FMECA assessment for railway safety-critical systems investigating a new risk threshold method

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 28, 2021, accepted June 10, 2021, date of publication June 14, 2021, date of current version June 22, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3088948

FMECA Assessment for Railway Safety-Critical Systems Investigating a New Risk Threshold Method

MARCANTONIO CATELANI[1], (Member, IEEE), LORENZO CIANI[1], (Senior Member, IEEE), DIEGO GALAR[2,3], GIULIA GUIDI[1], (Student Member, IEEE), SERENA MATUCCI[4], AND GABRIELE PATRIZI[1], (Student Member, IEEE)

[1]Department of Information Engineering, University of Florence, 50139 Florence, Italy
[2]Division of Operation and Maintenance Engineering, Luleå University of Technology, 97187 Luleå, Sweden
[3]Industry and Transport Division, Tecnalia Research and Innovation, 01510 Miñano (Araba), Spain
[4]Department of Mathematics and Computer Science "Ulisse Dini," University of Florence, 50134 Florence, Italy

Corresponding author: Gabriele Patrizi (gabriele.patrizi@unifi.it)

ABSTRACT This paper develops a Failure Mode, Effects and Criticality Analysis (FMECA) for a heating, ventilation and air conditioning (HVAC) system in railway. HVAC is a safety critical system which must ensure emergency ventilation in case of fire and in case of loss of primary ventilation functions. A study of the HVAC's critical areas is mandatory to optimize its reliability and availability and consequently to guarantee a low operation and maintenance cost. The first part of the paper describes the FMECA which is performed and reported to highlight the main criticalities of the HVAC system under analysis. Secondly, the paper deals with the problem of the evaluation of a threshold risk value, which can distinguish negligible and critical failure modes. Literature barely considers the problem of an objective risk threshold estimation. Therefore, a new analytical method based on finite difference is introduced to find a univocal risk threshold value. The method is then tested on two Risk Priority Number datasets related to the same HVAC. The threshold obtained in both cases is a good tradeoff between the risk mitigation and the cost investment for the corrective actions required to mitigate the risk level. Finally, the threshold obtained with the proposed method is compared with the methods available in literature. The comparison shows that the proposed finite difference method is a well-structured technique, with a low computational cost. Furthermore, the proposed approach provides results in line with the literature, but it completely deletes the problem of subjectivity.

INDEX TERMS Failure analysis, HVAC, railway safety, reliability, risk analysis.

I. INTRODUCTION

Each year, global transportation systems such as aircraft, motor vehicles, trains, and ships carry billions of tons of goods and billions of passengers. System failures can impact the global economy, the environment, and transportation reliability and safety [1]. In railways, device failure, whether electrical or mechanical, can usually be attributed to the degradation of a given material under stress. Stress generally refers to any external agent capable of causing degradation to occur in the material properties of a device such that it can no longer function properly in its intended application. For this reason, as well as the growing complexity of equipment and the rapidly increasing cost incurred by loss of operation and maintenance, interest in RAMS (Reliability, Availability, Maintainability and Safety) and diagnostic parameters is growing in many industrial fields [2]–[5]. Rail industry is rapidly developing, and rail becomes ever more viable in a wide range of regions. Therefore the passenger experience and comfort has become a major concern for operators in the world [6], [7]. An efficient heating, ventilation and air conditioning system (HVAC) is the best way of regulating temperature and air quality to contrast the overcrowding and overheating of the carriages. Railway temperature regulation is very challenging because of fluctuating climates, fluctuating heat loads and fluctuating speeds. Trains could cross different countries with different climates, nevertheless HVAC equipment must constantly adapt to diverse climates.

The associate editor coordinating the review of this manuscript and approving it for publication was Cristian Zambelli.

During a train travel, lots of passengers can board and depart train cars rapidly, that's cause a constantly variation of the heat (provided by bodies) in the carriage. HVACs must detect the heat changes and regulate the temperature consequently. The high speed of the train cause high gravitational forces on the HVAC which can produce damage to coils, so industries have to design HVAC able to tolerate high gravitational forces and high vibrations.

This paper builds on this interest and develops a Failure Mode, Effects and Criticality Analysis (FMECA) for a HVAC system in a high-speed train. A study of the HVAC's critical areas is mandatory to optimize its reliability and availability. The critical components identified by FMECA needs to be fully analyzed in order to find countermeasures and lower the risk level. The identification of the most critical parts is usually performed by experts, leading to a high subjective decision. Alternatively, some companies apply corrective actions in a hierarchical order starting from the most critical components. Then, countermeasures are applied until the budget allows it. The major flaw of this cost-oriented approach is that some critical risk could not be mitigated. For some application this approach is valuable, quite the opposite safety related applications such railway systems require a more precautionary point of view. Consequently, it is extremely important to identify which components are critical and which are not by means of a risk threshold. The international standard IEC60812 [8] which defines the FMECA technique does not explain how to evaluate a risk threshold value. Furthermore, only few papers in recent literature deals with this issue. This work introduces a new analytical approach to overcome this limit by estimating a Risk Priority Number threshold. The rest of the paper is organized as follows: section II illustrates the state of the art of FMECA in railway field and the existing threshold methods, section III describes the HVAC system in railway application, section IV illustrates the FMECA applied on the "Passenger unit" of the HVAC and finally section V proposes a new method to distinguish the negligible failure modes with the critical failure modes and tests its validness on two different datasets.

II. LITERATURE REVIEW

Failure Modes, Effects and Criticality Analysis (FMECA) is a widely used technique because it is a structured and systematic procedure which allows to identify the criticalities of a system. It is a powerful tool for early identification of failure mode in various industrial applications [9], [10]. It is also widely applied for reliability assessment of safety critical systems, such as in [11]. FMECA includes a means of ranking the severity of the failure modes to allow prioritization of countermeasures [12], [13]. This is done by combining the severity measure and frequency of occurrence to produce a metric called criticality, also known as the Risk Priority Number (RPN).

The analysis is usually done by identifying the failure modes and failure mechanisms, their respective causes, and their immediate and final effects. The analytical results can be presented on a worksheet that contains a core of essential information for the entire system and the details developed for that specific system. The worksheet shows the ways the system could potentially fail, the components and their failure modes that would be the cause of system failure and the cause(s) of each individual failure mode. Finally, there is a ranking of the frequency of occurrence (usually called O), a ranking of the severity measure (usually called S) and a ranking to take into account the detection of each failure mode (usually called D).

The three factors are combined to calculate the Risk Priority Number (RPN), as in the following expression [14]:

$$RPN = O \cdot S \cdot D \tag{1}$$

where:

- Occurrence O is the probability that a failure mode will happen; therefore, it is strongly linked to the failure rate of the equipment. It can assume integer values belonging to the interval [1; 10] where 10 is the most probable failure mode.
- Severity S defines the strength of the failure impact on the system. It can assume integer values belonging to the interval [1; 10] where 10 represents the worst scenario.
- Detection D indicates the possibility of diagnosing the failure mode before its effects are manifested in the system. It can assume integer values belonging to the interval [1; 10] where 10 is the least diagnosable event.

RPN can judge the risk level of failure modes; with this knowledge, designers can take effective actions to eliminate high risk failure modes [15], [16]. The method is simple and convenient, but its strong subjectivity and unified evaluation standards may result in inaccurate risk determination. Thus, it may have a misleading effect on establishing improvement actions. In addition, after determining the RPN risk sequence, it is necessary to implement corrective actions for the failure mode whose RPN value is higher than the acceptable risk standard.

In the last years, many studies have been carried out to analyze the failure occurrence of railway equipment as well as to evaluate the impact of a failure on transportation (see for example [17]). Cheng *et al.* [18] evaluate the reliability of metro door systems using a FMECA procedures. Kim *et al.* [19] investigate the effects of a failure of the brake system for a railroad unit with a FMECA. Dinmohammadi *et al.* [17] analyze the risk associated to a passenger door system. Carretero *et al.* [20] uses FMECA as starting point for the development of a maintenance plan in railway infrastructure. Deng *et al.* [9] proposes a new framework based on FMECA method to study the vulnerability of a subway system. Marquez *et al.* [21] carry out a Reliability Centred Maintenance based on FMECA for a railway turnout.

The international standard IEC 60812 (2018) [8] which defines and standardizes the FMECA doeas not sufficiently explain how to univocal distinguish the non-critical modes with the critical modes which need corrective actions. Many works in recent literature highlight some drawbacks of the RPN and try to propose different methods to overcome that problems. Several papers propose different RPN formulations introducing weight factors or innovative coefficients and parameters (e.g. [22], [23]). Others solve the problems introducing fuzzy-logic or other analytical theories in FMECA, see for instance [24], [25]. However, most of the papers does not deal with the RPN threshold estimation problem. Therefore, the aim of this manuscript is to fill this gap proposing a methodology for threshold estimation regardless the application field or the mathematical model used to calculate the RPN.

Usually the threshold for the modes is subjectively set by the judgement of multiple experts in the matter (see for instance but not only [26]–[29]), and only few papers propose their own approaches for the threshold value.

Kim *et al.* [30] combines RPN with SOD (Severity-Occurrence-Detectability, a simple composition of the 3 scores) to prioritize high severity of the modes in risk categories.

Bluvband *et al.* [31], [32] highlight for the first time that RPNs follows a trend and recommend a graphical tool for RPN analysis. Firstly, the RPN are plotted ordered from the smallest to the largest. Bluvband illustrates that the RPNs of a complete FMECA form a right-skewed distribution, the critical modes belong to the upper-right part while the negligible modes to the first tail on the left. The threshold value is calculated in a qualitative way by the division between the negligible failure modes and the critical failure modes. The method proposed by Bluvband [31], [32] is an intuitive and simple graphical tool. The idea at the basis of this approach seems to be very interesting. The main concern of the method is related to the subjectivity for the division of the two datasets characterized by different slopes.

Zhao et al [33] propose a method to obtain a more objective and accurate RPN analysis. The RPNs are plotted ordered by size, then using linear regression the RPNs are fitted with a polynomial approximation of the first order, finally the confidence levels are plotted on the same figure. The threshold RPN is determined by the turning point from the confidence levels. This approach is based on a simple linear approximation method, but in many practical cases the RPNs do not follow a linear trend. Therefore, the approximation of the values with a single straight line provides a significant error.

Another procedure to evaluate the threshold value is the 80:20 Pareto principle [34]–[36]. According to this technique, 20% of failure modes produce 80% of the total RPNs. In contrast to the Bluvband method, the Pareto approach uses a bar chart where the failure modes are sorted from the highest risk priority number to the lowest. This bar graph is combined with a cumulative distribution function that shows the percent contribution of all preceding failures. The 80:20 rule is used to distinguish the negligible and critical modes. Pareto chart is not suitable for some kind of risk-assessment application because it is not always verified that the 80% of the criticalities arise from 20% of the causes, or in other words that the 80% of the RPNs represents the 20% of the failure modes.

A preliminary study on RPN threshold has been already published in [37] where a statistical approach based on a boxplot was compared with the other method proposed in literature. It is an easy, practical and efficient solution recommended as a first evaluation to distinguish critical and negligible failure modes. The method proposed in [37] could be used as a first screening of the failure modes, while more accurate and quantitative approach is required in case of safety-critical system (such railway systems).

III. HEATING VENTILATION AND AIR CONDITIONING

This work deals with the risk assessment and RPN threshold estimation of a Heating Ventilation Air Conditioning (HVAC) system. HVAC is the technology of indoor and vehicular environmental comfort. The objectives of HVAC systems are to provide an acceptable level of occupancy comfort and process function, to maintain good indoor air quality (IAQ), and to keep system costs and energy requirements to a minimum [38].

HVAC is an important part of residential structures, such as single family homes, apartment buildings, hotels and senior living facilities; it is also essential in medium to large industrial and office buildings, such as skyscrapers and hospitals, and in vehicles, such as trains, ships and submarines. In all these structures, safe and healthy conditions are regulated with respect to temperature and humidity, using fresh air from outdoors.

In underground trains, the influx of a large number of people and the presence of moving trains generate a reduction in oxygen and an increase in heat and pollutants. Mechanical ventilation is required to achieve the necessary air exchange and grant users of the underground train systems comfortable conditions. Ventilation systems have a second and even more important purpose: to guarantee safety in the event of a fire emergency. Moreover, to create a safe and clean environment, ventilation is required both in the tunnels and in the stations. Consequently, in high-speed trains the HVAC is a safety critical system, it must be working properly during the entire train journey to ensure emergency ventilation in case of hazardous events.

Furthermore, an HVAC system has also comfort related functionalities: it has to move heat to where it is wanted (the conditioned space), or remove heat from where it is not wanted (the conditioned space), and put it where it is unobjectionable (the outside air).

The heating and air-conditioning system, whose central unit is usually placed on the roof of the train, ensures the thermal comfort and the quality of the air on board. Temperature and air quality sensors also play a decisive role, because as well as managing the temperature, the system recycles the air and therefore regulates the amount of oxygen available in the train cars [39].

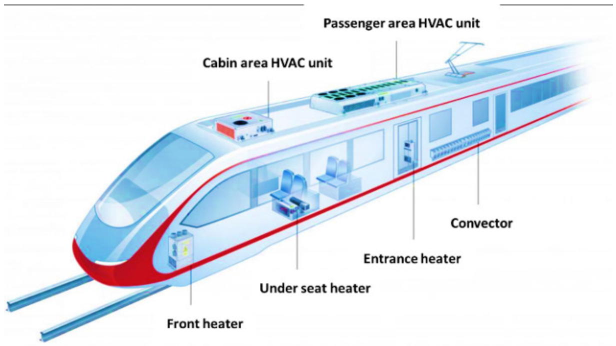

FIGURE 1. Examples of HVAC units located on a high-speed train.

The first step of the functioning of the air condition unit is the suction of warm air by ventilators from the train exterior, then a liquid refrigerant absorb the heat, therefore the heat is rejected outside the train and finally cooled air is released into the train interior. A sensor measures the temperature and the quality of the air inside the train, then the air conditioning absorbs in the air, mixing 1/3 of external air with 2/3 of internal air. The unit reinjects recycled, filtered air into the train unit.

Each car is equipped with two units to provide Heating, Ventilation and Air Conditioning (HVAC) to the car. In order to ensure the proper system functionality, a control system is required to manage all the HVAC. In particular temperature and humidity control are regulated through inside and outside sensors connected directly to a microcontroller-based unit.

IV. RISK ANALYSIS OF HVAC

In order to identify all the risks associated to the use of an HVAC system, in this work a Failure Modes, Effects and Criticality Analysis is proposed. Figure 1 shows the location of the train's HVAC system [40], [41]. There are two units located on the roof of the train: one for the cabin area (called ''Cabin unit'' in the following) and another one for the passenger area or salon (called ''Passenger unit'' in the following) [42]–[44]. The system under analysis is an HVAC assembly in S-121, a high-speed CAF train. Table 1 describes the high level taxonomy of the HVAC under study, according to ISO 14224 [45].

Figure 2 shows a block diagram of the ''Passenger unit'' HVAC under analysis. In particular it is composed by four different sub-systems: cooling, heating, ventilation and control system. The cooling and heating systems aim is to provide a thermal comfort inside the train (the cooling provides air-conditioned while the heating increases the temperature), ventilation provides fresh air and finally the control has to regulate and manage all the other devices. Each system is also divided into several subunit as shown in the figure.

The ''Cabin unit'' is a bit different from the ''Passenger unit''. It is simpler, it is composed by a lower number of components and it uses the control system integrated in the ''Passenger unit''.

TABLE 1. High-level taxonomy of the system under test.

Taxonomy level	Taxonomy hierarchy	Description
1	Industry	Railway
2	Business Category	High Speed
3	Installation	S121
4	Unit	Front car
5	System	HVAC system

TABLE 2. Criteria for severity S assessment.

Severity	Criteria	Rating
None	No discernible effect	1
Very minor	Comfort reduction	2
Minor	Possible failure of one component	3
Very low	Partial loss of one function	4
Low	Considerable loss of one function	5
Moderate	Loss of one function	6
High	Loss of two functions	7
Very high	Loss of all function	8
Hazardous with warning	Possibility of fire	9
Hazardous without warning	Loss of safety without warning	10

TABLE 3. Failure mode occurrence O related to probability of occurrence.

Failure mode occurrence	Rating	Failure rate λ_M [FPMK]
Remote: Failure is unlikely	1	$\leq 1 \cdot 10^{-5}$
Low: Relatively few failures	2	$1 \cdot 10^{-4}$
	3	$5 \cdot 10^{-4}$
Moderate: Occasional failures	4	$1 \cdot 10^{-3}$
	5	$2 \cdot 10^{-3}$
	6	$5 \cdot 10^{-3}$
High: Repeated failures	7	$1 \cdot 10^{-2}$
	8	$2 \cdot 10^{-2}$
Very High: Failure is almost inevitable	9	$5 \cdot 10^{-2}$
	10	$\geq 1 \cdot 10^{-1}$

Classification criteria are used in order to consistently attribute the level of severity, occurrence and detection to each failure mode. These criteria are established in part from the literature and others are specifically chosen for the type of device analyzed. Table 2 illustrates the criteria for the choice of the severity index, Table 3 gives the criteria for the assignment of occurrence values and Table 4 shows the assessment of the detection value. The above-mentioned

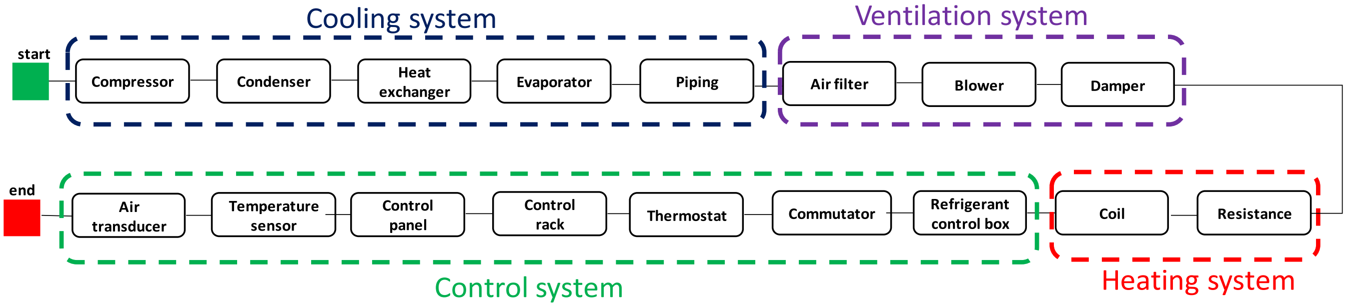

FIGURE 2. Block diagram of HVAC under study.

TABLE 4. Failure mode detection D evaluation criteria.

Criteria	Rating
Completely detectable	1
Partially detectable	2
Impossible to detect	3

tables were developed to analyze both ''Passenger unit'' and ''Cabin unit''.

A severity rank is allocated to the failure effect from each failure mode based on the severity of the effect on the overall system performance and safety in light of the system requirements, objectives and constraints [8].

Table 3 propose the assessment of the occurrence based on the mode failure rate value. If λ is the failure rate of the component, then the mode failure rate λ_M is given by:

$$\lambda_M = \alpha \cdot \lambda \tag{2}$$

where the failure rate fraction expressed by α represents the weight of the mode compared to the other failure modes. In particular, a 1-to-10 scale is assessed, where the higher is the mode failure rate, the higher is the occurrence rate.

The failure rate is generally expressed in failure/hour, but for this application, the information on time is less meaningful than distance. In fact, trains only work certain hours, so the information on the distance travelled is more important and more significant than time. Therefore, the failure rate of the mode in Table 3 are expressed in FMPK - failures per million kilometers.

Table 4 gives the detection criteria used in the case study. Since detection data were barey available for the HVAC system under study, the proposed scale varies from 1 to 3.

Table 5 shows an extract of the whole FMECA for the ''Passenger unit'' of the HVAC system studied. The columns report the following information:

- Failure mode description: manner in which an equipment or machine failure can occur.
- Failure rate fraction (α): a percentage which describes the weight of each failure mode in the component. The sum of every failure rate fraction has to be 100%.

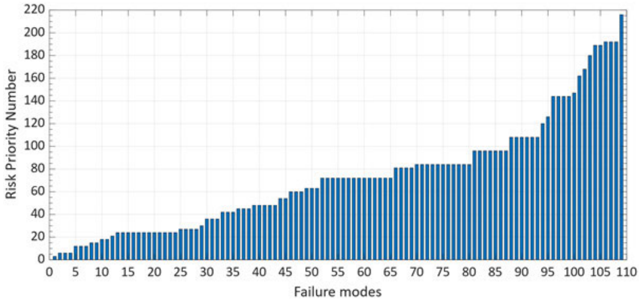

FIGURE 3. Representation of the whole "Passenger unit" FMECA result. All the RPNs are plotted ordered by size.

- Failure rate for failure mode (FPMK): frequency with which the failure mode appears, expressed in failures per million kilometers.
- Failure causes: causes of the failure mode.
- Local effect: normally limited to the effects on the item exhibiting the specific failure mode.
- Global effect: effects of the failure as it would be seen at the next higher/lower level (within the system/equipment structure).
- Occurrence (O): rating of the likelihood of occurrence of each cause of failure
- Severity (S): rating of the severity of each effect of failure
- Detection (D): rating of the likelihood of prior detection for each cause of failure (i.e. the likelihood of detecting the problem before it reaches the end user or customer.
- Risk priority number (RPN): product of the three ratings.

Failure data were provided by the HVAC manufacturer ''MERAK.'' Note that data do not consider any stress applied.

The whole ''Passenger unit'' FMECA is composed of 109 different modes and table 5 shows only an extract of them. The result of the whole FMECA are reported in Figure 3 which illustrates all the 109 Risk Priority Number ordered by size from the smallest to the largest, to improve the readability of the values.

The minimum RPN value is 3, associated to the relay, and the maximum is 216, associated to the blower.

TABLE 5. Extract from the whole FMECA for the "Passenger unit" of the HVAC system under analysis.

Failure mode	α	Failure rate [FPMK]	Cause of failure	Local effect	Global effect	O	S	D	RPN
COMPRESSOR									
Motor seize up	60%	1,68E-02	-Internal failure -Blocked compressor - Damage winding	Loss of pumping capacity	Loss of cooling function	8	6	3	144
Thermostat doesn't detect temperature over limit	2%	5,62E-04	-Overheating of compressor -Thermostat dirty	Loss of overheating protection	Possible damage of compressor	3	5	3	45
Pumping leakage	25%	7,02E-03	-Mechanical failure -Fretting compressor	Loss of refrigerant pumping	Loss of cooling function	6	6	3	108
Valve fails to close	8%	2,25E-03	-Internal failure -Valve dirty	The refrigerant doesn't increase the pressure	Loss of cooling function	5	6	3	90
Internal overload motor protection	5%	1,40E-03	- Motor is short circuit - Electric overload -Motor protection failure	Short circuit of compressor	Loss of cooling function	4	6	3	72
HIGH PRESSURE SWITCH									
Pressure switch in close position	30%	3,08E-03	-Internal failure of the pressure switch -Dirtiness in the refrigerant circuit	No detection in case of high pressure of refrigerant	Possible overpressure	5	5	3	75
Pressure switch in open position	50%	5,13E-03	-Internal failure -Dirtiness in the refrigerant circuit	Incorrect indication of overpressure	Compressor is stopped	6	6	3	108
Refrigerant leakage	20%	2,05E-03	-Refrigerant leakage in the distributor	Leak of refrigerant in the component	Compressor is stopped	5	6	3	90
EVAPORATOR COIL									
Refrigerant leakage	100%	1,04E-02	-Presence of corroded or critical zones	Leak in the component	Loss of cooling function	7	6	3	126
EXPANSION VALVE									
Refrigerant leakage	80%	4,62E-03	-Presence of corroded or critical zones	Leak in the component	Loss of cooling function	6	6	3	108
Valve is not opened	5%	2,89E-04	-Internal failure	Expansion valve is blocked close	Loss of refrigerant circulation	2	6	3	36
Valve is not closed	15%	8,67E-04	-Internal failure	Expansion valve is blocked open	No expansion of refrigerant	4	5	3	60

The figure also highlights several duplicates in the risk priority number scale, in particular the maximum repetition frequency is related to RPN 72, which can be formed by 14 different combinations.

Also, the "Cabin unit" of the HVAC system was analyzed using the FMECA procedure. The complete results were not reported in this work for the sake of brevity. In this second analysis, the minimum RPN value is 4, associated to the pipes, and the maximum is 168, associated to the emergency inverter. Also, in the "Cabin unit" FMECA there are several duplicates in the risk priority number, in particular the maximum repetition frequency is for the RPN 12, which can be formed by 12 different combinations.

V. A NEW APPROACH FOR THE THRESHOLD ESTIMATION

The failure modes characterized by high RPNs have to be distinguish from the modes with lower RPN values. As explained in section II, very few papers in literature deal with this concept. Therefore, a new analytical approach is introduced to overcome the subjectivity and to find a RPN threshold value.

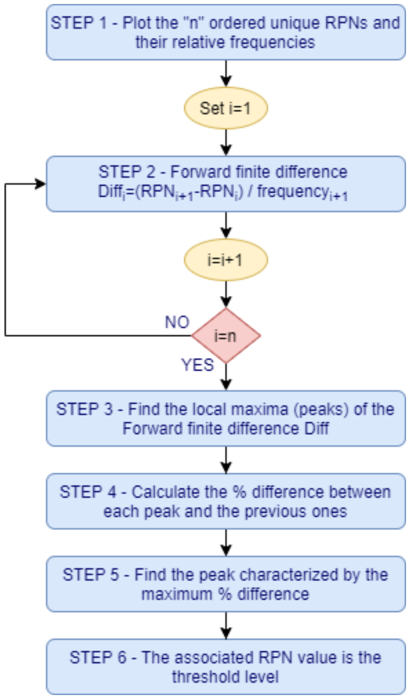
STEP 1 - Plot the "n" ordered unique RPNs and their relative frequencies
Set i=1
STEP 2 - Forward finite difference Diff$_i$=(RPN$_{i+1}$-RPN$_i$) / frequency$_{i+1}$
i=i+1
NO
i=n
YES
STEP 3 - Find the local maxima (peaks) of the Forward finite difference Diff
STEP 4 - Calculate the % difference between each peak and the previous ones
STEP 5 - Find the peak characterized by the maximum % difference
STEP 6 - The associated RPN value is the threshold level

FIGURE 4. Flowchart of the new procedure for risk priority number threshold estimation.

A. DESCRIPTION OF THE PROCEDURE

Figure 4 shows the flowchart of the proposed procedure. The first step is to consider the frequency of each RPN, i.e. the repetition number of each RPN.

For each unique RPN the forward finite difference is calculated. Then the difference is weighted with the size of the sample (frequency of each unique RPN).

In particular, the weighted finite difference $Diff_i$ is defined as the ratio between the forward finite difference of the unique RPN and the frequency of the unique RPN:

$$Diff_i = \frac{RPN_{i+1} - RPN_i}{frequency_{i+1}} \tag{3}$$

where RPN_{i+1} and RPN_i represent the $(i + 1)$*-th* and the i*-th* unique failure modes respectively, while $frequency_{i+1}$ stands for the repetition frequency of the $(i + 1)$*-th* unique RPN.

As the first derivative of a continuous function represents the instantaneous rate of change, the finite difference represents the same concept for discrete data set. So, the higher is the difference, the higher is the variation between two consecutive values. The forward finite difference introduces the repetition of the RPN value as denominator in order to take into account how the repeated values lower the increment. The following step is the identification of the local maxima (peaks) of the finite difference $Diff$. Each peak represents a remarkable increase of two nearby RPNs, the higher the peak the greater the RPN increase. The aim of the proposed procedure is to precisely identify a value that divides the ordered RPNs trend in two different groups: the negligible modes characterized by a gradual change of the RPN values, and the critical modes characterized by a sudden increase of those value. Consequently, the identification of the peaks in the finite difference trend is a fundamental step that allows to quantitatively understand the RPN increments.

Then, the following steps are used to identify the *"first significant peak"*, which is the peak that divides the RPNs into two well-defined and different subsets. In order to find this peak, the proposed procedure is based on the evaluation of the percentage difference $\Delta Peak_i$ between each peak and the previous ones (step 4). More in detail, equations (4)(5) explain the evaluation of percentage increment between the peak i and the mean value of the three previous peaks PP_i.

$$PP_i = \frac{Peak_{i-1} + Peak_{i-2} + Peak_{i-3}}{3} \tag{4}$$

$$\Delta Peak_i = 100 \cdot \frac{Peak_i - PP_i}{PP_i}\% \tag{5}$$

Then, step 5 consists in the identification of the maximum value of the percentage differences evaluated in the previous step. The peak characterized by the maximum value of percentage difference is the *"first significant peak"* and the associated RPN divides the RPNs into two subsets.

The evaluation of $\Delta Peak_i$ as the simple increment between the peak i and the peak $i - 1$ could lead to untrustworthy results since the percentage increase is great enough also for the lower peaks. Moreover, comparing each peak with the same constant value (e.g. the minimum peak, or the first peak, or the first finite difference value, etc.) leads always to identify the peak with the greater value, regardless the dataset. As explained before, the aim of this procedure is not to identify the highest peak, instead it is to identify the first peak much higher than all the previous peaks. Consequently, $\Delta Peak_i$ has been evaluated as the percentage difference between a peak and a small set of previous peaks. More in detail, the mean value of the three previous peaks was used since it provides effective results in several datasets.

The final step consists in the identification of the unique RPN which divides the dataset into two subsets. The index of the *"first significant peak"* is the index of the unique RPN associated to the threshold level.

The proposed approach uses the idea of the identification of two different data set but allows to delete the subjectivity issue that influences most of the previous works using an analytical procedure based on weighted forward finite differences.

The following subsections illustrates the application of the procedure to different FMECAs. Firstly, the proposed procedure has been applied to the "Passenger unit" FMECA described in the previous section. Then, it has also been applied to the "Cabin unit" FMECA in order to validate the method with a different dataset.

B. CASE STUDY 1: "PASSENGER UNIT" FMECA

In this section the procedure is applied to a first case study, so the data coming from the "Passenger unit" FMECA are used to test the effectiveness of the proposed method.

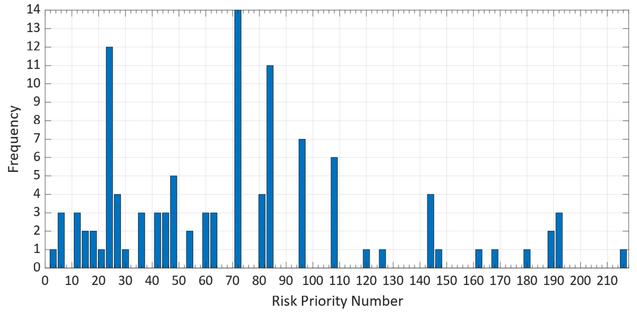

FIGURE 5. Step 1: repetition number of each RPN value. The data referred to the "Passenger unit" FMECA.

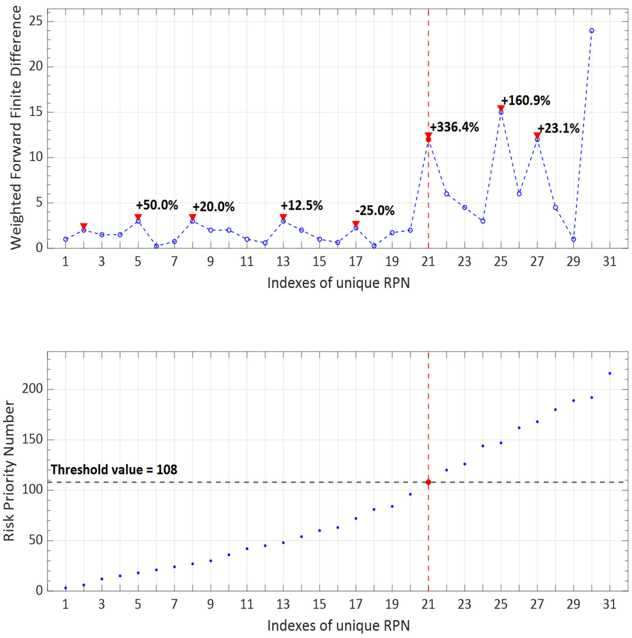

FIGURE 6. Application of the proposed procedure to the "Passenger unit" of the HVAC. The top plot illustrates the steps from 2 to 5 of the procedure, while the bottom plot is used to carry out the final step.

Figure 5 shows the first step of the procedure. The height of the bar represents how the RPN (in the abscissa) is repeated in the FMECA, higher is the bar more frequent is the mode. This plot helps to identify all the unique RPNs and their relative number of repetitions. The value of RPNs unique numbers (the number of bars in fig. 5) is $n = 31$ so the finite difference *Diff* will be composed by 30 elements.

The top plot of fig. 6 illustrates the steps from 2 to 5 of the procedure carried out on the "Passenger unit". The forward finite differences are calculated, and the values are illustrated as blue dots in the top of figure 6. The figure highlights that the first twenty markers are lower than 3, while the 21st value is very different respect to the others. This high value represents a significant difference between the 21st and 22nd unique RPNs, which involves a rapid increase of the subsequent ordered RPN. In the top graph of Fig. 6 the peaks are marked using red triangles, 8 peaks were identified in the "Passenger unit" FMECA.

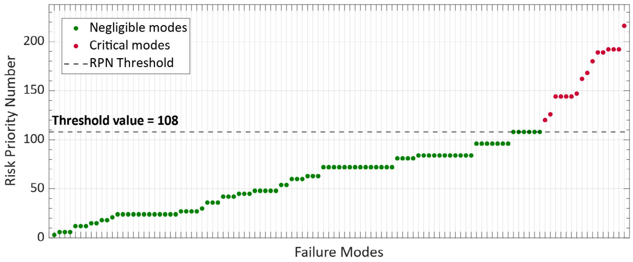

FIGURE 7. Division of risk priority numbers identified in the "Passenger unit" FMECA in negligible and critical values.

Near each peak there is a label indicating the percentage difference $\Delta Peak_i$ between this peak and the three previous peaks. The index of the *"first significant peak"* is the one that corresponds to the maximum value of $\Delta Peak_i$. It is highlighted using a red dotted line, which indicates the index of the unique RPN associated to the threshold level. The final step is illustrated on the bottom plot of fig. 6, which corresponds to the identification of the RPN threshold value. This graph highlights that the corresponding RPN to the 21th index is the value 108, which will be the threshold value.

All the RPNs higher than the threshold have to be considered critical, while all the RPNs lower than or equal to 108 are considered negligible. Figure 7 shows all the values of RPN evaluated for the "Passenger unit" FMECA (the same data of Figure 3) and the threshold line (black dotted line). All the RPNs below the threshold are illustrated using green dots and are considered negligible, while the red dots stand for the RPNs above the threshold which are considered critical.

In the "Passenger unit" FMECA, 16 out of 109 failure modes were found unacceptable. This means that nearly 15% of the failure modes require some sort of corrective action.

C. CASE STUDY 2: "CABIN UNIT" FMECA

This subsection tests the proposed procedure with another set of data coming from the analysis of the cabin unit of the same HVAC. A FMECA has been developed and the resulting RPNs are used as input of the method.

The top plot of figure 8 shows the trends of the forward finite differences (step 2). The peaks are highlighted by red triangles (step 3), and from a qualitative point of view it is possible to note a sudden increase of the difference between the 20th and 21st unique RPN. To quantitative identify the first significant peak, step 4 and 5 are used with this dataset. Clearly the highest variation is the 21st unique RPN with a 408.7% increase.

Then step 6 allows to identify the threshold value associated to the 21st unique RPN, the bottom of figure 8 shows all the unique Risk Priority Numbers and their indexes. The threshold associated to the 21st index is the RPN = 70.

Figure 9 shows all the Risk Priority Numbers as dots and the threshold limit. In this case study the method identifies 12 critical failure modes over 90 total modes. So, in this case the 13% of the modes needs to be mitigated.

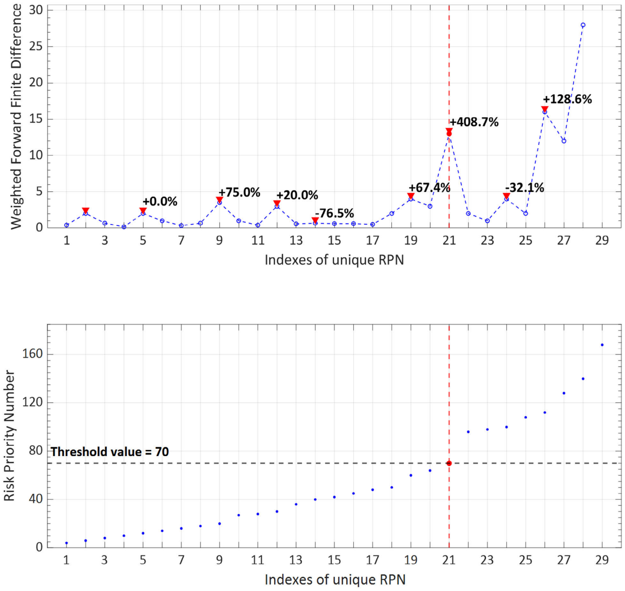

FIGURE 8. Application of the proposed procedure to the "Cabin unit" of the HVAC. The top plot illustrates the steps from 2 to 5 of the procedure, while the bottom plot is used to carry out the final step.

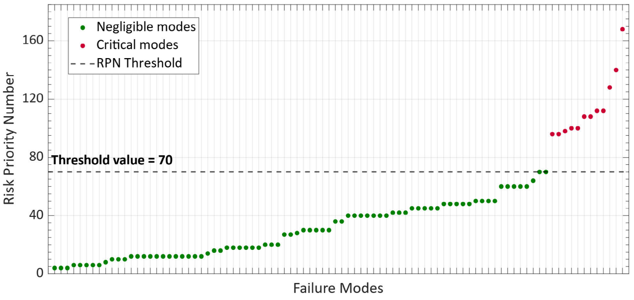

FIGURE 9. Division of risk priority numbers identified in the "Cabin unit" FMECA in negligible and critical values.

D. COMPARISON

Finally, the proposed procedure was compared with the other approaches available in literature. The results achieved for both case studies are summarized in table 6 which includes the RPN threshold value and the number of critical failure modes.

The comparison firstly highlights the inadequacy of Zhao and Pareto approaches for this kind of application.

In both the case studies, the method proposed by Zhao identifies the highest RPN threshold, on the other hand the 80-20 Pareto principle identifies the lowest value.

Such high threshold, given by the Zhao method, could not be reasonable in many safety-related applications, because it requires a risk mitigation only for few modes.

While the low threshold given by the Pareto principle requires an expensive plan for the risk mitigation of the modes, that could be not applicable for many companies.

The proposed method provides intermediate results, in line with the threshold proposed by Bluvband, mostly because both start from the same idea.

TABLE 6. Results comparison achieved using the proposed method and the other method available in literature.

METHOD	Case study 1		Case study 2	
	$\mathrm{RPN_{th}}$	Critical modes	$\mathrm{RPN_{th}}$	Critical modes
Proposed method	**108**	**16**	**70**	**12**
Bluvband [31]	105	22	57	20
Zhao [33]	177	7	124	3
Pareto [34]–[36]	63	60	36	45
Boxplot [37]	96	29	50	24

The main advantage of the proposed approach is that it completely deletes the subjectivity, still present in Bluvband.

Finally, several kinds of risk mitigation actions could be taken into account in order to lower the Risk priority number above the threshold.

A very efficient improvement is to get some changes in the design of the equipment by using components with improved quality and performances, this will lower the failure rate of the component and consequently the occurrence, but it leads to a cost impact for the industry. The use of condition monitoring (sensors which monitor the state of the system) allows to monitor the health state of the system and to diagnose failure before it occurs. So the introduction of these maintenance tools lowers the detection index. Also the use of redundancy system allows to obtain a lower Risk Priority Number, but this solution needs high cost to be performed.

VI. CONCLUSION

This paper shows how a complete risk assessment should be designed for a complex system such as a HVAC system for railway application. HVAC is a system composed by several components both mechanics and electronics; a full and complete study of its risk is mandatory to identify which are the most critical items. Some approaches were proposed in literature to find a threshold value which distinguish critical failure modes to negligible modes after carried out a FMECA procedure. Some of them are not suitable and not efficient while other are only qualitative procedure of the identification of two data sets. To overcome the subjectivity of the establishing a threshold between the acceptability and unacceptability of a risk, a new analytical procedure has been proposed in this paper. The method starts with the aim to identify two different subsets characterized with two different trends: the first subset of RPNs grows gradually and the second has a sudden increase. A weighted forward finite difference is introduced to calculate where is located the variation of the slope, then the *"first significant"* peak of the difference leads to the identification of the threshold value. The strength and effectiveness of the proposed procedure have been tested on two different datasets coming from two different units of the HVAC: "Passenger unit" and "Cabin unit". Finally, the procedure was compared with the other approaches available in literature to highlight the significance of the results.

The proposed approach has proven to be a powerful solution in risk assessment since it uses the idea of the identification of two different subsets allowing to delete the subjectivity issue that influences most of the previous works by means of an analytical procedure based on weighted forward finite differences.

REFERENCES

[1] B. Dhillon, *Transportation Systems Reliability and Safety*. Boca Raton, FL, USA: CRC Press, 2011.

[2] A. Birolini, *Reliability Engineering*. Berlin, Germany: Springer, 2017.

[3] M. Rausand, A. Barros, and A. Høyland, *System Reliability Theory: Models, Statistical Methods, and Applications*, 3rd ed. Hoboken, NJ, USA: Wiley, 2021.

[4] L. Ciani, G. Guidi, G. Patrizi, and M. Venzi, "System maintainability improvement using allocation procedures," in *Proc. IEEE Int. Syst. Eng. Symp. (ISSE)*, Oct. 2018, pp. 1–6.

[5] M. Catelani, L. Ciani, D. Galar, and G. Patrizi, "Optimizing maintenance policies for a yaw system using reliability-centered maintenance and data-driven condition monitoring," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 9, pp. 6241–6249, Sep. 2020.

[6] M. Aliahmadipour, M. Abdolzadeh, and K. Lari, "Air flow simulation of HVAC system in compartment of a passenger coach," *Appl. Thermal Eng.*, vol. 123, pp. 973–990, Aug. 2017.

[7] C. Luger and R. Rieberer, "Multi-objective design optimization of a rail HVAC CO_2 cycle," *Int. J. Refrigeration*, vol. 92, pp. 133–142, Aug. 2018.

[8] *Failure Modes and Effects Analysis*, Standard IEC 60812, International Electrotechnical Commision, 2018.

[9] Y. Deng, Q. Li, and Y. Lu, "A research on subway physical vulnerability based on network theory and FMECA," *Saf. Sci.*, vol. 80, pp. 127–134, Dec. 2015.

[10] M. Giardina and M. Morale, "Safety study of an LNG regasification plant using an FMECA and HAZOP integrated methodology," *J. Loss Prevention Process Ind.*, vol. 35, pp. 35–45, May 2015.

[11] F. Mhenni, N. Nguyen, and J.-Y. Choley, "SafeSysE: A safety analysis integration in systems engineering approach," *IEEE Syst. J.*, vol. 12, no. 1, pp. 161–172, Mar. 2018.

[12] K. O. Kim and M. J. Zuo, "General model for the risk priority number in failure mode and effects analysis," *Rel. Eng. Syst. Saf.*, vol. 169, pp. 321–329, Jan. 2018.

[13] *Procedures for Performing a Failure Mode, Effects, and Criticality Analysis*, Standard MIL-STD-1629A, United States Department of Defense, Washington, DC, USA, 1980.

[14] L. Ciani, G. Guidi, and G. Patrizi, "A critical comparison of alternative risk priority numbers in failure modes, effects, and criticality analysis," *IEEE Access*, vol. 7, pp. 92398–92409, 2019.

[15] A. Pillay and J. Wang, "Modified failure mode and effects analysis using approximate reasoning," *Rel. Eng. Syst. Saf.*, vol. 79, no. 1, pp. 69–85, Jan. 2003.

[16] Y.-M. Niu, Y.-Z. He, J.-H. Li, and X.-J. Zhao, "The optimization of RPN criticality analysis method in FMECA," in *Proc. Int. Conf. Apperceiving Comput. Intell. Anal.*, Oct. 2009, pp. 166–170.

[17] F. Dinmohammadi, B. Alkali, M. Shafiee, C. Bérenguer, and A. Labib, "Risk evaluation of railway rolling stock failures using FMECA technique: A case study of passenger door system," *Urban Rail Transit*, vol. 2, nos. 3–4, pp. 128–145, Dec. 2016.

[18] P. Liu, X. Cheng, Y. Qin, Y. Zhang, and Z. Xing, "Reliability analysis of metro door system based on fuzzy reasoning Petri net," in *Proc. Int. Conf. Electr. Inf. Technol. Rail Transp. (EITRT)*, in Lecture Notes in Electrical Engineering, vol. 288, 2014, pp. 283–291.

[19] J. Kim and H.-Y. Jeong, "Evaluation of the adequacy of maintenance tasks using the failure consequences of railroad vehicles," *Rel. Eng. Syst. Saf.*, vol. 117, pp. 30–39, Sep. 2013.

[20] J. Carretero, J. M. Pérez, F. García-Carballeira, A. Calderón, J. Fernández, J. D. García, A. Lozano, L. Cardona, N. Cotaina, and P. Prete, "Applying RCM in large scale systems: A case study with railway networks," *Rel. Eng. Syst. Saf.*, vol. 82, no. 3, pp. 257–273, Dec. 2003.

[21] F. P. G. Márquez, F. Schmid, and J. C. Collado, "A reliability centered approach to remote condition monitoring. A railway points case study," *Rel. Eng. Syst. Saf.*, vol. 80, no. 1, pp. 33–40, Apr. 2003.

[22] K.-H. Chang, Y.-C. Chang, and P.-T. Lai, "Applying the concept of exponential approach to enhance the assessment capability of FMEA," *J. Intell. Manuf.*, vol. 25, no. 6, pp. 1413–1427, Dec. 2014.

[23] Y. Tang, D. Zhou, and F. T. S. Chan, "AMWRPN: Ambiguity measure weighted risk priority number model for failure mode and effects analysis," *IEEE Access*, vol. 6, pp. 27103–27110, 2018.

[24] S. Carpitella, A. Certa, J. Izquierdo, and C. M. La Fata, "A combined multi-criteria approach to support FMECA analyses: A real-world case," *Rel. Eng. Syst. Saf.*, vol. 169, pp. 394–402, Jan. 2018.

[25] Y. W. Kerk, K. M. Tay, and C. P. Lim, "An analytical interval fuzzy inference system for risk evaluation and prioritization in failure mode and effect analysis," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1589–1600, Sep. 2017.

[26] A. Pandey, M. Singh, A. U. Sonawane, and P. S. Rawat, "FMEA based risk assessment of component failure modes in industrial radiography," *Int. J. Eng. Trends Technol.*, vol. 39, no. 4, pp. 216–225, Sep. 2016.

[27] R. Y. Trianto, M. R. Pahlevi, and B. Z. Bardani, "FMECA development in PLN TRANS-JBTB," in *Proc. Int. Conf. High Voltage Eng. Power Syst. (ICHVEPS)*, Oct. 2017, pp. 567–570.

[28] S. Broggi, M. C. Cantone, A. Chiara, N. D. Muzio, B. Longobardi, P. Mangili, and I. Veronese, "Application of failure mode and effects analysis (FMEA) to pretreatment phases in tomotherapy," *J. Appl. Clin. Med. Phys.*, vol. 14, no. 5, pp. 265–277, Sep. 2013.

[29] A. Jomde, V. Bhojwani, S. Kedia, N. Jangale, K. Kolas, P. Khedkar, and S. Deshmukh, "Failure modes effects and criticality analysis of the linear compressor," *Mater. Today, Proc.*, vol. 4, no. 9, pp. 10184–10188, 2017.

[30] J. Kim, B. Miller, M. S. Siddiqui, B. Movsas, and C. Glide-Hurst, "FMEA of MR-only treatment planning in the pelvis," *Adv. Radiat. Oncol.*, vol. 4, no. 1, pp. 168–176, Jan. 2019.

[31] Z. Bluvband, P. Grabov, and O. Nakar, "Expanded FMEA (EFMEA)," in *Proc. Annu. Symp. Rel. Maintainability (RAMS)*, 2004, pp. 31–36.

[32] Z. Bluvband and P. Grabov, "Failure analysis of FMEA," in *Proc. Annu. Rel. Maintainability Symp.*, Jan. 2009, pp. 344–347.

[33] Y. Zhao, G. Fu, B. Wan, and C. Pei, "An improved cost-based method of risk priority number," in *Proc. IEEE Prognostics Syst. Health Manage. Conf. (PHM- Beijing)*, May 2012, pp. 1–4.

[34] J. B. Bowles, "The new SAE FMECA standard," in *Proc. Annu. Rel. Maintainability Symp. Int. Symp. Product Quality Integr.*, 2002, pp. 48–53.

[35] S. Duicu and A.-E. Dumitrascu, "Researches concerning risk assessing using Pareto diagram for design process of technological processes," in *Proc. 11th WSEAS Int. Conf. Signal Process., Comput. Geometry Artif. Vis.*, 2011, pp. 189–192.

[36] R. Kent, "Design quality management," in *Quality Management in Plastics Processing*. Amsterdam, The Netherlands: Elsevier, 2016, pp. 227–262.

[37] M. Catelani, L. Ciani, D. Galar, and G. Patrizi, "Risk assessment of a wind turbine: A new FMECA-based tool with RPN threshold estimation," *IEEE Access*, vol. 8, pp. 20181–20190, 2020.

[38] S. C. Sugarman, *HVAC Fundamentals*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2007.

[39] *How Does the Air Conditioning Work in a Train?* Alstom, Saint-Ouen, France, 2020.

[40] K. O. Kim and M. J. Zuo, "Optimal allocation of reliability improvement target based on the failure risk and improvement cost," *Rel. Eng. Syst. Saf.*, vol. 180, pp. 104–110, Dec. 2018.

[41] K. O. Kim, Y. Yang, and M. J. Zuo, "A new reliability allocation weight for reducing the occurrence of severe failure effects," *Rel. Eng. Syst. Saf.*, vol. 117, pp. 81–88, Sep. 2013.

[42] L. Tanghong and X. Gang, "Test and improvement of ventilation cooling system for high-speed train," in *Proc. Int. Conf. Optoelectron. Image Process.*, vol. 2, Nov. 2010, pp. 493–497.

[43] C. F. Bonnett, *Practical Railway Engineering*, 2nd ed. London, U.K.: Imperial College Press, 2005.

[44] *Guideline for the Design and Application of Heating, Ventilation and Air Conditioning Equipment for Rail Passenger Vehicles*, Amer. Soc. Heating Refrigerating Air-Conditioning Eng., ASHRAE Guideline 23P, Atlanta, GA, USA, 2014.

[45] *Petroleum, Petrochemical and Natural Gas Industries—Collection and Exchange of Reliability and Maintenance Data for Equipment*, document ISO 14224, International Organization for Standardization, 2016.

MARCANTONIO CATELANI (Member, IEEE) received the M.S. degree in electronic engineering from the University of Florence, Florence, Italy, in 1984. He is currently with the Department of Information Engineering, University of Florence. Strictly correlated with reliability, availability, maintainability, and safety (RAMS) are the fields of interest of both the fault diagnosis and reliability testing for components and equipment. In particular, the research activity concerns the development of test profiles used both for the characterization and the evaluation of reliability performance and the development of new degradation models able to estimate the life cycle of electronic components. His current research interests include development of automatic measurement systems, characterization of A/D converters, quality control and related statistical methods, and RAMS context.

LORENZO CIANI (Senior Member, IEEE) received the M.S. degree in electronic engineering and the Ph.D. degree in industrial and reliability engineering from the University of Florence, Florence, Italy, in 2005 and 2009, respectively. He is currently an Assistant Professor with the Department of Information Engineering, University of Florence. He has authored or coauthored more than 160 peer-reviewed journal articles and conference papers. His current research interests include system reliability, availability, maintainability, and safety, reliability evaluation test and analysis for electronic systems and devices, fault detection and diagnosis, and electrical and electronic instrumentation and measurement. He is a member of the IEEE IMS TC-32 Fault Tolerant Measurement Systems and an Associate Editor of IEEE Access and the IEEE Transaction on Instrumentation and Measurement. He received the 2015 IEEE Instrumentation and Measurement Society Outstanding Young Engineer Award for "his contribution to the advancement of instrumentation and measurement in the field of reliability analysis."

DIEGO GALAR is currently a Professor of condition monitoring with the Division of Operation and Maintenance Engineering, Luleå University of Technology (LTU). In the international arena, he has been a Visiting Professor with the Polytechnic of Braganca, Portugal, the University of Valencia and NIU, USA, and the Universidad Pontificia Católica de Chile. He is also a Visiting Professor with the University of Sunderland, U.K., the University of Maryland, USA, the University of Stavanger, Norway, and Chongqing University, China. He is a principal researcher in Tecnalia, Spain, heading the Maintenance and Reliability Research Group within the Division of Industry and Transport. He was involved with the SKF UTC Center, Lulea, focused on SMART bearings and also actively involved in national projects with the Swedish industry or funded by Swedish national agencies like Vinnova. He has been involved in the raw materials business of Scandinavia, especially with mining and oil & gas for Sweden and Norway, respectively. Indeed, LKAB, Boliden or STATOIL have been partners or funders of projects in the CBM field for specific equipment like loaders, dumpers, and rotating equipment, linear assets. He is coordinating several H2020 projects related to different aspects of cyber physical systems, Industry 4.0, the IoT or Industrial Big Data with LTU. He has authored more than 500 journal articles and conference papers, books, and technical reports in the field of maintenance. He is working as a member of editorial boards, scientific committees, and chairing international journal articles and conference papers and actively participating in national and international committees for standardization and research and development in the topics of reliability and maintenance.

GIULIA GUIDI (Student Member, IEEE) received the B.S. degree in electronic and telecommunications engineering and the M.S. degree in electronics engineering from the University of Florence, Florence, Italy, in 2015 and 2018, respectively, where she is currently pursuing the Ph.D. degree in industrial and reliability engineering.

Her research interests include reliability analysis and optimization of availability and maintainability for railway application.

SERENA MATUCCI received the Laurea degree in mathematics and the Ph.D. degree in mathematical physics from the University of Florence, in 1993 and 1998, respectively.

From 2000 to 2018, she was an Assistant Professor with the Faculty of Engineering, University of Florence, where she is currently an Associated Professor of Mathematical Analysis with the Department of Mathematics and Computer Science. Her current research interests include qualitative theory for ordinary differential equations, difference equations and integral inclusions, and asymptotic analysis of solutions.

GABRIELE PATRIZI (Student Member, IEEE) received the B.S. degree in electronic and telecommunications engineering and the M.S. degree in electronics engineering from the University of Florence, Florence, Italy, in 2015 and 2018, respectively, where he is currently pursuing the Ph.D. degree in industrial and reliability engineering. His research interests include reliability, availability, maintainability, and safety (RAMS) models and experimental analysis for complex systems used in industrial applications.