System Engineering Methods for Reliable Electrical Power Train Design for All Electric Aircraft

Jonas Franzki
Institute for Electrical Machines, Traction and Drives
Technische Universität Braunschweig
Braunschweig, Germany
e-mail: jonas.franzki@tu-braunschweig.de

Anna Nanzig
Institute :metabolon
Technische Hochschule Köln
Köln, Germany
e-mail: anna.nanzig@th-koeln.de

Markus Henke
Institute for Electrical Machines, Traction and Drives
Technische Universität Braunschweig
Braunschweig, Germany
e-mail: m.henke@tu-braunschweig.de

Anna-Lena Menn
Department of Engineering and Communication
Hochschule Bonn-Rhein-Sieg
Sankt Augustin, Germany
e-mail: anna-lena.menn@h-brs.de

***Abstract*—Reliability management, including hazard and risk analysis, is essential for the product development of All Electric Aircraft (AEA) systems to ensure the safety of people and the robustness of the system. In this study, a Model-Based System Engineering (MBSE) approach is proposed that integrates reliability and safety analysis into an accessible system model that improves collaboration among stakeholders, especially those with framed technical involvement. Using a bond graph-based method in Mathworks' System Composer, the interfaces and interactions of the components are modelled and the consequences of possible failures are shown. Established methods, such as Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), and Reliability Block Diagrams (RBD) are compared. All of these safety analyzes are compatible with the proposed MBSE approach. The aim is to outline an approach to analyze system reliability and safety rather than cataloguing every possible failure of an electric drive system. This method provides structured, visual means of analyzing complex failures that go beyond traditional, spreadsheet-based documentation, allowing for better alignment between safety and design.**

Keywords-MBSE, reliability, all electrical aircraft, system model, safety analysis, electrical powertrain

I. Introduction

Reliability management and Hazard And Risk Analysis (HARA) are one of the most important aspects in the product development process of all electrical aircraft systems. Therefore, the focus of research and development is on reliability improvement of electrification components as, e.g., presented in [1] and on the conscientiously conducted HARA to avoid injury and death of people. The aim of HARA is to avoid systematic errors in the product development process and to make the system robust against errors, requirements for the technical system are derived from the HARA. In addition, HARA is mandatory according to CS-23 and 25 [2][3].

This complex part of product development is to be simplified through the use of a complexity-reducing method and simple MBSE language, so that even stakeholders with little involvement have easy access to the technical system. Our method includes a physical approach and is based on bond graph theory [4]. SysML language is consciously not used, but System Composer, block-oriented language, because of the intuitive use and linkability to multiphysical 1D simulation (Simscape). Nevertheless, the building of the system model requires a deep understanding of the technical system.

The core of our method is the interface visibility to show the consequences of failures of the electric porpulsion system. At the beginning of this development, links between faults are shown in a systemic, model-based way, thereby promoting a better overview and collaboration between safety and design engineers. As a rule, HARA results are recorded in tables that do not provide any information about the possible relationships between faults. Our system model enables the direct derivation of HARA [5].

To discuss the method and the proposed procedure, an all electric aircraft propulsion system is chosen, in particular the drive unit consisting of: electric motor, gearbox, and propeller.

In electric aviation, performance, mass, and safety are the three most important development aspects, so it is particularly important to understand safety and technical requirements as a common construct from the outset. Finally, it is important to note that the focus is on showing and discussing a method; it is not the aim to show all possible failures of an electrical propulsion system as displayed in Figure 1.

The remaining content is structured as follows: In Section II the applicable standards as well as existing methods and their respective challenges are presented as a background for the system engineering method proposed in Section III. In Section IV a functional safety analysis is performed on an electric drive unit as a basis before applying the proposed system engineering method in Section V. Finally, conclusions are drawn in Section VI.

II. Standards, Methods and Challenges

In the context of aircraft, many standards define the requirements and procedures to follow. The most important ones for the design of electrical drives will be presented in this section

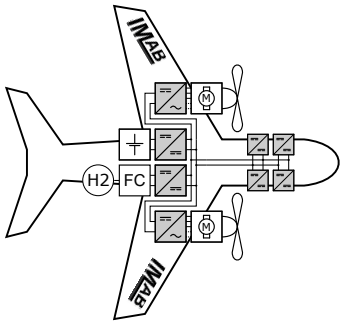

Figure 1. On-board power supply of an AEA concept

alongside methods and challenges in the evaluation of reliability of new electrical drives for aircrafts. Many procedures of realiability and safety analysis are already known: FMEA, FTA, HARA, RBD and PoF (Physics of Failure). Some of these methods are presented and discussed in this section. The method developed is intended to support existing methods and to improve and clarify their application and results.

A. Standards

The Certification Standards (CS) CS-23 [2] and CS-25 [3] define most important requirements for the certification of small and large aircrafts, respectively. The manufacturer must demonstrate compliance to these standards for the aircraft to be granted type certification. This involves requirements applicable to components such as electrical drives.

CS-23 [2] applies to small airplanes (e.g., commuter, private, and training aircrafts). Design and performance criteria are generally less strict than for large airplanes and apply to simpler systems with less redundancy since the operational environment is considered less demanding (fewer passengers, simpler flight profiles). Although safety is still a priority, the measures may be more straightforward and potential failure mode analysis and their mitigation less extensive. Thus, testing is less costly with fewer tests required compared to CS-25 and simpler documentation.

The design should ensure that there are means to give immediate warning to the flight crew in case of a failure of any generator or propulsor, and each must have an overvoltage protection system to prevent damage to the electrical system or equipment supplied by it in case of an overvoltage condition. Furthermore, each electrical system must be free from hazards in its operation and effects on other parts of the aircraft, ensuring safety and reliability. [2]

In contrast, CS-25 involves more complex systems with high redundancy requirements with great emphasis on redundancy, fault tolerance, and fail-safe design to ensure safety of more passengers and demanding operations. Hence, more rigorous testing, validation, and documentation processes including extensive Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) are required to minimize risk of failure. [3].

TABLE I. FUNCTIONAL RELIABILITY METHODS

	HAZOP	FMEA	FMEDA	FTA	RBD	Markov
in-/de-ductive	in	in/de	in	de	de	de
qualitative quantitative	qual	qual	quan	quan	quan	quan
depth of detail	rough	variable	detail	detail	rough	rough
IEC Standard	61882	60812	61508	61025	61078	61165

The complex nature of the compliance process highly motivates the development and use of guiding, supporting, structuring, and visualizing tools to facilitate the process.

B. Functional Safety Methods

There are many methods to investigate the functional safety of a system. They can be divided into inductive and deductive methods. Deductive methods work top-down, they start from known causes to find unknown effects, whereas inductive methods work bottom-up, starting with known effects to seek their unknown causes. Additionally, they can be split into qualitative and quantitative methods: qualitative methods look for the robustness and fault tolerance of architectures, while quantitative methods look into the failure rate, sum of parts and unavailability[6].

Common methods for the analysis of functional safety are: HAZard and OPerability study (HAZOP), Failure Modes and Effects Analysis (FMEA), Failure Modes, Effects and Diagnostic Analysis (FMEDA), Fault Tree Analysis (FTA), Reliability Block Diagram (RBD), Markov, and many more (see Tab. I).

As previously presented, FMEA and FTA are already integral parts in the certification process. They are well compatible with each other. While FMEA offers mainly a bottom-up approach (inductive), FTA can be used for top-down (deductive). Both require an initial Hazard and Risk Assessment (HARA). Thus, HARA can be used to perform an initial analysis and then either a FTA can be conducted or the failure modes can be assessed in their Severity (S), probability of Occurence (O) and Detection (D), the product of which results in a Risk Preference Number (RPN) for a FMEA. Thus, HARA and FMEA allow for a variable depth of detail in the analysis and are, hence, easy-access tools.

The combination of HARA, FMEA, and FTA is a compelling and often used tool chain in traction applications, also as manifested in the ISO 26262 automotive standard for functional safety ISO 26262 [7]. For this reason, the present study will conduct a combination of HARA and FMEA for an electric drive train to achieve a basis example on which a system reliability model will be created, which allows for a comprehensible and visually appealing depiction of system engineering approaches on reliability.

C. Challenges

HARA and FMEA are table-based tools with often extensive lists and little visual appeal, making it hard for less technically

adept stakeholders. Model-Based Systems Engineering gives the possibility to visualize the system topology from the beginning. System models using a simple modeling language could close this gap. Model-Based Systems Engineering (MBSE) is a methodology that focuses on using models as the primary means of information exchange and system design throughout the engineering lifecycle. Instead of relying solely on traditional documents, MBSE emphasizes graphical and digital representations to capture, analyze, and communicate system requirements, design, analysis, and validation. This approach improves consistency, traceability, and collaboration between stakeholders. Key advantages include reducing errors, enabling early detection of design issues, and facilitating integration across disciplines.

III. Proposed System Engineering, Method and Procedure

A. Structure MBSE method

The proposed method leads to an advanced system model that enables the mitigation of a hazard and risk analysis. To achieve the aim, the method is divided into four parts building on each other, the method is illustrated in Figure 2. The first part of "abstract modeling" is mandatory if a new product is developed, which did not exist before. The result of this part is the knowledge of the physical elementary functions and the possible solutions to convert energy from one form to another, like electrical to mechanical. If the system under investigation is already known, it can be skipped and initialized with system consideration with "basic modeling". In advance, it is mandatory to set up the framework that includes the nomenclature and the specification of the modeling language. This is important to create a common understanding of the description of the technical system. The next part is mainly concerned with the superordinate representation of the system to be analyzed, i.e., to clarify which main components make up the system and which components are connected to each other via which physical domain. The result of "basis modeling" is a basic system model that shows the energy and signal flow structure of all components. It represents only one level and shows which energy flow represents the input and output of the respective component. This one-level system model is the basis for the next part, which leads to the final advanced system model. This part is divided into three subparts: function analysis, risk analysis, and final risk mitigation.

Function analysis begins with a decomposition of the components, the components are disintegrated into subcomponents, and more levels are created. The motivation of this decomposition is to get to know the causes and hazards. Therefore, functions and possible malfunctions of the subcomponents are determined, and thus the system is analyzed by possible loss of function. The loss of function is declared for causes and hazards derived from this. Malfunctions are always a disturbance in the energy transmission or power transmission in the sense of the bond graph theory, divided into flow and effort variables. This theory also empowers the multiphysical system view, because each component is connected to several

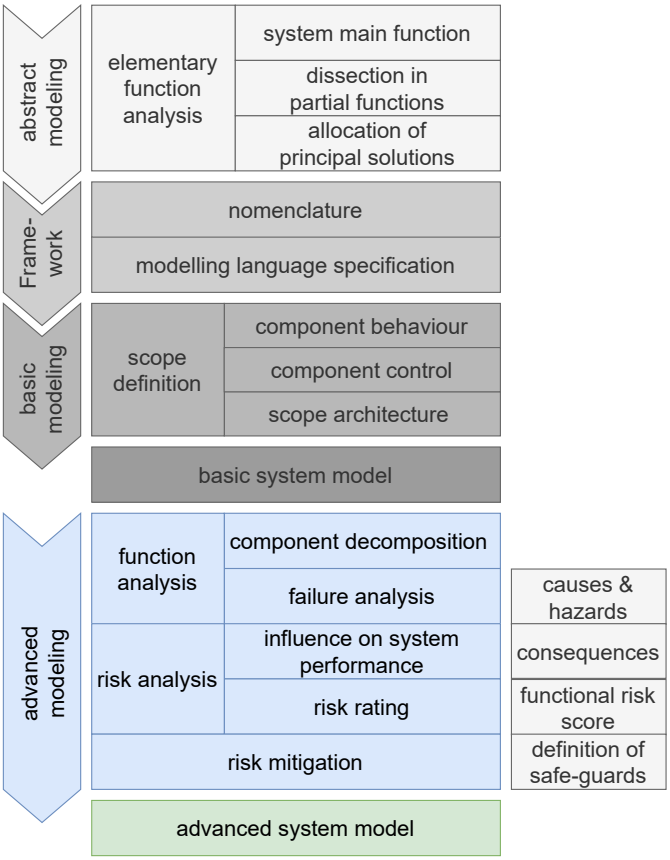

Figure 2. Schematic diagram of the method

physical domains. So, the result of the first subpart are causes and hazards, while hazards bundle several causes. To start risk analysis, the influence on the system performance is the next step. The result is called consequences and describes the impact on system behavior. Risk anlaysis ends with a risk rating according to severity, exposure, and controllabity, resulting in defining a functional risk score. This rating is still provided by human intelligence. The last step of the method is to mitigate the risks and define safe guards. The final advanced system model completely replaces any table. Technical requirements are derived from the safe guards and their effect can be proofed by 1D multiphysical simulation.

Thus, the proposed method offers a strategic and clearly visualized way to show compliance of newly developed systems with CS-23 / CS-25 or automotive standards. It maps failure scenarios, facilitates finding interacting failures, and includes mitigation strategies. A comparison to FMEA and FTA is shown in Table II.

Section V will show a detailed application of the method.

IV. Applied Functional Safety Analysis

As outlined in the previous section, the system model is based on the functional safety analysis of a defined subsystem. This is generically performed here on the electrical machine drive to demonstrate the applicability and merits of the proposed method. Usually HARA is performed on complete

TABLE II. COMPARISON OF PROPOSED SYSTEMS ENGINEERING METHOD (SEM) TO FMEA AND FTA

Criteria	FMEA	FTA	SEM
Visualisation	No	Yes	Yes
Link between interacting components and failures	No	No	Yes
System wide evaluation of failure consequences	Yes	No	Yes
Failure mitigation and safeguards	Yes	No	Yes

TABLE III. SCORING SYSTEM

Criteria	Score	Definition
Severity	0	No function reduction
	1	Moderate reduction in degree of performance
	2	Severe harm to drive unit
	3	Loss of full drive unit
Exposure	0	Incredible
	1	Very low probability
	2	Low probability
	3	Medium probability
	4	High probability
Control-lability	0	Controllable in general
	1	Simply controllable
	2	Normally controllable
	3	Difficult to control or uncontrollable

systems, however, it can also be utilized for subsystems with appropriate adaptation as later expanded.

Exemplary hazards to the electrical machine are overheating and winding failure. The former can be induced by a variety of causes like failure of coolant pump, coolant leaks, or other component failures (reservoir, filter). Winding failure could be caused by insulation aging or short circuit after overload operation. The hazard of power loss due to magnet demagnetization can be caused by a number of causes as well, like overheating, manufacturing error, or overcurrents.

All causes can be sorted according to the failing system (e.g., cooling or motor) and physical domain (e.g., hydraulic, thermal, mechanical, electrical), which can later be used for graphical highlighting. Furthermore, all cause-hazard combinations must be scored according to their severity, exposure, and controllability according to HARA. The scales according to ISO 26262 can be utilized while translating "harm to and loss of life" to "harm to and loss of the drive unit", as can be seen in Table III.

An examplary score for PM mechanical damage and demagnetization can be found in Table III.

Safeguards can then be defined based on these hazards, causes, etc. The SIL score gives an indication on the scope of measures to be taken. That is, the rating "QM" indicates quality management is sufficient, whereas A, B and C-levels require increasing consideration, respectively. These HARA results are used to augment the basic system model with reliability aspects as described in the following section.

V. SYSTEM MODELING APPLICATION

The concrete application of the developed method will be presented in this section. The Mathworks System Composer is used as a tool for creating the system model. The creation of an advanced system model will be carried out using the example of the motor of an AEA.

The first step is the creation of the basic system model, which is skipped at this point and started directly with the creation of the advanced system model. This is an important step in order to be able to perform a risk analysis based on a system model. Figure 3 therefore already shows the completed basic system model of the left wing of an AEA. The colors of the components are chosen to indicate their respective domains. Electrical components are shown in blue, while mechanical components are labeled in green.

This section describes the development of the advance system model of the motor. The term ‘system’ should be understood to mean that each subcomponent consists of further, more in-depth components that together form the overall model.

The first step is to decompose the motor into its main components: rotor and stator. These two components can in turn be decomposed into further subcomponents. Figure 4 shows a detailed decomposition of the rotor, which consists of the magnet system, the shaft bearing system, the rotor laminations and the rotor sleeve.

Analyzing possible faults, also known as causes, in the individual subcomponents inevitably identifies potential hazards that can result from these malfunctions. These hazards are shown as red blocks in the system model, as different faults can lead to the same hazard. For example, both bearing friction and loss of magnetization can lead to heating of the rotor. Risks can be derived from identified hazards that are assessed directly in the system using a risk score. This can be based on previously performed (or known) risk analyzes.

The identified risks leave the rotor component as the output. Logically, action must now be taken to manage these risks. Figure 5 shows how the various risks leave the PMSM. Basically, solutions are identified here to minimize the risks. For example, the risk of ‘dysfunction of magnets’ can be reduced through a more robust design, higher safety margins, or improved quality management.

TABLE IV. SCORING EXAMPLE

ID	Hazard	Causes	System	Category	Severity	Exposure	Controllability	SIL-Score
1	Demagnetization	overheating	motor	thermal	2	1	1	QM
2	Demagnetization	manufacturing	motor	mechanical	1	1	1	QM
3	Demagnetization	overcurrent	motor	electrical	2	2	2	QM
4	PM mechanical damage	incorrect sleeve	motor	mechanical	3	2	3	B
5	PM mechanical damage	incorrect operation	motor	mechanical	3	1	1	QM

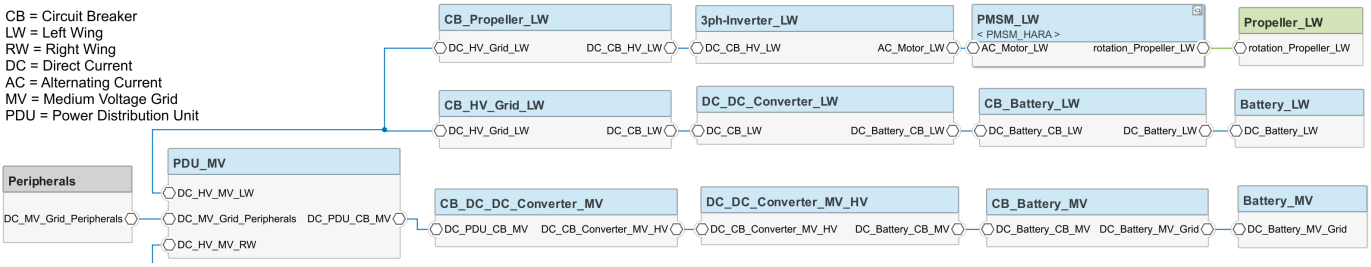

Figure 3. Basic system model of the left wing of AEA.

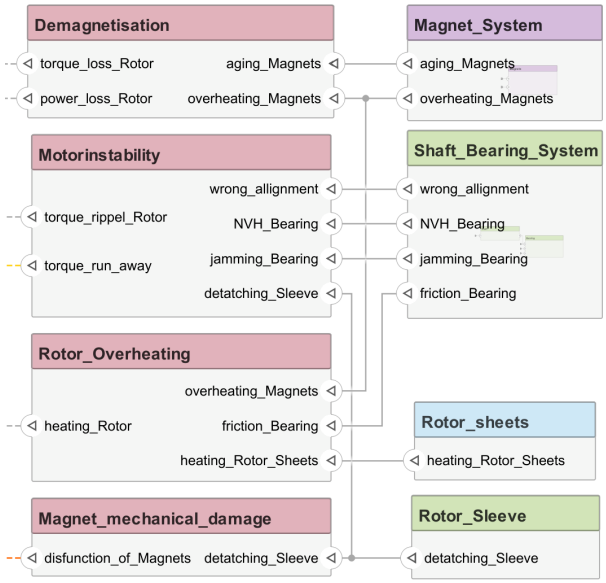

Figure 4. Decomposition of the rotor

The diagram also clearly shows that different risk scores are assigned to the various hazards. Particularly critical hazards are marked in red, less critical ones in yellow, and hardly critical ones in gray according to their SIL score.

VI. Conclusion

This paper presents a low-threshold MBSE method that integrates functional safety considerations into the system modeling process. Using this approach, the system model facilitates the identification and derivation of hazards and their causes in a structured and traceable manner. On the other hand, it must be said that setting up the system model for the first time requires expert knowledge in the respective technical field of application. The physical complexity is very high. Causes are always an impairment in energy transport according to bond graph theory. Moreover, the system model enables the mapping of functional safety aspects in a way that promotes better understanding, even among individuals with limited prior experience or involvement in safety-related topics. This aspect enhances cross-disciplinary collaboration and improves communication within teams. However, it is important to note that the creation of a comprehensive and advanced system model demands a deep understanding of the underlying technical system. This prerequisite highlights the need for skilled practitioners during the initial model development phase. The system model can be reused in a subsequent FMEA later in the product development process. Thus, the proposed MBSE method not only supports the integration of functional safety considerations but also contributes to the efficiency and effectiveness of safety engineering practices.The connection between the detection of errors and the bond graph theory will be addressed in greater depth in future research projects. It is planned to take a closer look at the mathematical underpinning with the help of the bond graph theory of the method presented here.

References

[1] R. Keilmann, L. Radomsky, D. Ferch, and R. Mallwitz, "Study of inverter topologies for electrified aircraft propulsion systems based on cyclic loading induced bond wire fatigue," in *2024 Energy Conversion Congress and Expo Europe (ECCE Europe)*, 2024, pp. 1–8. DOI: 10.1109/ECCEEurope62508.2024.10752026.

[2] EASA, *Easy Access Rules for Normal-Category Aeroplanes (CS-23) - Amendment 6 (AMC/GM 4) | EASA*, en, https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-normal-category-0, retrieved: April 2025.

[3] EASA, *Easy Access Rules for Large Aeroplanes (CS-25) - Revision from January 2023 | EASA*, en, https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-large-aeroplanes-cs-25, retrieved: April 2025.

[4] A.-L. Menn and A. Nanzig, "Komplexitätsreduktion von Methoden im MBSE," in *Tag des Systems Engineering*, Würzburg: GfSE Verlag, Nov. 2023, S.100–107, ISBN: 978-3-910649-00-2.

[5] Y. Jiang *et al.*, "MBSE-based functional hazard assessment of civil aircraft braking system," in *2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, Dec. 2020, pp. 460–464. DOI: 10.1109/ICMCCE51767.2020.00107.

[6] L. Fendrich and W. Fengler, Eds., *Handbuch Eisenbahninfrastruktur*, de. Berlin, Heidelberg: Springer, 2013, ISBN: 978-3-642-30020-2 978-3-642-30021-9. DOI: 10.1007/978-3-642-30021-9.

[7] N. Adler, *Modellbasierte Entwicklung funktional sicherer Hardware nach ISO 26262* (Steinbuch Series on Advances in Information Technology / Karlsruher Institut für Technologie, Institut für Technik der Informationsverarbeitung). KIT Scientific Publishing, 2015.

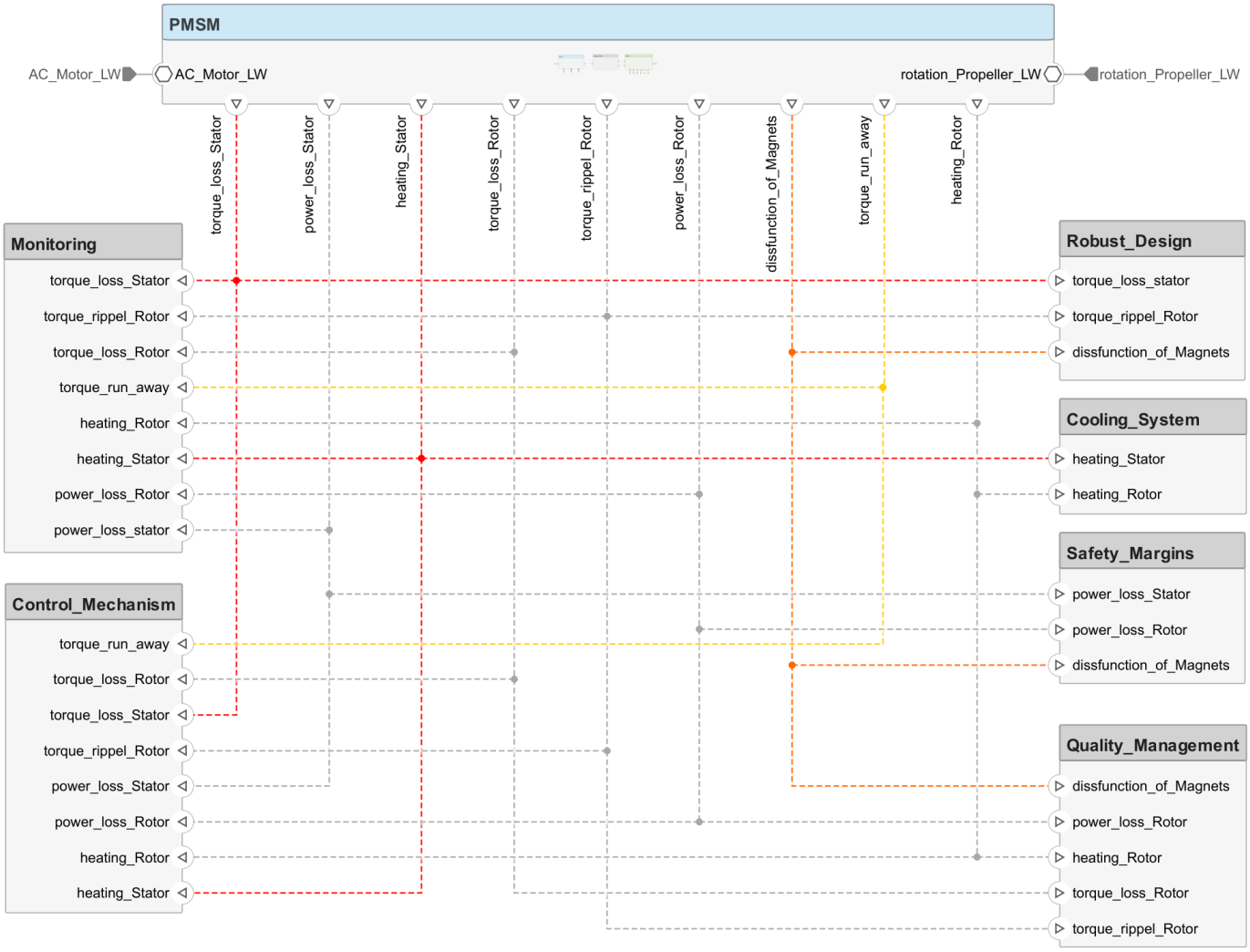

Figure 5. Definition of safe-guards for the PMSM