33RD CONGRESS
OF THE INTERNATIONAL COUNCIL
OF THE AERONAUTICAL SCIENCES
STOCKHOLM, SWEDEN, 4-9 SEPTEMBER, 2022

ICAS 2022 SWEDEN

COUPLING OF MODEL-BASED SYSTEMS ENGINEERING AND SAFETY ANALYSIS IN CONCEPTUAL AIRCRAFT SYSTEM DESIGN

Sascha M. Lübbe[1], Michael Schäfer[1] & Oliver Bertram[1]

[1]German Aerospace Center (DLR), Institute of Flight Systems - Department of Safety Critical Systems and Systems Engineering, Braunschweig - Germany

Abstract

Modern commercial aircraft are highly mature and proven systems. At the same time the air transport system as is will have to undergo a major transformation in the face of climate change and global efforts to reach carbon neutrality. To achieve this, new technologies and functions as well as an increasing degree of multi-functionality in aircraft systems need to be implemented. At the same time aircraft system design is fundamentally driven by the industry's safety standards. The impact of the introduction or adaption of aircraft or system functions is difficult to estimate in early design stages. The goal of this paper is to demonstrate how integrating safety analysis into conceptual system design can improve early system architecture design. The Institute of Flight Systems of the German Aerospace Center (DLR) conducted a design study that will serve as an illustration of modelling safety processes relevant in aircraft and aircraft system design. The aircraft and its systems are modelled in a model-based systems engineering environment and Aircraft FHA, PASA and System FHA are applied within it. The model hosts current standard safety processes and allows to track design impacts on architecture and in between systems. The process will be examined with regard to adequacy and effectiveness by comparing it to a preexisting FHA.

Keywords: model-based systems engineering; ARP4761; conceptual aircraft system design; functional hazard analysis

1. Introduction

Today's air transport system faces fundamental challenges to follow global efforts to reach carbon neutrality [1]. For this it is necessary to introduce new technologies, functions and an increasing the degree of multi-functionality in aircraft systems.

At the same time, these new and partially highly complex systems have to meet the high safety standards in aviation. Modern commercial aircraft are highly mature and proven systems with accident rates of less than $1 \cdot 10^{-6}$ per flight hour [2], placing them as one of the safest means of transportation. However, the impact of the introduction or adaption of aircraft or system functions is difficult to estimate in early design stages. The approach usually applied is to assume the current state-of-the-art for system architectures in early design and to consider detailed solutions in later design stages. For disruptive technologies this is an obstacle because it may lead to wrong assumptions about system complexity, mass and overall sizing procedures [3]. Wrong assumptions disqualify certain innovations while others have to be corrected in later design stages, which leads to intense and costly redesign.

This paper aims to demonstrate how integrating safety analysis and conceptual system design within a shared model can improve confidence in early system architecture assumptions and the resulting design. Furthermore, applying model-based systems engineering (**MBSE**) [3] results in increasing traceability between safety and design requirements, and potential re-usability of information obtained during safety analysis. For this purpose Systems Modeling Language (**SysML**) [4] is used in the example. Safety relevant design implications are often opaque and inaccessible to researchers and system developers. Tracking design changes in the aircraft architecture and their related safety

implications in model form allows highlighting analysis demands or rationalising a system design's invariability. An important aspect of the process is that specific design rationales and decisions can be tracked within the model in such a way, that influences from design changes on aircraft level can be efficiently propagated towards system level and vice versa.
This paper investigates how processes from ARP4761 [5] can be applied within an MBSE approach in early design stages of an aircraft program to support analysis and engineering activities. For this, the considered safety analysis processes will be described. The scope of MBSE will be given and its advantages presented. The modeling methodology connecting both aspects will be outlined. It will then be demonstrated using the conceptual design and analysis of a landing gear system as an example. The model hosts the described standardized safety processes and enables to track design impacts on architecture and in-between systems. This use case was part of the German Aerospace Center's (**DLR**) project MoBEFAS, in which design and safety analysis for commercial aircraft systems during preliminary design stages were conducted. Finally, the adequacy and effectiveness of the process will be examined by comparing the generated analysis to the results of a traditional safety analysis.

2. Safety Analysis and Model-Based Systems Engineering

Regulations and requirements for the certification of commercial aircraft are put forward by civil aviation agencies. For commercial transport aircraft these are collected in CS-25 [6] and FAR-25 [7] for Europe and America. Conformity to these regulations is certified through various accepted means of compliance (**AMC**) The design and safety processes for modern commercial aircraft are defined by the industry through the Society of Aerospace Engineers (**SAE**) in the Aerospace Recommended Practices (**ARP**).
The two main documents that build the foundation for the safe design and safety analysis are the ARP4754A [8] and ARP4761 [5]. The ARP4754A states the recommended order, content and interaction of design processes throughout the aircraft program. The ARP4761 describes the safety processes and their analysis procedures. These standards are regarded as part of the AMC by civil aviation authorities. They aim to cooperatively build a reliable process which ensures the certifiable design of a safe aircraft. This results in a vast and time consuming process that has to be performed fully in order to develop a safe aircraft design.
The results of these design processes and safety analyses is usually communicated through dedicated documents according to the standard and propagated towards the system design in the form of requirements. Many design decisions for the aircraft have to be made as a result of the safety analyses, resulting for example in the common triplex redundancy for hydraulic supply. Strong influences between systems result from systems' inter-dependencies, functional overlap or the implied use of common resources such as provided power or computing capability [9]. This effect may increase further for novel functions, where design inter-dependencies have yet to be established. This makes aircraft concept design studies incorporating new technologies and functions challenging.
Various research and development projects describe different approaches towards unifying safety analysis and MBSE. An example is the SafeSysE methodology, presented in [10], that integrates safety analysis into MBSE by extending SysML. The extended model covers the safety analysis methods Failure Mode Effect Analysis (**FMEA**) and Fault Tree Analysis (**FTA**). It establishes a formal design methodology to be followed to integrate the safety analysis into the system design process.
At the same time a long existing trend is the promotion of model-based safety analysis (**MBSA**) in the aviation field. Most applications employ models to (semi-)automatically conduct specific safety analysis methods [11]. Bretschneider et al. [12] describe how they conducted model-based Fault Tree Analysis for a commercial aircraft flap system and integrated it into their model-based process. Seguin et al. [13] apply MBSA methods throughout different stages of the ARP4754A processes. Different approaches and how they can contribute to or evolve the current ARP4754A processes are presented. In [11] Lisagor et al. evaluate MBSA's state across industries, illuminate limitations and challenges in commonly shared in the discipline.
In this paper we concentrate on applying existing safety analysis within MBSE to represent established safety processes, outlined in the following.

2.1 Safety Analysis

DLR researches and applies current and future safety processes for aircraft and aircraft systems. Central safety attributes used in the context of this paper are (functional) failure conditions and criticalities.
The foundation of current safety analysis in aviation is built through the processes:

- Aircraft Functional Hazard Analysis (**Aircraft FHA**),
- Preliminary Aircraft Safety Assessment (**PASA**),
- System Functional Hazard Analysis (**System FHA**),
- Preliminary System Safety Assessment (**PSSA**),
- Aircraft Safety Assessment (**ASA**),
- System Safety Assessment (**SSA**), and
- Common Cause Analysis (**CCA**) [8].

Aircraft FHA, PASA, System FHA are applied within this paper, as they are performed starting from a conceptual design stage and deliver safety requirements for the detailed design.
The **Aircraft FHA** aims to identify and classify all relevant potential failure conditions emerging from the aircraft's functions. It is initially created in the aircraft early development stages and updated throughout the development phase to track arising design implications. The Aircraft FHA serves as the basis for the following safety assessments and motivates most of the top level safety requirements. Its results are usually documented in the form of tables. [5]
The objective of the **PASA** is to examine the general concept of the aircraft and its architecture for its validity in regard to safety. Combinations of failure conditions of different aircraft functions have to be systematically examined for their functional implications and resulting hazard potential. PASA may among others incorporate analysis methods such as Fault Tree Analysis (**FTA**) or Reliability Block Diagrams (**RBD**). Within the PASA specific aircraft and system safety requirements are established. The PASA connects failure conditions from Aircraft FHA and System FHA. [8]
Similar to the Aircraft FHA, the **System FHA** is a table based analysis method to identify and classify functional failures. However, the analysis is not applied to aircraft level functions but to designated system level functions. It uses information input from the Aircraft FHA and PASA, such as failure conditions, criticalities and failure condition couplings between failures, and further analyzes the more detailed system level functions for failure conditions. System FHAs are performed per system and are regularly updated throughout development. The System FHA delivers failure conditions and criticalities on System Level to following safety assessments, and feeds arising failure conditions back upwards to PASA and Aircraft FHA. [5]
These processes are done separately and iteratively in a feedback loop to promote completeness of the analysis. Safety attributes have to be traced across different system levels. Classically this is done through exchanged and updated documents referencing each other.

2.2 The Aircraft in MBSE

The aircraft design used in this work has been conducted in the form of model-based systems engineering (**MBSE**) approach. MBSE aims to improve systems engineering by using models as common information source in the development process, while systems engineering communicates through documents. Textual descriptions of the system under development are enriched and/or replaced by objects and diagrams. This increases communication efficiency throughout the development stages especially across different system domains and disciplines. Improved communication helps to identify and solve design flaws and conflicts in early project stages. Cooperation between different disciplines, that regularly suffers from disagreeing terminology, benefits from diagrams as a central communication tool. On an organisational level strong advantages lie within the centralization of design information within a central model. This is often referred to as principle of Single Source of Truth (**SSoT**). Especially for complex systems, MBSE aims to succeed classical systems engineering. [14]

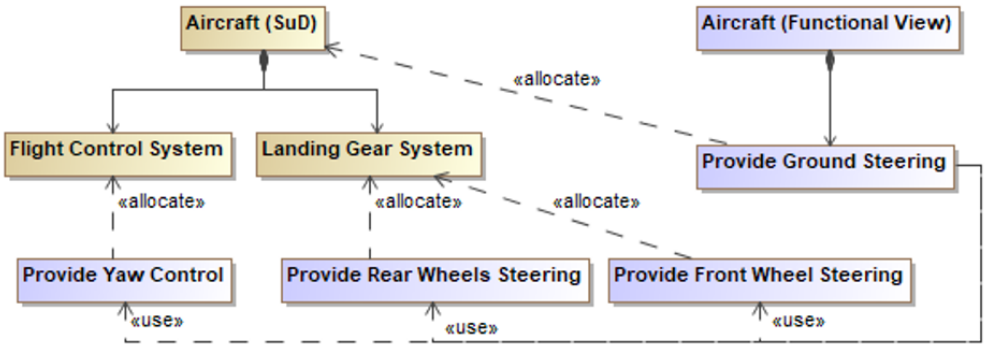

Figure 1 – Functional decomposition of *Provide Ground Steering* and Allocation to Aircraft Systems

Implementations of MBSE differ mainly in their scope and the employed modeling language. A widely used modeling language is the SysML [4]. It provides a common basis and is extended using profiles to implement specific domains. The presented example (Figure 1) uses SysML and is aimed to realise SSoT.
The landing gear system and in particular its *steering aircraft on ground* function, implemented in the model as *Provide Ground Steering*, are used as a demonstrator to investigate how the respective design and safety analysis fit into a common MBSE model. The *Provide* keyword is used to imply the conceptual state of the function in the model. The SysML based aircraft model is realised in two levels. It contains the aircraft and considered aircraft level functions on aircraft level.
On system level the aircraft is broken down into systems, while the aircraft level functions are decomposed into system functions. Any system may perform multiple functions and any function may be allocated to multiple systems, either cooperatively or independently. The *steering aircraft on ground* function for example can be broken down into three independent entities and allocated to two different systems as depicted in Figure 1. For this the aircraft model consists of a logical layer, made up of systems and subsystems, and a functional layer, made up of aircraft level functions using system level functions. The different layers are assigned to representing packages within the model structure. The model was pre-existing and had to be extended to accommodate the safety analysis as outlined in the next section. Within the example model only systems directly related to the examined function are implemented. Functions not considered within the project have been marked as such. Within this paper only the *steering aircraft on ground* function will be further investigated.

3. Implementation of Safety Analysis into MBSE Environment

Aircraft design involves multiple disciplines and is organised in various levels. Aviation has implemented extensive safety requirements over the decades that have been prominently collected for large aircraft in [6], [7] and in different standards. To efficiently track safety attributes a model has been defined in which design implications caused by safety considerations are documented in traceable and reproduceable manner. It has been adapted to include the aircraft to system safety analysis in conceptual design from ARP4761. The analysis is performed within a package parallel to the logical and functional layer.
To help the creation of the analysis model two SysML profiles have been used

- FHA Profile: an in-house developed SysML Profile [15] that allows for the creation of FHA tables
- Risk Analysis and Assessment Modeling Language (**RAAML**) Profile: a profile released by the Object Management Group (**OMG**) to enable safety modelling in SysML, which implements (among other methodologies) the application of FTA [16].

The FHA Profil introduces *HazardousFunction* as a specialisation of the *Block* element that represents the functional failure conditions from ARP4761. A failure condition is defined by its relevant information, such as function name, failure mode, flight phase, effect, and criticality. From the RAAML

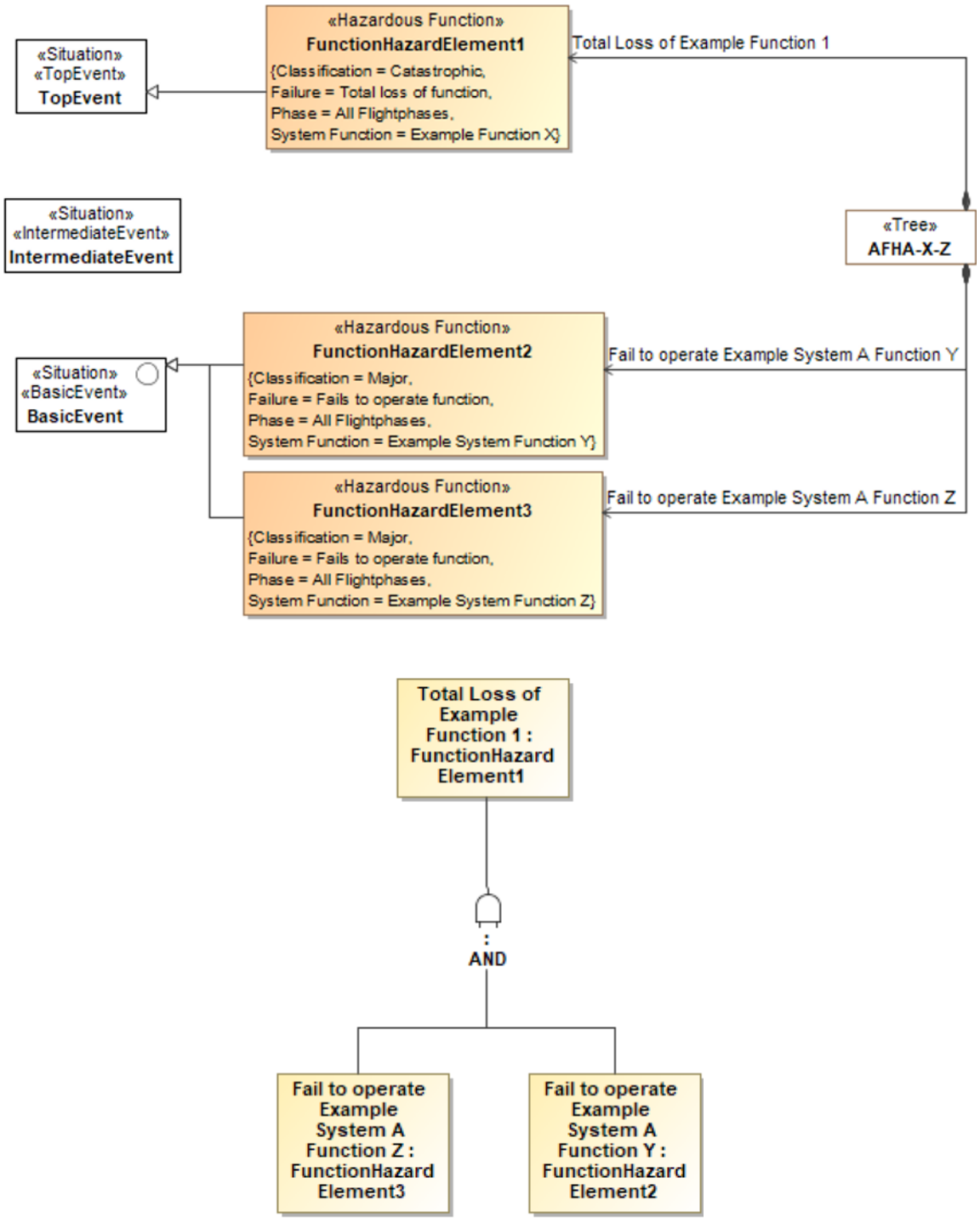

Figure 2 – Example PASA for *Aircraft Level Function X* referencing *System Level Functions Y & Z*

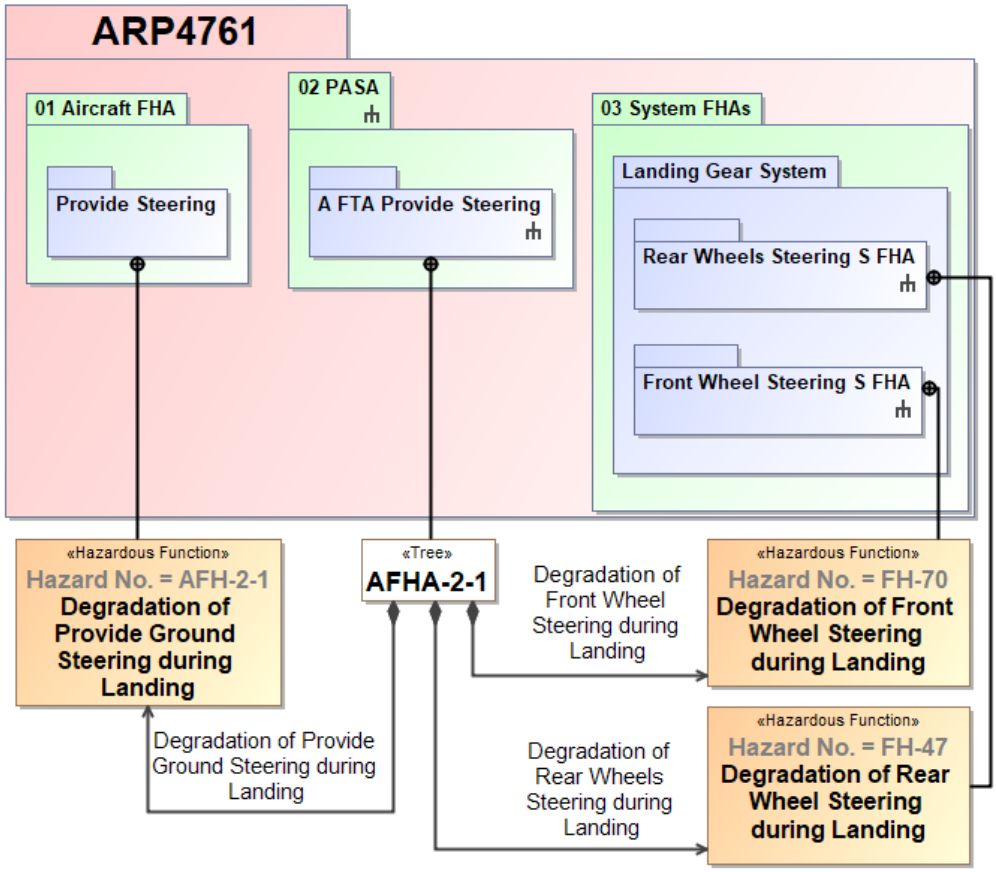

Figure 3 – Link up between Aircraft FHA, PASA, and System FHA for an example failure condition

Profile the *Tree* element was used to implement the FTA together with necessary descriptions of *BasicEvents* and *TopEvents*. Following the definition of FTA a single TopEvents is caused by one or more defined combinations of BasicEvents and thus describes causal relations [5].
Using these two profiles failure conditions from the FHAs can be described within the model and serve as events for the analyses within the PASA. The RAAML Profile is then used to perform the FTAs within the model. As a basic rule every FTA constitutes an analysis of a specific failure case and has to be tracked to aircraft level and system level accordingly. To ensure this every *Tree* is described through at least an internal block diagram and a block definition diagram. The diagrams further allow for a visual inspection of an analysis's progress and completeness.
A baseline structure of elements for an FTA within the model is presented in Figure 2, where the aircraft level function *X* consists of the system level functions *Y* and *Z*. In the figure two failure conditions on system level are connected to an aircraft level failure condition by declaring them as part of the FTA, as seen in the upper diagram in Figure 2. The causal connection between the system level failure conditions and aircraft level failure condition is formalized in the form of an FTA, as shown in the lower diagram. Figure 3 demonstrates how this enables to track safety elements across different packages representing the separated processes. Here, each failure condition is considered in a different FHA, represented by the packages in the diagram.

4. Analysis of the Function

The safety analyses were performed on the functional design of the aircraft level function *steering aircraft on ground* function for a conceptual commercial aircraft within the MBSE model. The considered use case was a commercial passenger transport flight between two airports.
The function *steering aircraft on ground* has been identified as a well suited case study in the project MoBEFAS for its availability of design data within the institute, and simplicity of function behaviour and interaction with other functions. The function should enable the aircraft to change its direction of

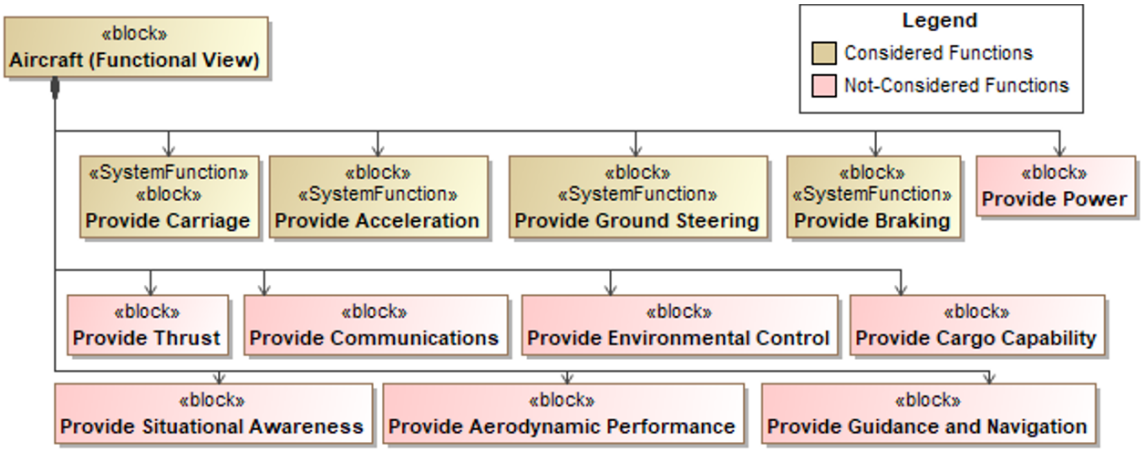

Figure 4 – Assumed functional breakdown (based on example in [17])

movement on ground during forward movement. It is used during Taxi phase to navigate over and between runways and taxiways. During Landing and Take-off the function is necessary to ensure that the aircraft stays on the runway while transitioning from and to being airborne. The function was analysed with the functional breakdown depicted in Figure 4 as a basis for the assumptions regarding the functional context at aircraft level, where it is referenced as *Provide Ground Steering*.
For the Aircraft FHA the considered functional failure modes and relevant flight phases to be analysed were defined. In the first iteration these were *total loss of function*, *degradation of function*, *inadvertent function* and *fail to operate function* during Taxi, Landing and Take-off respectively. This yielded 12 relevant failure conditions to be considered in the initial Aircraft FHA (see Figure 5).
All failure conditions with a criticality of major and beyond were then regarded as top events in the PASA within separated FTAs. The *total loss* of function during Take-Off and Landing has been identified as potentially catastrophic. Resulting from this the requirement was established in the PASA, that at least a redundant implementation of the function was necessary. This results in the necessity to update the PASA's FTAs accordingly and to regard the function instances *Front Wheel Steering* and *Rear Wheel Steering* in the landing gear system's System FHA.
Figure 6 visualizes the FTA for inadvertent operation of the function during Take-off under the assumption of redundant implementation of the *steering aircraft on ground* function. It displays the resulting requirement for the failure condition's probability, which in this example must not exceed $1 \cdot 10^{-9}$ per flight hour. Because a malfunction of either *Rear Wheel Steering* or *Front Wheel Steering* would cause the aircraft level failure condition, a functional composition of the *Front Wheel Steering* function that accommodates necessary fail-safe behaviour was established. For the *Rear Wheel Steering* a corresponding requirement applies, which is omitted in the figure for readability.
Basic events identified in the PASA were then used as a starting point for conducting the System FHA. The executed System FHA results are linked to the PASA and Aircraft FHA according to the example diagram in Figure 2 to establish the necessary traceability. To examine the resulting system description for inconsistencies the matrix in Figure 7 can be used to verify, whether

- failure conditions from the Aircraft FHA have been analysed within the PASA
- FTAs include failure conditions from the Aircraft FHA
- an FTA includes failure conditions from a specific System FHA
- a failure condition identified in the System FHA has been considered in the PASA
- FTAs cannot be regarded as separate because of common failure conditions.

In the shown example it is visible that the FTAs AFHA-2-10 and AFHA-2-16 (encircled in Figure 7) share system level failure conditions. This means that they do not constitute mutually exclusive

Hazard No.	System Function	Phase	Failure	Effects	Classification
AFH-2-1	Provide Ground Steering	Landing	Degradation of function	Slight / significant increase in workload	Major
AFH-2-2	Provide Ground Steering	Take-off	Degradation of function	Slight / significant increase in workload	Major
AFH-2-3	Provide Ground Steering	Taxi	Degradation of function	Slight increase in workload of the pilot	Minor
AFH-2-4	Provide Ground Steering	Landing	Fails to operate function	Possible runway excursion and loss of A/C	Catastrophic
AFH-2-5	Provide Ground Steering	Take-off	Fails to operate function	Possible runway excursion and loss of A/C	Catastrophic
AFH-2-6	Provide Ground Steering	Taxi	Fails to operate function	A/C can not take off. Inconvenience, but no safety effect	No safety effect
AFH-2-7	Provide Ground Steering	Landing	Operates function inadvertend	Possible runway excursion and loss of A/C	Catastrophic
AFH-2-8	Provide Ground Steering	Take-off	Operates function inadvertend	Possible runway excursion and loss of A/C	Catastrophic
AFH-2-9	Provide Ground Steering	Taxi	Operates function inadvertend	Possible runway excursion at low speed, aircraft must be towed, higher workload for pilot	Major
AFH-2-10	Provide Ground Steering	Landing	Total loss of function	Possible runway excursion and loss of A/C	Catastrophic
AFH-2-11	Provide Ground Steering	Take-off	Total loss of function	Possible runway excursion and loss of A/C	Catastrophic
AFH-2-12	Provide Ground Steering	Taxi	Total loss of function	Possible runway excursion, aircraft must be towed, higher workerload for pilot	Major

Figure 5 – Excerpt from Aircraft FHA of the analysed function

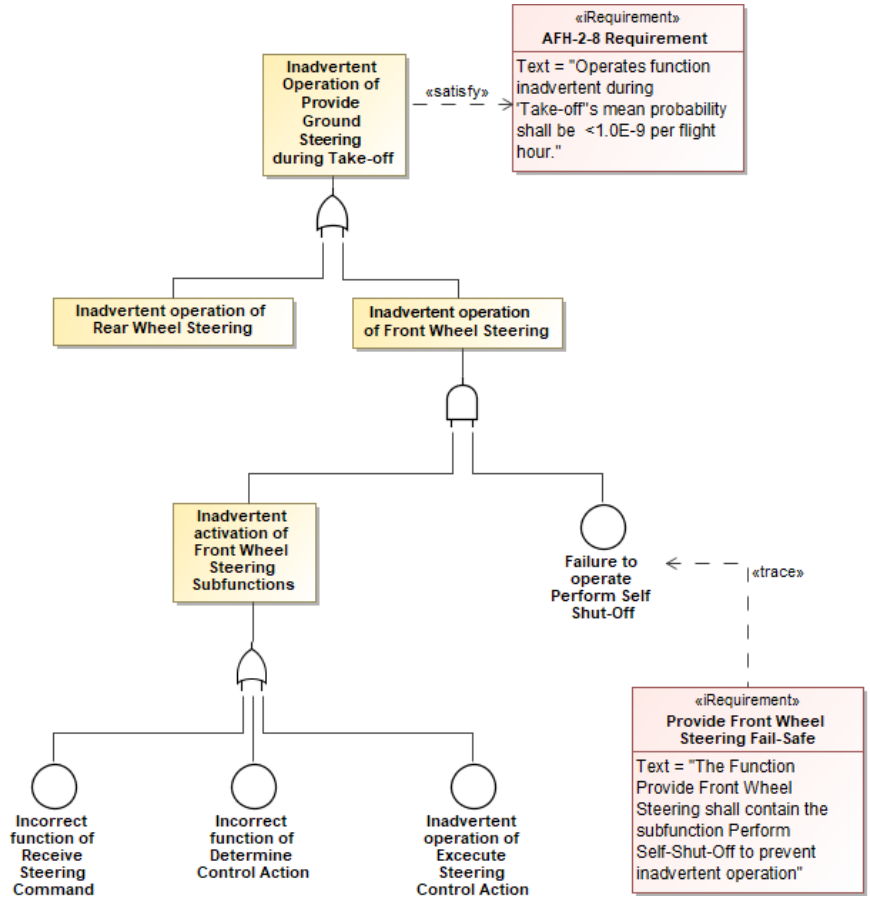

Figure 6 – Fault Tree Analysis of the inadvertent operation during Take-Off

events, which implies that these failure conditions have to be analysed together. In a real development program the generated and iterated failure conditions would have to be communicated towards the system development team in the form of the System FHA tables and collected requirements from the PASA.

5. Results and Discussion

The adequacy of the methodology in its MBSE adaption and its applicability when used with a reduced set of functions were examined. The results from the analysis were compared against pre-existing design inputs for a conceptual landing gear system.

If the MBSE adaption were to be effective, it was expected to deliver at least the needed initial System FHA results that an experienced systems developer had assumed and link them to hazards at aircraft level.

In the considered case study we found that the design critical system level hazards identified in the pre-existing design inputs could be reliably identified in our model. These are namely the *inadvertent operation* and *total loss*, both during Take-off and Landing. They can be efficiently traced between system level and aircraft level, as highlighted in Figure 7. The criticality of the failure condition total loss requires an at least redundant implementation of the considered function. Additionally, through the PASA necessary sub-functions to the system functions were identified. An example for this is the *self-shut-off* function of all steering function instances. They result from aircraft level functional hazards. System level safety analysis in the benchmark design inputs had independently deemed these sub-functions to be necessary in later stages.

The analysis was conducted with respect to a subset of the assumed aircraft level functions. The results from this restricted set of functions indicate the adequacy of the investigated modelling concept. Nonetheless further modelling effort towards using the complete functional description at the aircraft level will be necessary to compare the applicability of the analysis with the full set of functions. System interaction will potentially introduce new failure conditions to be considered in the PASA.

The analysis within the MBSE environment appears to be effective. But in the presented example an already pre-established system was analysed and the influence of the analysts' knowledge about safety issues and potential implementations can not be disregarded. Thus, to objectively test the method's effectiveness dedicated design studies on novel systems will be necessary.

The implementation of the described ARP4761 processes into the MBSE model has yielded clear advantages for traceability and accessibility of the analysis and described system. Functional hazards and their rationals can be effectively traced to related requirements and descriptions of resulting system structure. References between results from Aircraft FHA, PASA and System FHA can be examined and efficiently accessed via diagrams and relations within the model.

6. Conclusion and Outlook

Within this paper an approach is demonstrated that applied ARP4761 based analysis methods in the context of MBSE. An FHA Profile is used to implement Aircraft FHA and System FHA. The RAAML Profile is applied to introduce FTA into the model. The Aircraft FHA is performed for a single aircraft level function. After conducting the Aircraft FHA, its results are used in the PASA. In the PASA related failure conditions from the Aircraft FHA and Systems FHA are connected and analysed together. Emerging failure conditions from the System FHA are communicated to the PASA. During this analysis necessary subfunctions and critical failure conditions are identified. This approach is demonstrated using an aircraft landing gear system. Results from the safety analysis are compared to a separated existing landing gear system's safety analysis.

Overall, conducting the examined ARP4761 processes within the MBSE design approach in the conceptual stage proves useful. Safety critical design implications are identified and the analysis results improves in traceability and accessibility compared to document based analysis.

Future work will try to extend the amount of functions in the aircraft model by implementing existing and novel functions. The model has to be extended to accommodate more ARP4761 processes, such as PSSA and CCA, that build the connection to safety analysis of system components. A transition of the PASA towards ASA within the model will be necessary to support later design stages and

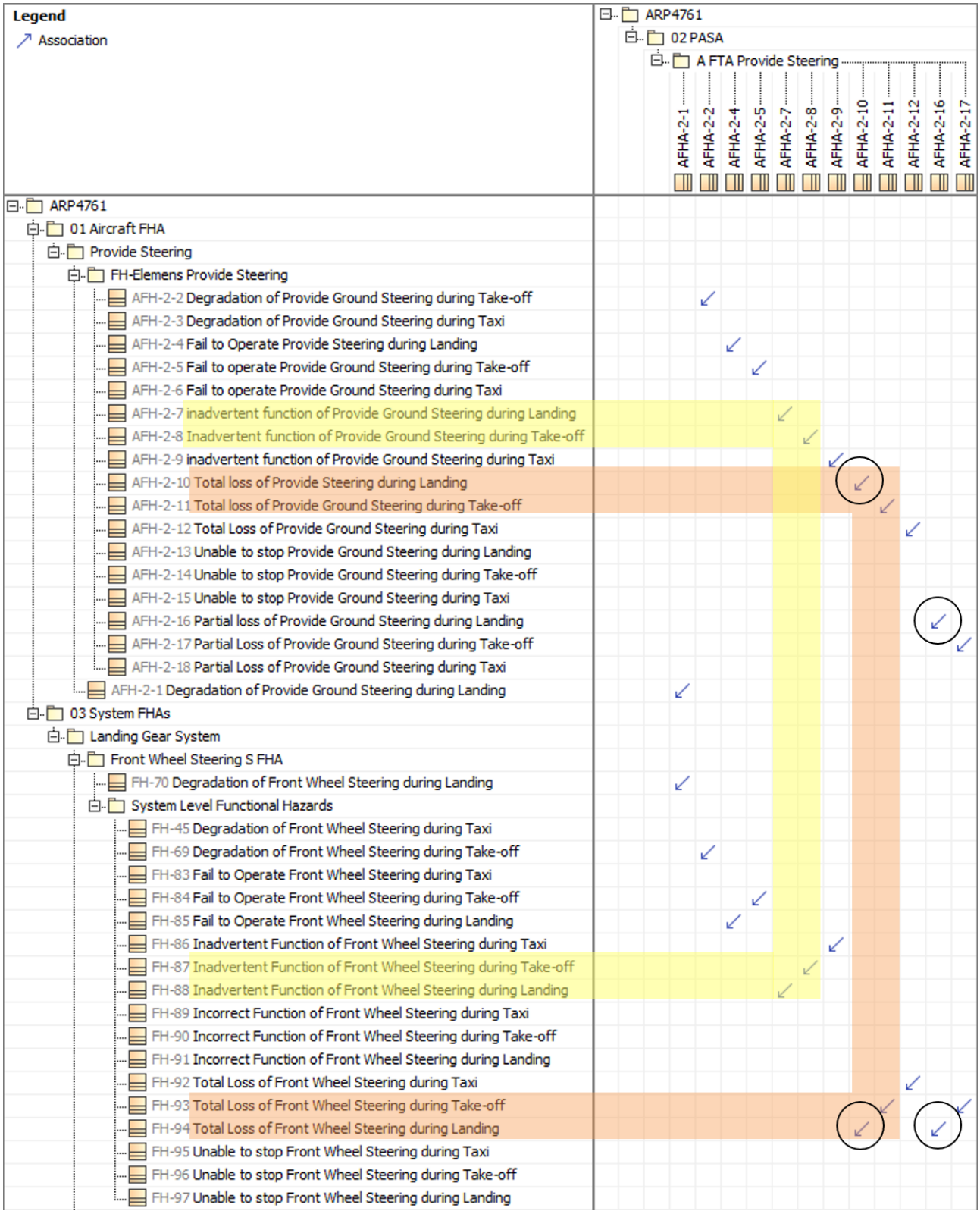

Figure 7 – Excerpt from the matrix evaluation of Aircraft FHA to PASA to System FHA tracing. Highlighted are identified most design critical failure conditions.

safety verification activities. Through these steps the approach described in this paper will be further developed and confidence in the analysis results will be built.

7. Contact Author Email Address

sascha.luebbe@dlr.de

8. Copyright Statement

References

[1] Matthias Finger, Juan Montero, and Teodora Serafimova. *Navigating towards the decarbonisation of European aviation*, volume 2021/53, November 2021 of *Robert Schuman Centre for Advanced Studies Policy Briefs*. EUI, Florence, 2021.

[2] European Union Aviation Safety Agency (EASA). *Annual Safety Review 2014*. EASA, 2015. URL: https://www.easa.europa.eu/downloads/19934/en.

[3] INCOSE. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Wiley, New York, 4th ed. edition, 2015.

[4] Sanford Friedenthal, Alan Moore, and Rick Steiner. *A Practical Guide to SysML*. Elsevier, 2015. doi:10.1016/C2013-0-14457-1.

[5] SAE International. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment (ARP4761), 1996. doi:10.4271/ARP4761.

[6] European Union Aviation Safety Agency (EASA). Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes: CS 25 - Amendment 27, 2021. URL: https://www.easa.europa.eu/downloads/134259/en.

[7] Federal Aviation Adminstration (FAA). PART 25 - AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES , 2022. URL: https://www.ecfr.gov/current/title-14/part-25.

[8] SAE International. Guidelines for development of civil aircraft and systems (ARP4754A), 2010. doi:10.4271/ARP4754A.

[9] Marion Morel. Model-based safety approach for early validation of integrated and modular avionics architectures. In Frank Ortmeier and Antoine Rauzy, editors, *Model-Based Safety and Assessment*, volume 8822 of *Lecture Notes in Computer Science*, pages 57–69. Springer International Publishing, Cham, 2014. doi:10.1007/978-3-319-12214-4_5.

[10] Faida Mhenni, Nga Nguyen, and Jean-Yves Choley. Safesyse: A safety analysis integration in systems engineering approach. *IEEE Systems Journal*, 12(1):161–172, 2018. doi:10.1109/JSYST.2016.2547460.

[11] Oleg Lisagor, Tim Kelly, and Ru Niu. Model-based safety assessment: Review of the discipline and its challenges. In *The Proceedings of 2011 9th International Conference on Reliability, Maintainability and Safety*, pages 625–632. IEEE, 12.06.2011 - 15.06.2011. doi:10.1109/ICRMS.2011.5979344.

[12] Matthias Bretschneider, Hans-Jürgen Holberg, Eckard Böde, Ingo Brückner, Thomas Peikenkamp, and Harriet Spenke. 2.2.1 model-based safety analysis of a flap control system. *INCOSE International Symposium*, 14(1):246–256, 2004. doi:10.1002/J.2334-5837.2004.TB00493.X.

[13] Christel Seguin, Pierre Bieber, Eckard Boede, Marco Bozzano, Matthias Bretschneider, Antonella Cavallo, Johann Deneux, Jean-Pierre Heckmann, Oleg Lisagor, Marion Morel, Chris Papadopoulos, Laurent Sagaspe, Valerie Sartor, and Rémi Delmas. Model-based safety assessment for the three stages of refinement of the system development process in arp4754a. In *SAE Technical Paper Series*, SAE Technical Paper Series. SAE International400 Commonwealth Drive, Warrendale, PA, United States, 2011. doi:10.4271/2011-01-2548.

[14] Azad M. Madni and Michael Sievers. Model-based systems engineering: Motivation, current status, and research opportunities. *Systems Engineering*, 21(3):172–190, 2018. doi:10.1002/sys.21438.

[15] Michael Schäfer, Axel Berres, and Oliver Bertram. Integrated Model-Based Design and Functional Hazard Assessment with SysML on the Example of a Shock Control Bump System. In *Conference paper*

presented at 70. Deutscher Luft- und Raumfahrtkongress, 31.8.2021 - 2.9.2021 in Bremen, Germany, 2021.

[16] OMG. *Risk Analysis and Assessment Modeling Language (RAAML)*, 2020. URL: https://www.omg.org/spec/RAAML/.

[17] Scott Jackson. *Systems Engineering for Commercial Aircraft: A Domain-Specific Adaptation*. Ashgate Publishing Ltd, Farnham, 2nd ed. edition, 2015. doi:10.1201/9781003075042.