failure rate and subsequently reliability is underpinned. The applied safety assessment method is then summarised pointing out the relevant steps associated to this process. In the final section, some selected results of the whole assessment procedure are discussed. As a conclusion, the advantage of the chosen assessment method is summarised and shown from an industrial efficiency-orientated point of view.

Nomenclature

ARP	Aerospace Recommended Practice
BPR	Bypass Ratio
CCA	Common Cause Analysis
CC-TRU	Cascade TRU
CMA	Common Mode Analysis
DD	Dependence Diagram
ETRAS	Electronic TRAS
FHA	Failure Hazard Assessment
FMEA/S	Failure Mode&Effect Analysis/Summary
FMECA	Failure Mode&Effect Criticality Analysis
FTA	Fault Tree Analysis
FWD	Forward
HW / SW	Hardware (Parts) / Software
MA	Markov Analysis
PRA	Particular Risk Assessment
PSSA	Preliminary SSA
SAE	The Engineering Society For Advancing Mobility Land Air and Space (SAE)
SSA	System Safety Assessment
TRAS	Thrust reverser actuating system
TRU	Thrust Reverser Unit
ZSA	Zonal Safety Analysis

Introduction

The aero engine thrust reverser unit (TRU) is one of the components used to decelerate an aeroplane. The TRU is most often part of the Nacelle System. Exception to this are applications utilised also for the core engine, see Pratt & Whitneys F117-PW-100 engine used for the plane C17 Globemaster III.

Integrating a TRU to the powerplant of an aeroplane has several benefits:

- reduction of breaking distance [1],
- reduction of taxiing time (fuel burn),
- reduction of abrasive wear of the mechanical brakes of the landing gears [2],
- reduction of the maximum temperature of the mechanical brakes [2],
- shorter flight cycle intervals [2],
- Enhancement of safety during landing operation on wet or icy landing strips [1].

TRUs can be used to redirect the engines' bypass flow only, but also to redirect the mixed flow of the core and bypass system. Mixed stream TRUs are installed in the rear part of the powerplants' nacelle, near to or combined with the nozzle. This application is relevant for low bypass ratio (BPR) engines. High bypass ratio engines have TRUs that redirect the bypass flow only due to low thrust influence of the hot stream but high additional weight and complexity [1]. For cold stream applications there are typically two types of reverser that can be used: pivot door TRUs and cascade TRUs, see Figure 1 and Figure 2.

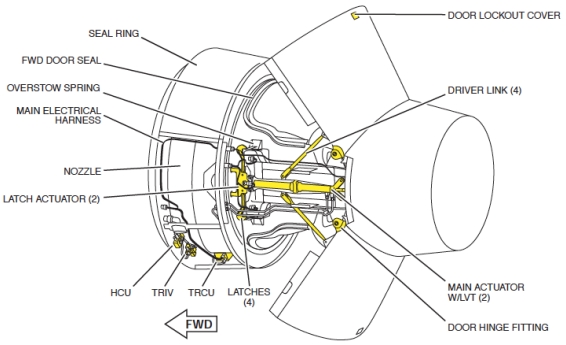

Figure 1 Pivot Door TRU [3]

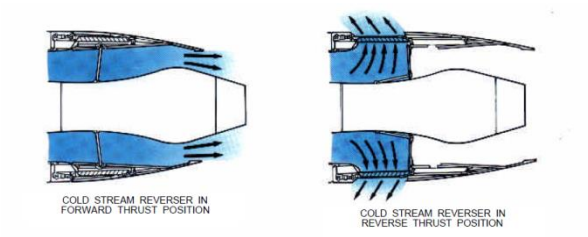

Figure 2 Cascade TRU [1]

Every thrust reverser unit consists of the following components:

- The structural parts (e.g. pivot door, cascade, blocker door, drag link, sliders),
- The thrust reverser actuation system (TRAS),
- The control system
- The indication system

Pivot door TRUs compared against cascade thrust reverser have fewer parts, a simple kinematic but heavy loads operating directly on the actuator.

The operation of the TRU is safety relevant. The probable consequences of a malfunction of such a system are well known. In 1991, an incident on the Lauda Air flight 004 caused 223 fatalities [4]. The plane broke up in flight as the reverser of the Pratt & Whitney 4000 engine inadvertently deployed. Investigations revealed "contamination in the hydraulic system could have been the cause" and led to blocking of "a directional control valve, causing it to activate the thrust reverser accidentally". As a consequence, the safe operation of a powerplant with a TRU has to be ensured through the design methodology. Furthermore the civil aviation authorities introduced several regulations that aim at stricter monitoring and increased safety mechanisms to reduce the probability of inadvertent deployment to less than 10^{-9} events per flight hour [5]. This is the allowed upper limit probability of catastrophic events for civil aviation [6]. This limitation, among others, leads to multiple independent locking mechanisms which additionally have to be redundant. The effort needed to meet such requirements can furthermore be made clear with the following example. The software of the TRU control system has to be redundant and independent as well to reduce the probability of programming or processing malfunctions. Therefore the code is developed by three different software developer teams, who have to use different programming languages. Each processing result of these three programs is then compared to each other to finally yield a statistically certain result.

The amounts of effort spent on securing safety relevant systems are a consequence of the knowledge about the behaviour of such a system. The effort is spent to deceed the failure rate to a certain required value. The knowledge about the system behaviour is based upon experience and the analysis results. Unfortunately, for new systems it is possible to reference on previous service experience only under limited conditions. Furthermore, a thorough analysis is able to bring failure modes and effects of a complex system to an easily understandable state.

Problem, Cause and Consequences

Modern technical systems, especially transportation systems are gradually increasing in their complexity. Mechanical components are combined with or controlled by electronic devices. This leads to failure modes that become dependent from interacting components. An individual is no longer able to analyse such systems from scratch. However, there are several options to recognise weak spots:

- Brainstorming
- Mind Mapping
- Tests on Part-, Component- or System-Level
- System Safety Assessment

An analysis method to gain knowledge about the failure modes and effects as well as the probability is a System Safety Assessment (SSA). The methodology of a SSA is described by the aerospace recommended practice 'ARP4761' of 'The Engineering Society For Advancing Mobility Land Air and Space' (SAE) as systematic and "comprehensive evaluation of the implemented system to show that relevant safety requirements are met" [7].

Significant effort is necessary to design a safe TRU. Although the expenses are high, the advantages outweigh the effort. The expenses are caused by the strong safety regulations by the authorities on the one hand. On the other hand the industrial requirements and realised components accomplish even higher

reliabilities. With the ARP 4761 methodology it is possible to understand very complex systems like aeroplanes, aero-engines or the TRU subsystem.

Systematic Analysis Method

The SSA can be described as a modular analysis approach for evaluating existing designs, see right side of Figure 3. A preliminary SSA (PSSA) can be used to evaluate proposed architectures and derive system or item safety and reliability requirements, left side of Figure 3. With the determined probability budgets it is possible to forward the architecture to the development department or an external supplier for further design realisation.

On top of the figure the specific system level is indicated: aircraft level, system level, item level. For each system and subsystem level (e.g. TRU, locking system, primary lock) the same tools are used to analyse the actual system level and to derive the inputs for the connected system level:

- List and classify failure conditions:
  Functional Hazard Assessment (FHA),
- Analyse failures qualitatively:
  Fault Tree Analysis (FTA), Dependence Diagram (DD), Failure Modes and Effects Analysis (FMEA),
- Analyse failures quantitatively:
  FTA, DD, Markov Analysis(MA), FMEA,
- Analyse failure coherence:
  Common Cause Analysis (CCA),
- Develop assurance levels for HW / SW,
- Verify incorporation of requirements to the design and testing process.

An FHA is a top level failure identification approach and defined as "a systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity". An FHA is usually performed at aircraft level and at system level [7]. Examples will be presented later in the next paragraph.

FTAs, DDs or MAs are used to analyse top-down the failure conditions identified in the FHA to a more detailed level of the design. Single (part) failures or combinations of these basic events are identified which can lead to a failure at system or aircraft level condition. Failure rates for the FTA/DD/MA basic events are received from FMEAs. The objective of these techniques can be to:

- Quantify probability of top event occurrence,
- Establish Hardware (HW) reliability budgets and development assurance levels,
- Assess the design modification impact,
- Identify required modifications,
- Prove compliance,
- Illustrate the significance of the Software (SW) with respect to failure condition classif.
- Establish crew and maintenance tasks.

Boolean logic gates (AND/OR/…) are used to show the relationship of failure effects to each other with an FTA. The logic gates can be replaced by (parallel/series) paths of a DD. To calculate the probability of the state of a system as a function of time an MA can be utilised.

As a counterpart an FME-Analysis can be used to investigate bottom up and systematic the failure

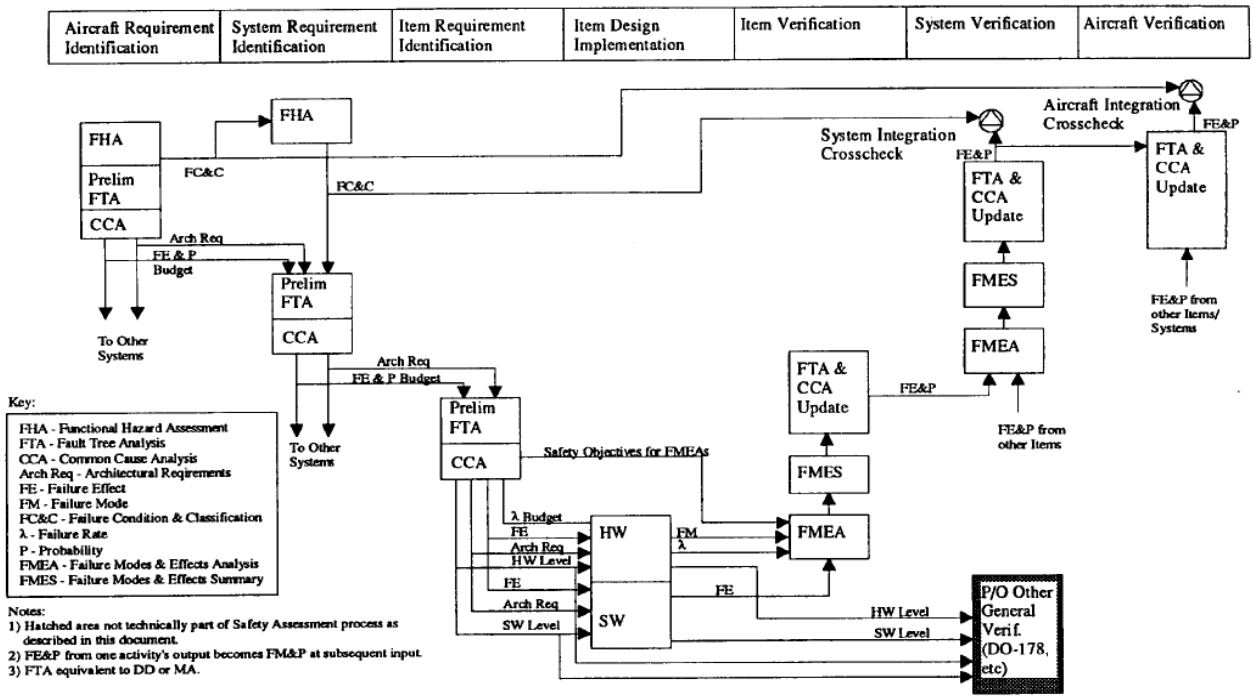

Figure 3 System Safety Assessment Diagram [ARP 4761]

modes of a system, item, or function and determine the effects on the higher system level. Grouping all single failure modes that produce the same failure effect gives an FMES.
Single basic failure events can depend on each other. The safety requirements may require independent functions, systems or items. A CCA

- can verify independence, or
- identify individual failure modes, or
- identify external events,

that lead to a severe failure condition. Three types of analysis within a CCA can be identified: a zonal safety analysis (ZSA), a particular risks analysis (PRA) and a common mode analysis (CMA).
The objective of a ZSA is to check that the safety requirements are met by the installed equipment with respect to:

- Basic installation
  (Design and installation requirements),
- Interference between systems
  (Failures of equipment and impact),
- Maintenance errors and effects.

Events outside of the system or item itself, which may influence the failure independence, are covered with the PRA. Typical PRA events are fire, leaking fluids, lightning, bird strike, etc.
Basic conjunctively (AND) combined events can be verified to be independent in the actual design applying a CMA. Especially effects of design, manufacturing, maintenance errors and failures of system components should be analysed with respect to their function and monitors [7]. Multiple item malfunctions can be caused due to use of common identical HW/SW.

Application

A PSSA can be used to derive item safety requirements for a proposed TRAS architecture. An SSA can be used to prove the actual TRAS to meet the probability requirements. Since the system which will be discussed is a concept study only, a PSSA has to be applied.

The FHA for this case is applied on system level with the aero engine as the considered system. The subsystem level FHA is focussing on the TRU and the items that will be investigated are parts of the TRAS. The analysis begins with identifying the functions of the subsystem that are reflected by its items. The main function of the TRAS is to move the parts of the TRU and to activate or deactivate the reverser.

The failure scenarios for a Cascade TRU (CC-TRU) in general can be:

a) Reverse Thrust cannot be activated
b) Reverse Thrust cannot be de-activated
c) Inadvertent activation of reverse thrust
d) Inadvertent de-activation of reverse thrust.

Each failure scenario has to be considered under several flight conditions. This is necessary to classify the failure condition. Since the classification of the scenarios a), b), and d) may have only minor effects, only the scenario c) will be discussed in this paper. The knowledge about the classification of the other three scenarios is a result of the FHA, too. These three scenarios will not be discussed in this paper.

The flight phase investigation results for scenario c) "Inadvertent activation of reverse thrust" are listed in Table 1.

Table 1 FHA - Inadvertent activation

Phase	**Effect**	**Class.**
Engine start	Abort Mission	minor
Taxi	No FWD Thrust	minor
Take off roll	Abort Start	major
Take off	Total loss	catastrophic
Climb	Total loss	catastrophic
Cruise	Total loss	catastrophic
Approach	Total loss	catastrophic
Landing	Total loss	catastrophic
Go Around	Total loss	catastrophic
Decelerate	No	negligible/no safety effect
Taxi	No FWD Thrust	minor
Engine turn off	No	negligible/no safety effect

As it can be seen, an event c) could end up with catastrophic or major consequences in several flight phases. A more detailed investigation is required. As stated in CS-E 510 (a) (2) a summary of major or hazardous engine effects must be made "together with an estimate of the probability of occurrence". This can be done with a more detailed investigation approach only, for example a FTA of the subsystem items.
The maximum allowed probability of effects is listed in Table 2 [8][9][10][11].

Table 2 Acceptable Probability of Failure Effect Classes

Failure Effect Classification	Qualitative Condition Probability Requirement	Quantitative Condition Probability Requirement
No effect	No requirement	-
Minor	Probable	$10^{-3} – 10^{-5}$
Major	Remote	$< 10^{-5}$
Hazardous	Extremely remote	$< 10^{-7}$
Catastrophic	Extremely Improbable	$<10^{-9}$

For hazardous effects it is allowed to prove the probability for the system at a total rate or for all individual failures. When the individual failure rate is applied the probability requirement is 10^{-8} per Engine flight hour [8]. The total rate is the result of the combination of all individual failure rates. The combination of individual failure rates is based on the logic operations in the FTA.
The probability of a conjunction (AND combination) of failures A and B can be analytically described using the function

$$\boldsymbol{P_{\wedge}(A \wedge B) = p(A) * p(B).} \quad (1)$$

The generalised form of equation (1) is

$$\boldsymbol{P_{\wedge} = \prod_{i=1}^{\infty} p_i.} \quad (2)$$

The probability of a disjunction (OR) of the failures A and B can be analytically described using the function

$$\boldsymbol{P_{\vee}(A \vee B) = p(A) + p(B) - p(A) * p(B).} \quad (3)$$

The generalised form of equation (3) is

$$\boldsymbol{P_{\vee} = 1 - \prod_{i=1}^{\infty}(1 - p_i).} \quad (4)$$

Finally the probability for events with non-equivalence (XOR) can be evaluated with

$$\boldsymbol{P_{\dot{\vee}}(A \dot{\vee} B) = p(A) + p(B) - 2 * p(A) * p(B)} \quad (5)$$

or the generalised form

$$\boldsymbol{P_{\dot{\vee}} = P_{\vee} - P_{\wedge}.} \quad (6)$$

The identified failure scenario has to be investigated based on the underlying TRAS architecture. The architecture investigated is a typical CC-TRU, see Figure 2. The parts identified belonging to an electric actuation system or having an influence on the system are:

- Control system,
- Primary lock,
- Secondary lock,
- Brake on driveshaft,
- Sensors,
- Cables,
- Actuator,
- Bearings,
- Motor,
- Shafts (flexible),
- Transmission.

An FTA is a top-down approach, see Figure 4. The diagram is created with respect to DIN 25424 [8]. The top level failure effect c) can be caused by a

1. Lock malfunction and a
2. Drive malfunction.

The effect c) is only possible when the failures 1 and 2 exist simultaneously (AND-Gate [13]). The probability of this combination can be evaluated by using equation (1).

Failure 1 can only occur with a

1.1 Malfunction of the primary lock, and a
1.2 Malfunction of the secondary lock, and a
1.3 Malfunction of the ‘brake-on-driveshaft’.

The probability of this conjunctive combined lock malfunction can be determined using equation (2). Because the failures of 1.1-1.3 have similar failure causes, only the fault tree for 1.2 is shown in Figure 4.

An event 1.2 can have its cause in either

1.2.1 A mechanical problem or
1.2.2 A corrupted signal.

The probability of the disjunctive (= OR-Gate [13]) combined lock malfunction can be determined using equation (3).

The failure 1.2.2 can appear when either

1.2.2.1 All sensors provide false data, or
1.2.2.2 The data handling is erroneous, or
1.2.2.3 A lead has a fracture

Thus, the basic events (= basic event [13]) of a lock malfunction are identified as failure 1.2.1, or 1.2.2.1, or 1.2.2.2, or 1.2.2.3 of each of the three locks. This means that at least three basic events are required to cause a lock malfunction, if the three lock subsystems are working independently, refer to the comments on CMA at the next page. Additionally a “drive malfunction” is required to cause the failure c) “Inadvertent activation of reverse thrust”.

The probability of failure 2 can be evaluated analogously to the approach for failure 1, using equation (4). It is obvious that a CMA can only be applied, when the failure root causes and the fault trees are well understood. Hence, the architecture has to be defined very detailed. The subitems of the conjunctively combined failure consequence c) and the subitems of the top level event 1 have to be investigated.

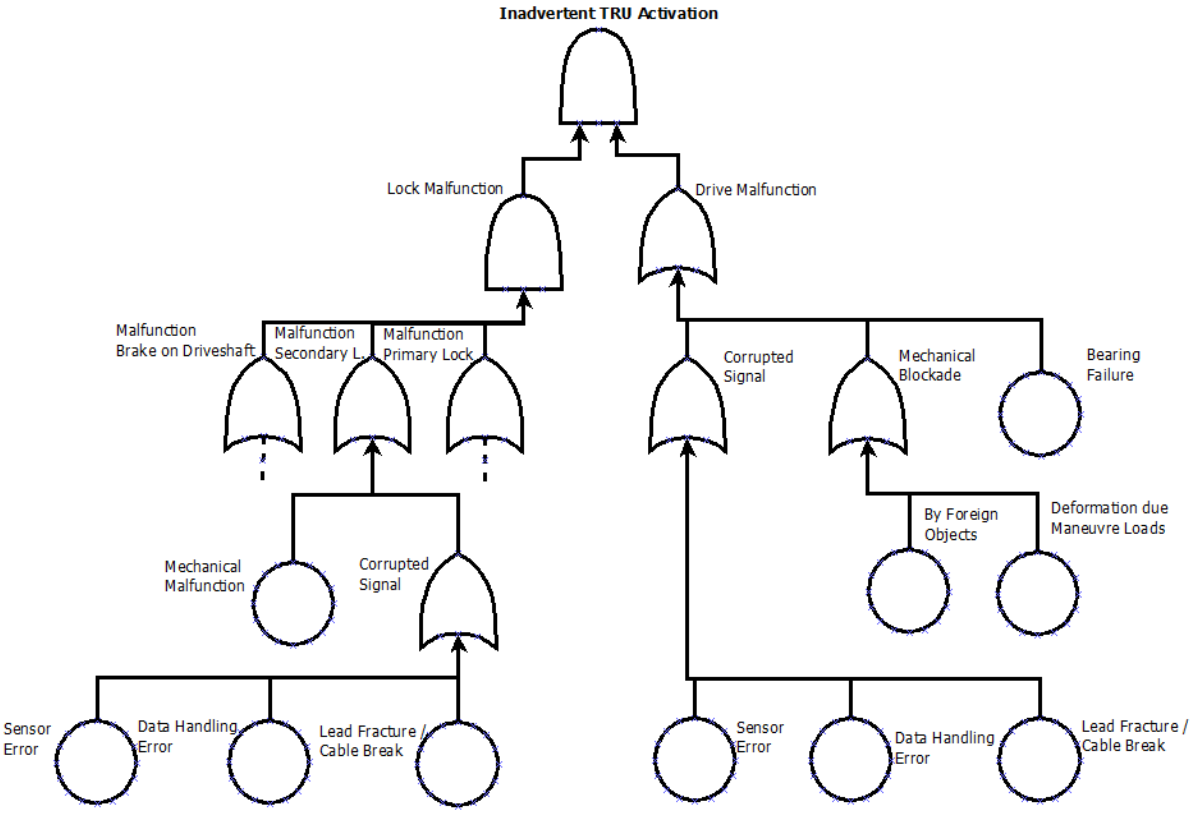

Figure 4 FTA and CMA of CC-TRAS

Functions and their monitors have to be independent from common

a) Design
b) Manufacturing
c) Maintenance
d) Failures of system components

failure modes. As an example, systems with identical hardware or software can be affected. The following common mode fault categories [7] should be analysed:

- Hardware Error,
- Software Error,
- Hardware Failure,
- Production / Repair Flaw,
- Situation Related Stress (abnormal conditions),
- Installation Error,
- Requirements Error,
- Environmental Factors,
- Cascading Faults,
- Common External Source Faults.

These categories and potential effects can be used to provide requirements for the system architecture.

The design effects can be eliminated introducing different types of subsystems, e.g. a different type of lock system to avoid a lock malfunction caused by design effects. In case of the failure level of an Inadvertent TRU Activation and its subitems it can be stated that a design effect can be neglected as long as a lock malfunction isn't possible and cables from redundant systems (locks and drive) are run spatially separated. Each lock and each drive requires its own circuit. Each electric cable or system must be isolated.

Manufacturing effects are avoided using redundant manufacturers for identical parts and assure the quality through the supply chain.

Maintenance effects are avoided introducing a maintenance handbook and a fail-safe design.

Failures of system components which lead to a lock malfunction are avoided introducing robust locks, which means, that each has the capability to resist the complete load. The load can be the force of the drive or an external effect. Sensors have to be 2n+1 redundant, where n stands for a specific quantity. This means that a single quantity has to be observed by three redundant sensors. Errors of a single component of a 2n+1 redundant system are detectable and can be indicated in the cockpit. The control logic also has to be 2n+1 redundant.

Conclusion

The systematic analysis method of an SSA that has been applied in this paper is a powerful tool to investigate complex systems with respect to failure scenarios, failure modes, and basic events. Within this work, a preliminary SSA was applied to a standard CC-TRU with an electric TRAS. Besides the failure

scenario which is obvious since the Lauda Air accident, it was possible to analyse the TRU architecture completely and to list all kinds of failure scenarios using an FHA. As an example, possible scenarios have been captured, such as an inadvertent self-deactivation, or a TRU that cannot be deactivated after use. These scenarios may not be identified with an unstructured approach, only with increased effort using bottom-up methods, or with increased costs using physical tests. Furthermore, even a hardware test may not be able to capture scenarios with very small probabilities. Besides, an unstructured approach would not be applicable in development projects due to their immense expenditure of time and the strong demand to decrease engine development time. In addition, a CCA is required for the certification and demands a systematic approach to detect potential common causes.

For aircraft certification procedures it is not enough to bring in possible failure scenarios without statistically proven probabilities. Random methods like brainstorming with experienced engineers from departments for reliability, certification, safety, and further pertinent departments are important and can increase the quality of such an analysis, but for the certification itself, only statistically validated systems are relevant. Important information from the certification specifications for example are methods that are applicable to provide evidence: read across, tests, analysis, etc. [14][15]. Wherever it is possible, the methods of a (P)SSA should be combined with the knowledge from previous certifications to improve the assignment of resources.

Each critical failure condition that has been identified was furthermore investigated within an FMEA. The results of this analysis were required in the following investigations in the project on which this paper is based on. Based on the results of the criticality FMEA (FMECA) the critical failure conditions were decomposed down to part level.

In summary, the advantage of a top-down – bottom-up combination is that it neglects the non-essential failure chains within a FMEA, which otherwise would have been required and would have caused a huge man power effort. In this way all possible information is encapsulated within one approach. The superiority of this approach is caused by the FHA based combination of a top-down method (FTA) with a bottom-up method (FMECA). In addition, the (preliminary) SSA has benefits for the design process, as it provides not only an analysis of the requirements, but also of functions, subsystems and single parts.

References

[1] Rolls-Royce plc., 1997, “The Jet Engine”, p.159, p.161

[2] Willy J.G. Bräunling, 2009, “Flugzeugtriebwerke”, p.220, Springer-Verlag, ISBN 978-3-540-76368-0 e-ISBN 978-3-540-76370-3, DOI 10.1007/978-3-540-76370-3

[3] James Albright, Chris Parker, Chris Manno, Website called 2015 , “G450 Systems: Powerplant Exhaust” http://code7700.com/g450_powerplant_exhaust.html

[4] Barry James, New York Times, 17.8.1991, “U.S. Orders Thrust Reversers Deactivated on 767s”,http://www.nytimes.com/1991/08/17/news/17iht-thru.html

[5] EASA, 2015, CS-25 Large Aeroplanes Amendment 16, 8.b.(1)

[6] EASA, 2015, AMC 25.1309, 7.c.(5) and 8.a.(5)

[7] SAE International, 1996, “Aerospace Recommended Practice 4761” (ARP4761)

[8] EASA, 2015, CS-E 510 (a)(3) and (4)

[9] EASA, 2015, AMC E 510 (3) (d-f)

[10] EASA, 2015, CS-E 15

[11] EASA, 2015, CS 25.1309 7. and 8.

[12] Deutsches Institut für Normung e.V., 1981, „DIN 25424 Teil 1“

[13] Gerd F. Kamiske, 2013, „Handbuch QM-Methoden: Die richtige Methode auswählen und erfolgreich umsetzen“, ISBN 978-3446420199 http://risikomanager.org/methodenassistent/fehlerbaumanalyse/

[14] Martin Hinsch, 2012, „Industrielles Luftfahrtmanagement“, p.72, Springer-Vieweg, ISBN 978-3-642-30569-6, e-ISBN 978-3-642-30570-2, DOI 10.1007/978-3-642-30570-2

[15] EASA, 2012, “AMC/GM to Part 21”, “Appendix to AMC 21.A.20(b) – Means of compliance codes”, p.30, https://www.easa.europa.eu/system/files/dfu/Annex%20I%20to%20ED%20Decision%202012-020-R.pdf