Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P181-cd

Challenges of a distributed Hazard Identification

Axel Berres

German Aerospace Center, Braunschweig, Germany, E-Mail: Axel.Berres@dlr.de

Igor Sokolov

German Aerospace Center, Hamburg, Germany, E-Mail: Igor.Sokolov@dlr.de

Our task in the FLHYSAFE project is to analyse risks for a fuel cell system in the early stages of development. From the perspective of a distributed project like FLHYSAFE, challenges identified for example by [Da99] only partially cover our experience. This paper aims to look at the different aspects and specificities of hazard identification in a distributed project. The focus will be on the early development phases, the process and the methods for hazard identification. Using the example of the Emergency Power Unit, the results will be presented and discussed. Furthermore, recommendations for pragmatic hazard identification will be given.

Keywords: Functional Hazard Assessment, Hazard Identification Process, Collaborative Engineering

1. Introduction

With the goal of reducing dependence on fossil fuels and CO_2 emissions, hydrogen can become a future primary energy carrier in the foreseeable future. Compared to paraffin, it stores about 3 times as much gravimetric energy. However, in order to obtain a high volumetric energy density of hydrogen, it must be stored under high pressure or cooled in liquid form [Of23].

The use and safe operation of hydrogen in mobile systems, such as transportation, is well established. In the transportation sector, series-produced hydrogen-powered automobiles are available, such as Mercedes' GLC or BMW's iX5 [Me23], [Bm23]. As indicated in [Ho23], several research studies have been conducted in aviation sector. However, a new widespread commercial application in passenger airplanes has yet to occur. One possible explanation for this could be a lack of hydrogen infrastructure.

Partially integrating hydrogen into commercial aircraft is one feasible option. The hydrogen in our scenario is employed as an energy source for aviation systems. Existing questions, required infrastructure, and operational challenges can all be outlined. Then, feasible solutions can be developed by this approach.

Partial integration could also pave the path for targeted system complexity reduction through intelligent integration. The More Electric Aircraft (MEA) could be one solution. This approach is already employed to some extent in the Boeing 787 [Sa15]. It increases the use of electrical systems for function implementation while decreasing the use of hydraulic systems, for example. If the system complexity is decreased in this manner, the manufacturer's production costs can be cut, and operating and maintenance expenses can be reduced. The example MEA, reduces energy consumption, relieves drive units and reduce fuel consumption [Fa06].

The EU research project FLHYSAFE is funding the development of a hydrogen-powered fuel cell for use in aviation. The fuel cell will be built in a way that it can be scaled as a component of a future energy systems to meet future demands.

2. The FLHYSAFE Project

SAFRAN, CEA, INTA, and DLR are collaborating in FLHYSAFE project to develop a fuel cell, which can be used as an emergency power supply

(EPU) in an A320-sized aircraft. Furthermore, this EPU should be able to entirely replace the Ram Air Turbine (RAT) operation. The Auxiliary Power Unit (APU) will also be investigated to determine whether it may be replaced by scaling the system in the long run.

An A320 has three hydraulic systems for flight control, labelled yellow, blue and green. If the green and yellow systems fail, the blue system provides the power to control the aircraft in emergency mode. In an emergency, the RAT is deployed from the aircraft fuselage. The airflow acting on the RAT generates electrical energy and supplies the Electric Motor Pump (EMP), which is used to pressurize the hydraulic system.

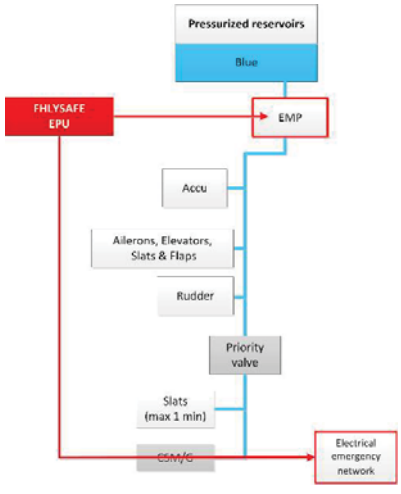

Fig. 1 RAT replacement scheme

To replace the RAT (Fig. 1), the EPU should provide electrical power directly to the EMP and to the A/C electrical emergency network. Since the RAT is part of a safety-critical function, the fuel cell system must meet the same safety requirements. As a result, a PSSA is required at the early development stages recommended by ARP 47564A [Sa95].

The next chapter outlines the FHA implementation in the FLHYSAFE project for hazard identification. [Be22] has already documented the distributed infrastructure and tools utilized.

3. FHA for distributed teams

Due to the increasing system complexity during development, production and operation, distributed development is becoming increasingly important. Today, for example, development and manufacturing may consist of a worldwide network of service providers and producers. To improve cost control and reduce risks, information exchange should be able to take place without delays. Thus, the challenge for development is to enable design in distributed teams.

To enable distributed development of safety-critical systems, the management process and the implementation of the method must be considered.

3.1 The management process

To provide value, the FHA should be considered as part of the safety management process as shown in Fig. 2 proposed by [RE00]. The interaction of management and development requires the support of both sides in order to successfully develop safe products. The best time to conduct an FHA, according to [RE00], depends on the firm, the development team, and the product. To achieve high effectiveness of this process, it should be implemented and applied after approval. Regular process reviews can ensure that the process is adapted to changing requirements.

Fig. 2 FHA Risk management process for

3.1.1. Safety strategy

The process is started by defining a security strategy. This involves establishing guidelines and principles, i.e. what should be done. This corresponds to the safety philosophy that a company wants to see implemented in its products. It can be specified that a product should not only be developed in a resource-saving way, but that the intervention in nature should be sustainable. In the case of safety-critical systems, this has the consequence of avoiding irreversible damage and reducing harmful hazards to a minimum through strategies.

3.1.2. Organisation

In the ***Organisation*** phase, it is determined how the described concept is to be implemented in the FHA. For this purpose, it is clearly defined which tasks have to be carried out. In addition, the necessary authority or powers are granted. The aim of the organisation should be to create an open culture that can continuously develop and quickly identify and eliminate critical problems in the process and in the products.

3.1.3. Planning and implementation

The ***Planning*** and ***Execution*** phases describe how the assessment is planned and later executed. The aim of this phase is the effective implementation of the FHA. For this purpose, all necessary activities and procedures are generated, prioritised and planned. After planning, the FHA is carried out. In addition, during the execution, measurements are collected that are needed for the evaluation of effectiveness and validity. Ideally, data is used that is already needed during the analysis and is not created additionally.

3.1.4. Verifying the performance

In order to be able to control the process, the activity ***Review Performance*** measures and evaluates the effectiveness of the process using previously defined metrics. For example, a metric such as the processing time of an FHA is used to measure performance. This metric can help determine whether the process was well implemented, the product was understood, and information was provided on time. Properly implemented metrics may so confirm assumptions. Unverified assumptions may lead to the development of new assumptions or metrics.

3.1.5. Audit

The final step ***Audit***, process is evaluated. For this purpose, in separate meetings between management and safety, the knowledge gained about the products manufactured, the process used, and possibly the philosophy practised is analysed. If this reveals problems, contradictions or opportunities for improvement, these should be considered.

3.2. The distributed application

For the project, the main challenge is that the distributed development brings together different corporate cultures. The management process proposed by [Re00] had to be adapted for effective implementation of the development. In the project context, ***Organisation*** and ***Planning and Implementation*** were essential.

To define the security strategy, the project agreed to consider ARP4754A during development. In doing so, each partner used the system engineering processes established in the respective company during development.

In order to better understand the needs of the partners, the respective SE processes and the tools used were presented at the beginning. Furthermore, the work was organised in such a way that besides telephone conferences, developer workshops were also held in presence.

An FHA Excel template was developed for the joint work. This template could be used by all partners without restrictions, due to company specifications. As a rule, a large table is proposed for the FHA. In order to enable distributed work, the FHA table was divided into the areas Functions, Hazards and Mitigation at the beginning of the template. In order to be able to observe the performance of the implementation, the status of the work was shown on an overview page. In addition, a table describing the application method was added. During the project, the requirements section was added to the Excel spreadsheet. This table was needed to improve the traceability of the requirements.

A special feature of the project was that the FHA was carried out in two phases. In the initial phase, each company started the FHA independently. In the second phase, the individual results were analysed and combined. The results are discussed in the following chapter.

As the process is used once in this form for the project. Audits were not carried out.

3.3 Functional Hazard Assessment

The FHA implementation shall be carried out in accordance with ARP 4761. The steps required to understand the challenges of distributed development are briefly discussed.

The FHA's purpose is to identify and assess hazards that can contribute to system failures [Da99]. If necessary, mitigations of these hazards must be identified. As such, the FHA serves as the foundation for controlling a system's risk. In order to enable this control, the FHA must carry out the process as shown in Fig. 3.

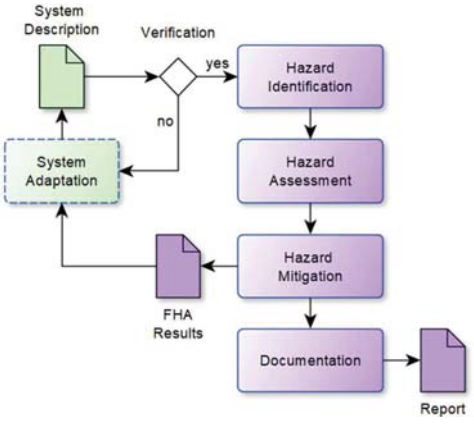

Fig. 3 Lean FHA process [Be20]

3.2.1 System Description

An acceptable system description is required to begin the FHA. Because FHA is performed at such an early development stage, the quality of the system description can have a significant impact on the analysis's outcome. Furthermore, early concepts and system descriptions are subject to uncertainty [Da99]. Because the FHA is also a black-box analysis, the quality of the description is critical. According to [Bi92], functions can be described both normalised and non-normalised form. A normalised description of the functions is advised.

3.2.2 Hazard Identification

In the identification phase, a systematic approach is used to identify potential hazards. Two aspects need to be considered, the process and the method.

We separated the hazard identification process into workshops and offline work. The workshops served to identify and later agree on the identified hazards. During the offline work, the system description was adapted or supporting material such as publications or reports were collected to improve the argumentation for the identified hazards.

In [Ti02] a review examined 62 different methods used for risk analysis. Some of these methods are suitable for the identification of hazards and were used by us. According to [Ly21], the Preliminary Hazard Analysis (PHA) is a fundamental method. Part of the PHA is the Preliminay Hazard List (PHL), which describes a list of known hazards of functions or systems. Thus, this can serve as a basis for identifying the system under investigation. If similar functions are found to be at risk, they should be considered. Since the PHL only considers known hazards, it may not be possible to identify all hazards of a system with this method.

Therefore, another systematic method is needed. One possible method is the Hazard and Operability (HAZOP) analysis, the application of which is described in [Re00]. This method uses guiding terms for the identification of hazards. The guiding terms are intended to point out certain typical sources of danger in a system during the analysis. The hazard is identified in such a way that effects of deviations from system parameters are analysed. For example, the keyword "late" may indicate that a temperature reading is provided too late. This omission may result in an incorrect command and system failure.

The challenge of guide words employment is that it pre-determines the thinking of individuals involved. To counteract this effect, the analysis can be guided by leading questions. The SWIFT method was used for this purpose. By combining a guiding concept in a "what-if" question, the identification of hazards can be facilitated. Unlike HAZOP, where the guide words refer to explicitly parameters, SWIFT uses broad ideas. For example, if hazards are related to materials utilized, a guide question might be "Do material problems exists?".

3.2.3 Hazard analysis and assessment

Once the hazards have been identified, the risk for each hazard must be analysed and assessed. In the analysis, the security expert can draw on his or her expertise and the knowledge of the system developers. Hazard tracking and knowledge management systems can be used to support the analysis. These databases collect knowledge about accidents that have already occurred. The analysis results provide information about the damage as well as possible causes and underlying hazards of functions and systems. Furthermore, these databases may contain information about how the systems work. The data collected is used to determine the severity of the hazards and the likelihood of their occurrence. After all hazards have been evaluated and the results documented, the assessment should be discussed with the system engineers.

Novel systems with concepts or technologies need to be treated differently. It is difficult to draw on existing information for these. As a result, hazards must be evaluated to the best of one's knowledge and judgment. By using simulations or evaluating

test results of similar systems, an overly optimistic assessment can be avoided and a realistic evaluation made possible. Thus, it is possible to ensure that novel systems are operated with acceptable risks. Gaining experience may also help to reduce the lack of knowledge.

3.2.4 Hazard Mitigation

The next step is to minimise hazards that can lead to intolerable damage. This damage can be the irreversible destruction of resources or the environment or personal injury. The result of the hazard minimisation is a list of possible measures or requirements for the system. This list contains proposals for the realisation of the system architecture, design or implementation. These suggestions may be based on verifiable ideas or experience.

3.2.5 Documentation

In the analysed standards, documentation is required as the last step of the analysis. These documents can be part of a certification of a system. This step cannot be generalised due to different certification procedures. However, it is possible to continuously record the results of the analysis during the individual steps. Word, PDF or HTML documents can be generated automatically. The continuously generated documents can then be reused for the creation of the certification documents.

As systems are developed in collaboration with different domains, it is possible that an analysis will need to be performed on different versions of the system description.

4. Results

The observations and results are divided into the management process and the methods.

4.1 Management Process

The analysis lasted nine months, from 2018 to 2019. During this time, as shown in Fig. 4 shown, 24 different versions of the FHA Excel sheet were created. During this time, the phases "Seperate" [1:5], "Merging" [6:10], "Approving" [11:16] and "Requirements" [17:24] emerged.

In the "Separate" phase, a system description was created and the first hazards were identified. The methods described above were used in brainstorming workshops to identify the hazards. During "Merging" stage, the system description and identified hazards were merged and aligned.

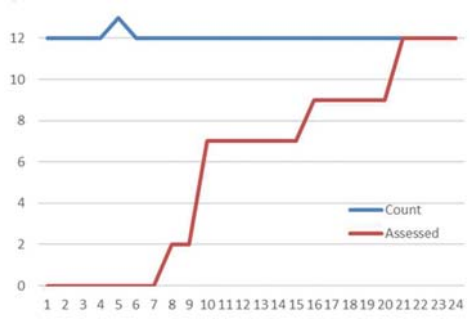

Fig. 4 Analyzed Function over versions

This was followed by the "Approving" phase. In this phase, the hazards were discussed in reviews. In addition, arguments and publications were collected to support the assessment. If possible, the first mitigation measures were discussed.

In the last phase, "Requirements", the agreed mitigations were converted into requirements. Finally, the analysis was documented in a report.

4.2 The FHA

The results and observations for the FHA are divided into three parts. The System Description as the foundation of the analysis, Hazard Identification and Analysis and Mitigation.

4.2.1 System Description

Since the ARP4754A does not make any clear statements about the quality of the system description, we observed in the project that each partner had its own system description at the beginning. This varied in the level of detail of the functions. In the DLR, an attempt was made to make the system description solution-neutral. This resulted in a very abstract description of the system functions. In order to be able to understand the concept better, the description was carried out through two functional levels. Due to the greater experience with the system to be developed, the functional description of SAFRAN was much more detailed and used up to four functional levels. This confirms the observation in [Al01] about the use of different abstractions. As was also shown, the functions themselves were described differently. While in DLR the function of the fuel cell was described as "Convert chemical to electrical energy", in SAFRAN this was done by the

two functions "Operate H2 to e- reaction" and "Collect e-". Both observations are due to a lack of a shared language. Furthermore, multiple meanings, i.e. semantic of terms, occur. As a result, we describe functions as verb-noun combinations as proposed in [Ro76]. Furthermore, by using unified terminology as suggested by [St00], we enabled a standardised functions description. Thus, a "unified" language evolved through time. As a result, we observed that the number of functions F_n remained constant at 12 (Fig. 4).

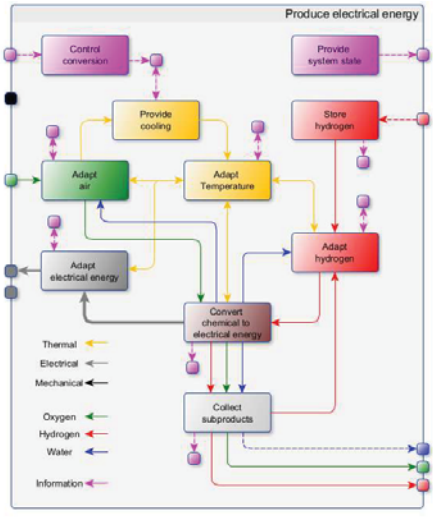

Fig. 5 System function of fuel cell

With the determinations described above, the "Merging" phase was used to create the Fig. 5 was obtained in the "Merging" phase. For the identification of hazards, the system states S1 "Normal" for use and S2 "Maintenance" were defined. In addition, the states C1 "Normal", C2 "Degraded" and C3 "Failure" were assumed for each function.

4.2.2 Identification of the hazards

First, the PHA can be carried out for the identification of hazards. However, since no PHL was available and had to be created, the hazards were derived from the functions and the states. For this purpose, the function, the system and the state of the function were considered for a hazard. For example, for the function "Store hydrogen", the state "degraded" results during normal use. Thus, all possible hazards can be combined as follows.

$$H = F_i \times S_j \times C_k \mid i\,[1 \ldots 12];\ j\,[1,2];\ k\,[1,2,3]$$

In the first step, this resulted in 72 possible hazards. The condition "Normal" was also considered, as the influence of the environment on the respective function should also be considered.

Following that, more hazards were discovered in workshops using guide words. "Too early," "too late," and "too much" were among the proposals. The hazards count must be increased because the guiding words refer to the number of states of a function. This yielded 144 possible hazards.

Finally, at a brainstorming session, "what-if" questions were asked. Supercooling, for example, can cause ice to form in the fuel cell. The number of hazards is difficult to determine and may vary depending on how the workshop is conducted.

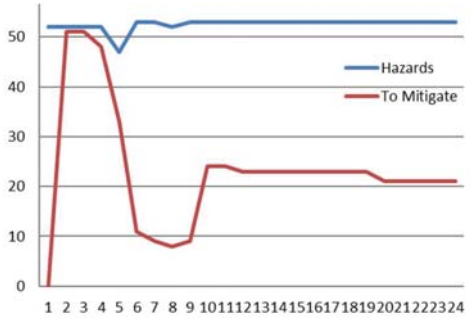

Fig. 6 Count of Hazards and Mitigations

As shown in Fig. 6 the count of possible hazards remained almost constant. Changes at the start are due to work being done separately in the "Separate" phase. From version 9 onwards, the number of hazards has stabilised. The following observations could be derived from the results. Working separately and using the guide words, a consensus on the hazards found may be achieved. Among other things, this strengthened the confidence in the identified hazards. Furthermore, additional hazards that had not been considered before were also identified in the workshops that were staffed by the different teams. This confirms that collaboration can be a fertile environment for discovery [Ba03]. Disagreements and different viewpoints during a discussion might encourage people reconsidering their preconceptions [Ro14].

The severity of the identified hazards was estimated to reduce the effort of the next phase. Also, it is known the risk of creating a bias may exist.

4.2.3 Hazard analysis and assessment

As shown in Fig. 7, following the initial identification, additional hazards were proposed during the analysis. These were consolidated in the "merging" phase. After merging, the number of hazards stabilised at 53.

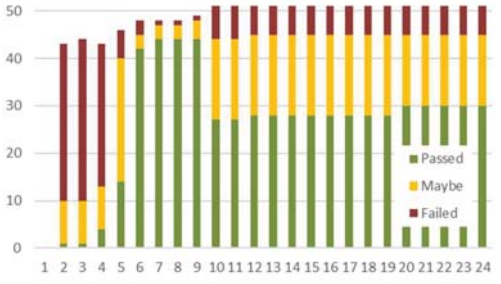

Fig. 7 Hazard assessment

As can be seen, the initial assessment was changed from version onwards. This was due to a better understanding of the application of the method in DLR. In merging, the impact estimate was finetuned through the discussions in the workshops. This led to the assessment becoming almost stable with the transition to "Approving". At the end of the assessment, 30 hazards were judged to be safe, 21 hazards need mitigation and two hazards are covered by other hazards. The function "convert chemical to …" is responsible for the six catastrophic hazards. One example is the likelihood of ice forming in the fuel cell, which might destroy the membrane.

Effort estimation

If one wants to estimate the effort E that is required to consider all functions and the associated states, the following formula results:

$$E = F_i \times S_j \times C_k \times E_e$$

Here, E_e represents the estimated effort of each individual assessment.

The estimated effort may depend on the experience in applying the method as well as the knowledge about the system to be assessed. Thus, a good estimate can only be based on experience. However, in order to get a rough idea of the effort required, an average effort should be assumed as an example. In a first approximation, this should be 45 - 60 minutes per assessment. This includes the analysis, the procurement of supporting material and the documentation of the results. Thus, a first estimate of the effort for 72 hazards would be 7 - 9 days.

If the required reviews are still to be considered, an additional 15 - 30 minutes per participant per assessment can be considered. On average, 6-7 developers took part in the reviews. The total time required for the reviews is thus estimated at around 16 days. If the review results in additional work, these costs must also be considered.

4.2.4 Hazard Mitigation

During the analysis, initial ideas for mitigating the hazards were already discussed. As shown in Fig. 8 the first mitigations were described from version 17 onwards. The number of mitigations increased until the end, but consolidated to 63.

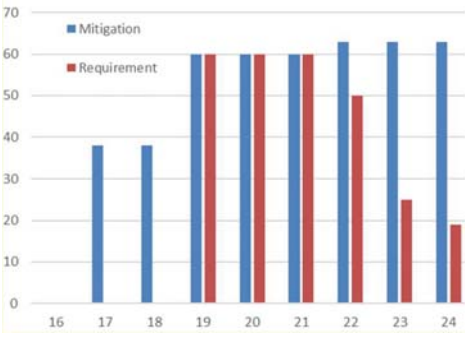

Fig. 8 Count of Mitigations and Requirements

Requirements were derived directly from the recommendations. This was done from version 19 onwards. In the course of the development workshops, the requirements were coordinated. In this way, existing requirements were considered and only previously unknown requirements were considered. Finally, the FHA proposed 19 requirements for the development. The FHA template had to be extended in order to trace the requirements. This was implemented by adding a new sheet.

5. Conclusion

Collaboration resulted in the identification of 19 requirements for 21 hazards. These were considered during development.

Distributed hazard analysis offers advantages and disadvantages. According to our assessments and observation, the former outweighs the latter.

We identified a clear need for open communication. We initially encountered understanding issues as a result of our varying experiences and

backgrounds. This could be mitigated with presence workshops to obtain a better understanding. We were able to observe this in the system description, which was quickly agreed upon and only minor changes were made to the functions during the analysis.

The workshops had a positive impact on the results quality. Being able to hold them in a variety of configurations allowed us to learn from one another while establishing a collaborative atmosphere. According to our observations, if possible, hold many workshops in mixed teams. Furthermore, it was discovered that the workshop leaders' experience might produce well-balanced results. Because some workshops could take many days for organizational reasons, a "fatigue effect" was noted. Short intensive workshops are advised.

From the perspective of the FHA method, the use of guiding terms can lead to quick initial results. However, a fatigue effect can occur as a repetitive pattern emerges. For example, during a midday workshop it was observed that there was a tendency to use standard terms. The use of brainstorming can help identify new hazards, as we observed. However, the quality of the brainstorming depends on the expertise and understanding of the system of the participants. An environment where participants could openly ask questions was beneficial. For workshops, it can be recommended to establish and value an atmosphere of learning.

Acknowledgement

Parts of the research have received funding by the Framework Program Horizon 2020 under grant agreement 779576 (FLHYSAFE).

References

[Al01] Allenby, Karen, and Tim Kelly. "Deriving safety requirements using scenarios." Proceedings fifth IEEE International Symposium on Requirements Engineering. IEEE, (2001).

[Ba03] Barron, Brigid. "When smart groups fail." *The journal of the learning sciences* 12.3 (2003): 307-359.

[Be20] Berres, Axel, and Tim Bittner. "A seamless Functional Hazard Analysis for a fuel cell system supported by Spreadsheets." (2020).

[Bi92] Birkhofer, Herbert. *Analyse und Synthese der Funktionen technischer Produkte*. Diss. Verlag nicht ermittelbar, 1992.

[Bm23] BMWGroup. iX5 Hydrogen trotzt extremer Kälte. 2023, https://www.bmwgroup.com/de/news/allgemein/2022/bmw-ix5-hydrogen.html.

[Da99] Dawkins, S. K., et al. "Issues in the conduct of PSSA." (1999).

[Fa06] Faleiro, Lester. "Summary of the European power optimised aircraft (POA) project." _25th International Congress of the Aeronautical Sciences, ICAS_. 2006.

[Ho23] Hoff, Tim, et al. 'Implementation of Fuel Cells in Aviation from a Maintenance, Repair and Overhaul Perspective'. *Aerospace*, vol. 10, no. 1, Multidisciplinary Digital Publishing Institute, 2023

[Ly21] Lyon, Bruce K., and Georgi Popov. "Preliminary Hazard and Risk Analysis." Risk Assessment: A Practical Guide to Assessing Operational Risks (2021): 123-136.

[Me23] Mercedes-Benz. *GLC F-CELL Mercedes-Benz*. 2023, https://www.mercedes-benz.de/passengercars/mercedes-benz-cars/models/glc/glc-f-cell/der-neue-glc-f-cell.html.

[Of23] Office of Energy Efficiency & Renewable Energy. 'Hydrogen Storage'. _Energy. Gov_, 2023, https://www.energy.gov/eere/fuelcells/hydrogen-storage.

[RE00] Redmill, Felix, Morris Chudleigh, and James Catmur. "System safety: HAZOP and software HAZOP." Industrial Management & Data Systems (2000).

[Ro14] Rodriguez, Edel. "How Diversity Makes Us Smarter." *Scientific American* 311.4 (2014).

[Ro76] Rodenacker, Wolf Georg, and Wolf Georg Rodenacker. *Methodisches konstruieren*. Springer Berlin Heidelberg, 1976.

[Sa15] Sarlioglu, Bulent, and Casey T. Morris. 'More Electric Aircraft: Review, Challenges, and Opportunities for Commercial Transport Aircraft'. _IEEE Transactions on Transportation Electrification_, vol. 1, no. 1, IEEE, 2015, pp. 54–64.

[Sa95] ARP4754A: Certification Considerations for Highly-Integrated or Complex Aircraft Systems. SAE Systems Integration Requirements Task Group AS-1C, ASD. (1995).

[St00] Stone, Robert B., Kristin L. Wood, and Richard H. Crawford. "A heuristic method for identifying modules for product architectures." *Design studies* 21.1 (2000): 5-31.

[Ti02] Tixier, Jerome, et al. "Review of 62 risk analysis methodologies of industrial plants." *Journal of Loss Prevention in the process industries* 15.4 (2002): 291-303.