future internet

MDPI

Article

Failure Mode and Effect Analysis for Cyber-Physical Systems

João Oliveira [1,*], Gonçalo Carvalho [2,*], Bruno Cabral [2] and Jorge Bernardino [1,2]

[1] Instituto Superior de Engenharia de Coimbra (ISEC), Polytechnic Institute of Coimbra, 3030-199 Coimbra, Portugal; jorge@isec.pt

[2] Centre for Informatics and Systems of the University of Coimbra (CISUC), Department of Informatics Engineering, University of Coimbra, 3030-290 Coimbra, Portugal; bcabral@dei.uc.pt

* Correspondence: a21260748@isec.pt (J.O.); gcarvalho@dei.uc.pt (G.C.)

Received: 18 September 2020; Accepted: 18 November 2020; Published: 20 November 2020

Abstract: Cyber-Physical Systems (CPS) are a prominent component of the modern digital transformation, which combines the dynamics of the physical processes with those of software and networks. Critical infrastructures have built-in CPS, and assessing its risk is crucial to avoid significant losses, both economic and social. As CPS are increasingly attached to the world's main industries, these systems' criticality depends not only on software efficiency and availability but also on cyber-security awareness. Given this, and because Failure Mode and Effect Analysis (FMEA) is one of the most effective methods to assess critical infrastructures' risk, in this paper, we show how this method performs in the analysis of CPS threats, also exposing the main drawbacks concerning CPS risk assessment. We first propose a risk prevention analysis to the Communications-Based Train Control (CBTC) system, which involves exploiting cyber vulnerabilities, and we introduce a novel approach to the failure modes' Risk Priority Number (RPN) estimation. We also propose how to adapt the FMEA method to the requirement of CPS risk evaluation. We applied the proposed procedure to the CBTC system use case since it is a CPS with a substantial cyber component and network data transfer.

Keywords: cyber-physical systems; failure mode and effect analysis; risk priority number; communications-based train control

1. Introduction

Most modern engineering systems have close interaction between cyber and physical components, leading to a new paradigm approach named Cyber-Physical Systems (CPS). CPS are networked systems composed of physical and software components integrated through networking, computation, and monitoring. They are usually misidentified for the Internet of Things (IoT) systems, although CPS emphasizes real-time control and monitoring features [1].

With the integration of CPS in critical infrastructures, the risk assessment of those systems requires important cautions to avoid social, environmental, and economic costs. Various authors deal with this issue, for example, Lyu et al. [1] reviewed different methods for CPS risk assessment considering safety and security concerns. Wu et al. [2] proposed a new risk assessment method based on real-time risk calculation considering CPS run-time conditions. Amin et al. [3] suggested a game-theoretic framework for CPS security risks assessment and systems' failures defense. CPS risk is often addressed with risk assessment methods without a risk prevention step. Regarding this concern, and that most Communications-Based Train Control (CBTC) security problems arise from cyber-attacks' effects, we will analyze CBTC from a risk prevention perspective.

Failure Mode and Effect Analysis (FMEA) is an engineering method designed to define, identify, and present solutions for system failures, problems, or errors. FMEA identifies necessary decisions to prevent individual system failures [4], and establish the risk priorities of failure modes through the Risk Priority Number (RPN) [5]. To quantify each failure mode's risk, this method takes into consideration the severity, occurrence, and detectability of each failure mode. Each one of these parameters is estimated in predefined categories. Then, calculating the RPN to prioritize the identified vulnerabilities, through the product of the three parameters mentioned previously. Even though FMEA is a renowned risk assessment method, its methodology presents various drawbacks, mostly when considering CPS risk assessment requirements. For example, FMEA's has a critical dependence on the study team evaluation experience, only covers single failures, and by not weighting the parameters under analysis, and it does not consider the influence of each parameter. Finally, the RPN formula is not focused on the economic impact of the systems' failures. Further ahead, these RPN limitations will be properly exposed and explained.

In this paper, we first demonstrate how the FMEA method behaves in assessing the CBTC system's risk. As the FMEA includes no risk prevention step in its methodology, we introduce a risk prevention analysis for software faults prevention. Regarding FMEA risk score calculation method, we propose an innovative RPN calculation, taking into consideration the failure modes' economic impact, which is calculated by estimating social, infrastructure, delay, and environmental costs.

The main contributions of this work are the following:

- Provide a CBTC risk prevention analysis.
- Propose a novel approach to the FMEA's RPN estimation, concerning CPSs' risk analysis importance.
- Provide a CBTC risk analysis through our version of the FMEA RPN calculation.

The rest of this paper is organized as follows: In Section 2, we provide the state-of-the-art review on CPS risk assessment. In Section 3, we explain FMEA, and propose an extension in Section 4. Next, in Section 5, we introduce the CBTC, describing its main components, and performing a risk prevention analysis to the CBTC system, regarding current approaches. In Section 6, we perform the FMEA risk analysis to the CBTC system. Finally, in Section 7, we conclude our paper and propose future work.

2. Related Work

In this section, a collection of works that addressed CPS risk assessment and RPN estimation improvements are presented chronologically and briefly described.

2.1. CPS Risk Assessment

Xie et al. [6] proposed a risk assessment for CPS using attack trees, assigning values to threats according to different levels. After obtaining a threat vector and a vulnerability vector, the risk value can be calculated for each attack tree path. However, the authors did not take risk prevention into consideration, neither specified the damage classification criteria. Ruckin et al. [7], tackled the security of CPS available in self-driving cars equipped with sensors for braking functionality. Through three different perspectives, FMEA analysis, sensor trustworthiness analysis, and control safety analysis, the authors aimed to exploit inter-domain vulnerabilities by specifying and verifying contained assumptions and dependencies between analyses. Wu et al. [2] introduced a novel method to assess the risk based on real-time risk calculation considering CPS run-time conditions. After gathering information of cyber-attacks and system's vulnerabilities, this data was used as an input to calculate attack severity, success probability, and consequences for each system's affected node. With these results, and the consequent design of a risk change curve, users get a better insight into the system's real-time risk and can take on time actions accordingly. While a risk change curve allows users to prevent risk, no risk prevention is taken into account throughout the paper. Ali et al. [8], addressed CPS failure detection and prevention. Their approach was through a derivation of FMEA which also

incorporates a Criticality analysis (Failure Mode Effects and Criticality Analysis—FMECA). The author proposed a new framework, based on an ontology, to detect and prevent failure by using a knowledge base on a Unified Modeling Language (UML) class diagram. Lyu et al. [1] addressed different methods for risk assessment considering safety and security concerns, establishing an advanced collective of risk assessment and management methods aiming at CPS and its safety and security integration. While it is a foremost contribution for the state-of-art of CPS risk assessment methods, the authors did not apply the method to an illustrative use case.

2.2. RPN Estimation Improvement

FMEA's traditional RPN has been heavily criticized for its calculation formula and its generic parameters. Over the past decade, several studies aimed at improving RPN calculation.

Tay et al. [9] applied fuzzy logic to FMEA aiming to diminish the number of rules needed for the RPN. The authors used a Guided Rules Reduction System (GRRS) where the user only had to provide the most relevant rules to the fuzzy RPN model. The authors' approach was assessed through real-world scenarios, and the results state its effectiveness in reducing the number of rules while maintaining the capability of predicting failure modes. Wang et al. [5] introduced a new RPN which encompassed the fuzzy nature of the risk factor and their corresponding weights, to prioritize the failure modes. According to the authors, their approach is more realistic, practical, and flexible than the original RPN calculation. Moreover, by presenting a linguistic evaluation, the assessment is easier rather than numerical values. Finally, they combined the three parameters of FMEA aiming to provide a clear differentiation amongst them and arrange the failure modes. Liu et al. [10], addressed the representation of uncertain information, labeled D numbers, through Grey Relation Projection (GRP) to assess the RPN of failure modes. The D numbers tackle the subjective nature of FMEA. By presenting an illustrative example, the authors state that their approach surpasses any drawback of the original RPN, thus granting their framework increased value.

Wu et al. [11] proposed an improvement to FMEA by adding cost, casualty, downtime, probability of occurrence, and detectability factors to the RPN calculation. Each factor value is obtained by comparing the failure mode with the worst situation in the affected area, contrary to the usual rank assignment by experts. To reduce the drawbacks of traditional RPN calculation, Kabak et al. [12] suggested the use of Multi-Criteria Decision Making (MCDM) in the prioritization of failure modes. The authors aimed to accomplish fitter results in prioritizing failure modes by using an Analytic Hierarchy Process (AHP) and a Preference Ranking Organization Method for Enrichment Evaluation (PROMETHEE) method. The authors prioritized the failure modes through an AHP scale and estimated the weight of each failure mode by applying the AHP to the outcome of the decision matrix. Moreover, the authors multiplied the weights of the failure modes by the RPN equivalents of the failure modes to determine AHP-RPN values which, in turn, was used to sort the failure modes. Finally, the authors concluded that compared to the other methods under scrutiny, the PROMETHEE method was more accurate to prioritize failure modes in FMEA.

Rezaei et al. [13] adapted FMEA's RPN equivalent to the needs of health-care systems. New weights, scales, and coefficients were defined, considering patients and treatment data, for severity, occurrence, and detectability parameters. The authors concluded that FMEA's standard parameters and categorization should be adapted with technical knowledge. Carpitella et al. [14], merged reliability analyses, and MCDM in maintenance services optimization. The authors started with a FMECA analysis and implemented a fuzzy logic method to rank the previously obtained failure modes. To further develop the RPN calculation, the authors also used AHP to assess their weight criteria to the parameters, which was evaluated through a sensitivity analysis. Following the shortcomings of the original RPN calculation, Ciani et al. [15] analyzed and compared some alternative methods within FMECA. The authors state that alternative RPN calculation formulas may be used depending on the type of application, and further provide recommendations and suggestions for such considerations. The authors used a scale reduction for the original parameters of the RPN, however,

did not introduce additional factors to the formula. Contrary to the previously described works, we not only propose different parameters and formulas to FMEA's RPN estimation, but also use this approach to perform a risk analysis to the CBTC system.

3. Failure Mode and Effect Analysis

FMEA is an engineering method designed to identify potential failure modes and its failure causes, assessing the effects these have within a given system. A failure mode is usually defined as a fluctuation inside the performance criteria for the component (inability to perform the design functions). The FMEA method identifies the decisions necessary to prevent individual system failures [4]. Nevertheless, FMEA has some associated problems, which Spreafico et al. [16] expose comprehensively, from which we gathered, among others, subjectivity, time consumption, staff level, too expensive, and late application. The authors also classified the FMEA's problems into four main classes (Applicability, Cause and effects representation, Risk analysis, and Problem-solving) and 18 different subproblems. Additionally, regarding FMEA's solutions/improvements they used the same four categories and 19 types of solutions.

FMEA's risk assessment procedure can be divided into five fundamental steps: System subdivision, failure modes identification, RPN calculation, prevention actions recording, and analysis reporting. The first step consists of system subdivision, in which the system is broken down into subsystems, with a complete list of components. In the second step, it is necessary to identify failure modes, its causes for each component, and determining the consequences for each. Subsequently, the third step is to assess the risk, considering Severity, Occurrence, and Detection of each failure mode. Where Severity is the reckoning of the severity of the potential failure, Occurrence is a numerical subjective assessment of the probability for each cause of failure, and Detection is the performance of detecting the failure before failure occurrence [8]. This assessment is usually represented as a cost caused by failures represented as probabilities [17]. Each one of these parameters is recorded and estimated in predefined categories. Then, calculating the RPN to prioritize the identified vulnerabilities, through the product of Severity, Occurrence, and Detection values. The fourth step consists of recording actions to prevent serious consequences, correct failures, and to restore system functions. Finally, the fifth, and last, step is to report the analysis, summarizing the FMEA process, and its results. The FMEA method is universally used and easy to understand the method, mainly because it applies to complex systems, and efficient for identifying all technical failure modes.

Table 1 represents the FMEA risk factors, evaluated through a 10-point scale [12]. Wang et al. [5] provided the crisp ratings for each parameter with a thorough description, thus we refer to this paper for a more in-depth analysis of the scale of each parameter.

Table 1. Failure Mode and Effect Analysis (FMEA) parameters for the Risk Priority Number (RPN) calculation Variables.

Occurrence	1	2	3	4	5	6	7	8	9	10
(O)	Nearly Impossible									Failure Almost Inevitable
Severity	1	2	3	4	5	6	7	8	9	10
(S)	No Effect									Hazardous Effect
Detectability	1	2	3	4	5	6	7	8	9	10
(D)	Almost Certain									Absolute Uncertainty

However, the FMEA's result outcome heavily depends on the study team experience, given the fact that the RPN parameters and its values are categorized by them. Moreover, FMEA only considers vulnerabilities that emerged from single failures, failing to identify vulnerabilities originated by combinations of failures. From a structural point of view, FMEA's classical RPN formula for risk index calculation has several drawbacks, such as the existence of gaps in the range of admissible values,

duplicated values resulting from different combinations of the base factors, and the high sensitivity to minor changes [15]. Because this formula has no parameter weighting on its multiplication, the different relevance of each parameter is not considered. This means that RPN values cannot be compared linearly [15]. For example, a failure mode with 10, 1, and 1 values assigned to the Severity, Occurrence, and Detection parameters respectively, results in the precisely same RPN equivalent as a second failure mode with 1, 2, and 5 values assigned to the same parameters. Moreover, Occurrence, Severity, and Detection are difficult to quantify accurately quantify because the categories of RPN values low, moderate, and high, despite the subjectivity of the categories associated with the user [15]. Moreover, when calculating the risk value from an economic point of view, detectability and occurrence parameters become ineffective to the desired purpose. These two parameters are used to evaluate the rate of detectability and the number of occurrences of the failure modes. Still, these are ignored in the economic impact because they represent information not needed to the cost of each failure mode.

As a result of these limitations, we further suggest modifications to the RPN formula and parameters, based on an economic perspective of railway risks, considering our approach to calculate risk indexes. Our proposed RPN categorization was mainly designed for railway CPS systems although it can be adapted to other use cases. We consider potential social, infrastructure, environmental, and delay costs resultant from CBTC railway signaling system failure modes. Through different procedures, we also estimate the economic impact of such costs. In the next section, we present our newly RPN criteria and estimation formula.

4. New RPN Criteria and Formula

In this section, we propose a new approach to FMEA's RPN calculation. Our goal is to assess the risk of different system failure modes based on the economic impact they represent. For our approach, we consider social, infrastructural, environmental, and delay costs. Our social parameters are fatalities (F), serious injuries (SI), and light injuries (LI). The average cost to each one of this type of injuries is 803,000 €, 107,400 €, and 7400 €, respectively. To obtain an estimated cost for each of these types of injuries, we used the Portuguese Value of Preventing a Casualty (VPC) [18], which is the value of preventing fatalities and significant damage (serious and slight injuries). The total cost (C) results from adding all the representative costs of each rank. Table 2 shows that our social costs ranged from 1 to 10, where 1 corresponds to Low and 10 to Catastrophic.

Regarding infrastructure costs, we considered railway track and bogie damage, derailments, Access Point (AP) destruction, and collisions between trains. The ranges of estimated values for each rank are based on reports of railway accidents made available by the Portuguese "Aircraft Accident and Railway Accident Prevention and Investigation Office" (GPIAAF) [19]. Concerning track damage, 1000 or fewer meters of damaged railway track represent low damage and more than 1000 m severe damage. Table 3 shows that our infrastructural costs ranged from 1 to 10 where 1 corresponds to Low and 10 to Catastrophic.

Table 2. Evaluation criteria to assess social impact.

Level	Description	Criteria
1	Low	Reduced number of light injuries $1 \leqslant LI \leqslant 10$ 7400 € $\leqslant C \leqslant$ 74,000 €
2	Low	Moderate number of light injuries $10 < LI \leqslant 30$ 81,400 € $< C \leqslant$ 222,000 €
3	Low	High number of light injuries $LI > 30$ $C >$ 222,000 €

Table 2. *Cont.*

Level	Description	Criteria
4	Moderate	High number of light injuries Reduced number of serious injuries LI $\geqslant$ 30 1 $\leqslant$ SI $\leqslant$ 10 773,400 € $\leqslant$ C $\leqslant$ 1,203,000 €
5	Moderate	High number of light injuries Moderate number of serious injuries LI > 30 10 < SI $\leqslant$ 30 1,203,000 € $\leqslant$ C $\leqslant$ 3,331,000 €
6	Moderate	High number of light injuries and serious injuries LI > 30 SI > 30 C > 3,444,000 €
7	High	Reduced number of serious injuries and fatalities 1 $\leqslant$ SI $\leqslant$ 10 1 $\leqslant$ F $\leqslant$ 10 910,000 € $\leqslant$ C $\leqslant$ 11,252,000 €
8	High	Moderate number of serious injuries and fatalities 10 < SI $\leqslant$ 30 10 $\leqslant$ F $\leqslant$ 30 8,137,400 € $\leqslant$ C $\leqslant$ 27,312,000 €
9	Catastrophic	High number of fatalities F > 30 C > 24,090,000 €
10	Catastrophic	High number of serious injuries and fatalities SI > 30 F > 30 C > 27,312,000 €

Regarding delay costs, the agreed statistical cost formula associated with delays due to the accident, available in "IMT—Calculation of Common Safety Indicators" [18], is used to calculate the economic impact of delays. To a period of 12 h interruption of the railway track the associated average cost is 25,000 €. The total cost (C) results of adding all the hours of railway track inactivity and converting the sum to currency units. Table 4 shows our delay costs ranged from 1 to 10 where 1 corresponds to Low and 10 to Very High.

Table 3. Evaluation criteria to assess infrastructure impact.

Level	Description	Criteria
1	Low	Low damage to the railway track ($\leqslant$ 1000 m) 0 < C $\leqslant$ 250,000 €
2	Low	Low damage to 1 or more bogies 250,000 € < C $\leqslant$ 500,000 €
3	Low	Low damage to the railway track and 1 or more bogies 500,000 € < C $\leqslant$ 750,000 €
4	Moderate	1 or more bogies derailment 750,000 € < C $\leqslant$ 1,250,000 €
5	Moderate	1 or more bogies derailment and access points destruction 1 250,000 € < C $\leqslant$ 1,750,000 €
6	Moderate	Serious damage to the railway track (> 1000 m) 1 or more bogies derailment and access points destruction 750,000 € < C $\leqslant$ 2,250,000 €

Table 3. *Cont.*

Level	Description	Criteria
7	High	2 trains collision 2,250,000 € < C ⩽ 3,250,000 €
8	High	2 trains collision and access points destruction 3,250,000 € < C ⩽ 4,250,000 €
9	Catastrophic	2 trains collision, access points destruction and severe damage to the railway track 4,250,000 € < C ⩽ 6,250,000 €
10	Catastrophic	2 trains collision, 1 or more bogies derailment, access points destruction and serious damage to the railway track C > 6,250,000 €

Table 4. Evaluation criteria to assess delay impact.

Level	Description	Criteria
1	Low	C ⩽ 25,000 € (± 12 h)
2	Low	25,000 € < C ⩽ 50,000 €
3	Low	50,000 € < C ⩽ 75,000 €
4	Moderate	75,000 € < C ⩽ 100,000 €
5	Moderate	100,000 € < C ⩽ 125,000 €
6	Moderate	125,000 € < C ⩽ 150,000 €
7	High	150,000 € < C ⩽ 175,000 €
8	High	175,000 € < C ⩽ 200,000 €
9	Very High	200,000 € < C ⩽ 225,000 €
10	Very High	C > 225,000 €

Table 5 displays the environmental costs where we considered carbon dioxide (CO_2) emissions from fires. Our parameterization is based on the Sustainable Structural Design Methodology (SSD) formula RSSD (CO_2) = $PCO_2 \times QCO_2$, where RSSD (CO_2) is the result of the financial value of environmental impacts, PCO_2 is the carbon price of a ton of CO_2 emissions in euro/ton and QCO_2 is the total CO_2 equivalent emissions developed from the Life Cycle Assessment (LCA) analysis, declared in tons [20]. To calculate the total cost, we used the 2019 OCDE CO_2 emission tax for Portugal [21], which is 25 €/ tonne (t) CO_2 and the formula already mentioned. Table 5 shows our categorization for environmental costs, classified from 1 to 10, where 1 corresponds to Low and 10 to Catastrophic. While we used Portuguese data to develop our RPN criteria, it can apply to railway systems in other countries or even to other systems. However, for this purpose, our categorization will have to be adapted to the country's socio-economic context or the system's requirements.

To a final risk estimation, we propose five different categories. Table 6 shows our 10 ranks distributed through these five categories: Very low, low, moderate, high, and catastrophic.

Considering the RPN calculation formula and its limitations already referenced above, we also propose a weight-oriented formula for calculating RPN ranks. Instead of the traditional multiplication based formula, we suggest a sum-based formula, of weighted variables Social Factor (SF), Infrastructure Factor (IF), Environmental Factor (EF), and Delay Factor (DF). Moreover, we imposed the weights' sum to be equal to 1, following the same criteria of easy analysis. The amount of variation, amongst the possible values of the parameters we considered in this process, was very high, having four variables ranging from 1 to 10 and with associated weights ranging between 0.01 and 0.99. We trimmed the possibilities by determining the parameters' weight according to the parameter's economic impact, which allows a straightforward and easy comparison. The social factor has a vital concern for human

health, thus we decided its weight to be half of the sum of the values of the overall weights, because human life is still more valuable than any other consequence. Nevertheless, this decision only curtails some of the possibilities that arise to 1,176,490,000, as a result of four variables between 1 and 10, and three weights that could range from 0.01 and 0.49 ($10 \times 10 \times 10 \times 10 \times 49 \times 49 \times 49$).

Table 5. Evaluation criteria to assess environmental impact.

Level	Description	Criteria
1	Low	$0 < QCO_2 \leqslant 500$ tCO_2 $0 <$ RSSD(CO_2) $\leqslant$ 12,500 €
2	Low	$500 < QCO_2 \leqslant 1000$ tCO_2 12,500 < RSSD(CO_2) $\leqslant$ 25,000 €
3	Low	$1000 < QCO_2 \leqslant 1500$ tCO_2 25,000 < RSSD(CO_2) $\leqslant$ 37,500 €
4	Moderate	$1500 < QCO_2 \leqslant 2000$ tCO_2 37,500 < RSSD(CO_2) $\leqslant$ 50,000 €
5	Moderate	$2000 < QCO_2 \leqslant 2500$ tCO_2 50,000 < RSSD(CO_2) $\leqslant$ 62,500 €
6	Moderate	$2500 < QCO_2 \leqslant 3000$ tCO_2 62,500 < RSSD(CO_2) $\leqslant$ 65,000 €
7	High	$3000 < QCO_2 \leqslant 3500$ tCO_2 65,000 < RSSD(CO_2) $\leqslant$ 67,500 €
8	High	$3500 < QCO_2 \leqslant 4000$ tCO_2 67,500 < RSSD(CO_2) $\leqslant$ 70,000 €
9	Very High	$4000 < QCO_2 \leqslant 4500$ tCO_2 70,000 < RSSD(CO_2) $\leqslant$ 72,500 €
10	Very High	$QCO_2 > 4500$ tCO_2 RSSD(CO_2) > 72,500 €

Table 6. RPN Categories

Category	RPN
Very Low	[1–2]
Low	[2–4]
Moderate	[4–6]
High	[6–8]
Catastrophic	[8–10]

Notwithstanding the associated subjectiveness, we also decided to give a higher weight value to the infrastructure factor due to the fact of the associated cost, translated in economic impact, of fixing tracks or bogies, among others. The remaining two variables have a similar economic impact, however, we decided to give more importance to the delay factor by the result an interruption has, compared to the CO_2 emissions. Equation (1) is the result of our assessment of the weights for each variable, representing the new RPN calculation method that we are proposing in this paper.

$$RPN = SF \times 0.5 + IF \times 0.35 + EF \times 0.05 + DF \times 0.1 \quad (1)$$

Table 7 is a small representation of a series of tests in which we kept changing the weight values that we assigned to the parameters. Within the provided examples, we display only high social impact, medium to high infrastructure impact, and low to medium environmental and delay risks, which we gathered amongst a table with all possible combinations of values and three examples of weight values

to the four variables. In Example 1, we used the weights that we considered to be the fittest for our use case. In Example 2, we subtracted some of the weight of the infrastructure variable and increased the environmental and delay variables. In Example 3, we added even more weight to the infrastructure variable and matched the weight of the two remaining variables. The RPN values do not change considerably amongst the samples we provide in this paper, notwithstanding, for an easier comparison, we provide, in Table 8 a comparison of three random sets of values, not only between the original RPN calculations but also amongst the different assessed weights for the four variables.

In Table 9 we performed a statistical evaluation of the samples provided in Table 7. We assessed three metrics, average, variance, and standard deviation for the original RPN and our three examples of weights variations, which lead us to add a fourth example ("Ex 4") as the average, variance, and standard deviation of the three previous examples regarding the values of our approach. Thus, we concluded that the weights we choose to use within this paper have a realistic representation of data since the average between the examples is 6.50 which is very close to the average value with our proposed weights, displayed in Example 1, and the standard deviation among all three is only 0.02.

We draw two main conclusions. First, the original RPN has values that correspond to 1.12% (112), 4.05% (405), and 11.2% (1120) of the available scale, meaning that even with high-risk values, the risk failure assessment would still be considered very low. Second, the changes in the weights for the other parameters rather than the social factor, lead to insignificant fluctuations. Allowing us to state that the values we assessed and display in Equation (1) expose the results of our tests, driving us to the conclusion that these values are fit to represent the economic impact we are evaluating. Next, we proceed to a brief description of the CBTC system functioning and its components.

Table 7. Example of some results obtained when testing the weight values.

Original RPN					Our Approach													
					Example 1					Example 2					Example 3				
Social	Infra Structure	Environ Mental	Delay	RPN	Social 0.5	Infrastr 0.35	Environ 0.05	Delay 0.1	RPN	Social 0.5	Infrastr 0.25	Environ 0.1	Delay 0.15	RPN	Social 0.5	Infrastr 0.4	Environ 0.05	Delay 0.05	RPN
7	4	1	1	28	7	4	1	1	5.05	7	4	1	1	4.75	7	4	1	1	5.2
7	4	2	2	112	7	4	2	2	5.2	7	4	2	2	5	7	4	2	2	5.3
7	4	3	3	252	7	4	3	3	5.35	7	4	3	3	5.25	7	4	3	3	5.4
7	4	4	4	448	7	4	4	4	5.5	7	4	4	4	5.5	7	4	4	4	5.5
7	5	1	1	35	7	5	1	1	5.4	7	5	1	1	5	7	5	1	1	5.6
7	5	2	2	140	7	5	2	2	5.55	7	5	2	2	5.25	7	5	2	2	5.7
7	5	3	3	315	7	5	3	3	5.7	7	5	3	3	5.5	7	5	3	3	5.8
7	5	4	4	560	7	5	4	4	5.85	7	5	4	4	5.75	7	5	4	4	5.9
7	6	1	1	42	7	6	1	1	5.75	7	6	1	1	5.25	7	6	1	1	6
7	6	2	2	168	7	6	2	2	5.9	7	6	2	2	5.5	7	6	2	2	6.1
7	6	3	3	378	7	6	3	3	6.05	7	6	3	3	5.75	7	6	3	3	6.2
7	6	4	4	672	7	6	4	4	6.2	7	6	4	4	6	7	6	4	4	6.3
7	7	1	1	49	7	7	1	1	6.1	7	7	1	1	5.5	7	7	1	1	6.4
7	7	2	2	196	7	7	2	2	6.25	7	7	2	2	5.75	7	7	2	2	6.5
7	7	3	3	441	7	7	3	3	6.4	7	7	3	3	6	7	7	3	3	6.6
7	7	4	4	784	7	7	4	4	6.55	7	7	4	4	6.25	7	7	4	4	6.7
8	4	1	1	32	8	4	1	1	5.55	8	4	1	1	5.25	8	4	1	1	5.7
8	4	2	2	128	8	4	2	2	5.7	8	4	2	2	5.5	8	4	2	2	5.8
8	4	3	3	288	8	4	3	3	5.85	8	4	3	3	5.75	8	4	3	3	5.9
8	4	4	4	512	8	4	4	4	6	8	4	4	4	6	8	4	4	4	6
8	5	1	1	40	8	5	1	1	5.9	8	5	1	1	5.5	8	5	1	1	6.1
8	5	2	2	160	8	5	2	2	6.05	8	5	2	2	5.75	8	5	2	2	6.2
8	5	3	3	360	8	5	3	3	6.2	8	5	3	3	6	8	5	3	3	6.3
8	5	4	4	640	8	5	4	4	6.35	8	5	4	4	6.25	8	5	4	4	6.4
8	6	1	1	48	8	6	1	1	6.25	8	6	1	1	5.75	8	6	1	1	6.5
8	6	2	2	192	8	6	2	2	6.4	8	6	2	2	6	8	6	2	2	6.6
8	6	3	3	432	8	6	3	3	6.55	8	6	3	3	6.25	8	6	3	3	6.7
8	6	4	4	768	8	6	4	4	6.7	8	6	4	4	6.5	8	6	4	4	6.8
8	7	1	1	56	8	7	1	1	6.6	8	7	1	1	6	8	7	1	1	6.9
8	7	2	2	224	8	7	2	2	6.75	8	7	2	2	6.25	8	7	2	2	7
8	7	3	3	504	8	7	3	3	6.9	8	7	3	3	6.5	8	7	3	3	7.1
8	7	4	4	896	8	7	4	4	7.05	8	7	4	4	6.75	8	7	4	4	7.2
9	4	1	1	36	9	4	1	1	6.05	9	4	1	1	5.75	9	4	1	1	6.2
9	4	2	2	144	9	4	2	2	6.2	9	4	2	2	6	9	4	2	2	6.3
9	4	3	3	324	9	4	3	3	6.35	9	4	3	3	6.25	9	4	3	3	6.4
9	4	4	4	576	9	4	4	4	6.5	9	4	4	4	6.5	9	4	4	4	6.5
9	5	1	1	45	9	5	1	1	6.4	9	5	1	1	6	9	5	1	1	6.6
9	5	2	2	180	9	5	2	2	6.55	9	5	2	2	6.25	9	5	2	2	6.7
9	5	3	3	405	9	5	3	3	6.7	9	5	3	3	6.5	9	5	3	3	6.8

Table 7. *Cont.*

Original RPN					Our Approach															
					Example 1					Example 2					Example 3				
Social	Infra Structure	Environ Mental	Delay	RPN	Social 0.5	Infrastr 0.35	Environ 0.05	Delay 0.1	RPN	Social 0.5	Infrastr 0.25	Environ 0.1	Delay 0.15	RPN	Social 0.5	Infrastr 0.4	Environ 0.05	Delay 0.05	RPN
9	5	4	4	720	9	5	4	4	6.85	9	5	4	4	6.75	9	5	4	4	6.9
9	6	1	1	54	9	6	1	1	6.75	9	6	1	1	6.25	9	6	1	1	7
9	6	2	2	216	9	6	2	2	6.9	9	6	2	2	6.5	9	6	2	2	7.1
9	6	3	3	486	9	6	3	3	7.05	9	6	3	3	6.75	9	6	3	3	7.2
9	6	4	4	864	9	6	4	4	7.2	9	6	4	4	7	9	6	4	4	7.3
9	7	1	1	63	9	7	1	1	7.1	9	7	1	1	6.5	9	7	1	1	7.4
9	7	2	2	252	9	7	2	2	7.25	9	7	2	2	6.75	9	7	2	2	7.5
9	7	3	3	567	9	7	3	3	7.4	9	7	3	3	7	9	7	3	3	7.6
9	7	4	4	1008	9	7	4	4	7.55	9	7	4	4	7.25	9	7	4	4	7.7
10	4	1	1	40	10	4	1	1	6.55	10	4	1	1	6.25	10	4	1	1	6.7
10	4	2	2	160	10	4	2	2	6.7	10	4	2	2	6.5	10	4	2	2	6.8
10	4	3	3	360	10	4	3	3	6.85	10	4	3	3	6.75	10	4	3	3	6.9
10	4	4	4	640	10	4	4	4	7	10	4	4	4	7	10	4	4	4	7
10	5	1	1	50	10	5	1	1	6.9	10	5	1	1	6.5	10	5	1	1	7.1
10	5	2	2	200	10	5	2	2	7.05	10	5	2	2	6.75	10	5	2	2	7.2
10	5	3	3	450	10	5	3	3	7.2	10	5	3	3	7	10	5	3	3	7.3
10	5	4	4	800	10	5	4	4	7.35	10	5	4	4	7.25	10	5	4	4	7.4
10	6	1	1	60	10	6	1	1	7.25	10	6	1	1	6.75	10	6	1	1	7.5
10	6	2	2	240	10	6	2	2	7.4	10	6	2	2	7	10	6	2	2	7.6
10	6	3	3	540	10	6	3	3	7.55	10	6	3	3	7.25	10	6	3	3	7.7
10	6	4	4	960	10	6	4	4	7.7	10	6	4	4	7.5	10	6	4	4	7.8
10	7	1	1	70	10	7	1	1	7.6	10	7	1	1	7	10	7	1	1	7.9
10	7	2	2	280	10	7	2	2	7.75	10	7	2	2	7.25	10	7	2	2	8
10	7	3	3	630	10	7	3	3	7.9	10	7	3	3	7.5	10	7	3	3	8.1
10	7	4	4	1120	10	7	4	4	8.05	10	7	4	4	7.75	10	7	4	4	8.2

Table 8. Example of three results.

Original RPN					Our Approach															
					Example 1					Example 2					Example 3				
Social	Infra Structure	Environ Mental	Delay	RPN	Social 0.5	Infrastr 0.35	Environ 0.05	Delay 0.1	RPN	Social 0.5	Infrastr 0.25	Environ 0.1	Delay 0.15	RPN	Social 0.5	Infrastr 0.4	Environ 0.05	Delay 0.05	RPN
7	4	2	2	112	7	4	2	2	5.2	7	4	2	2	5	7	4	2	2	5.3
9	5	3	3	405	9	5	3	3	6.7	9	5	3	3	6.5	9	5	3	3	6.8
10	7	4	4	1120	10	7	4	4	8.05	10	7	4	4	7.75	10	7	4	4	8.2

Table 9. Statistical evaluation of the sample.

	RPN				
	Original	**Ex. 1**	**Ex. 2**	**Ex. 3**	**Ex. 4**
Average	350.625	6.55	6.25	6.70	6.50
Variance	81,961.7	0.494	0.4688	0.525	0.0008
Standard Deviation	288.553	0.708	0.6901	0.7303	0.02

5. Communications-Based Train Control

CBTC is a modern communication-based system that uses radio communication to exchange train control information between trains and wayside equipment. Xu et al. [22] provided a complex CBTC system architecture which we compacted into Figure 1. Onboard the train the Automatic Train Control (ATC) functions, namely Automatic Train Protection (ATP) and Automatic Train Operation (ATO) actuate in consideration of the exchanged information between the train and the wayside devices. The train continuously sends traveling data, such as location and traveling speed, to the wayside equipment over a Wi-Fi connection. With this information, the limit of movement authority (LMA), which consists of the limit of speed and distance the train is permitted to travel, is calculated on the wayside's traffic control center and sent back to the train [23]. Based on this information, the train onboard ATC equipment continuously keeps the safety distance to any preceding trains adjusting the train speed. We chose CBTC as a use case for our CPS risk assessment study because, besides being a safety and time-critical system, the CBTC system is highly dependable on-network data transfer and software availability. Moreover, the social and economic impact of CBTC software faults may be catastrophic, as train collisions and fatalities emerge as the worst consequences.

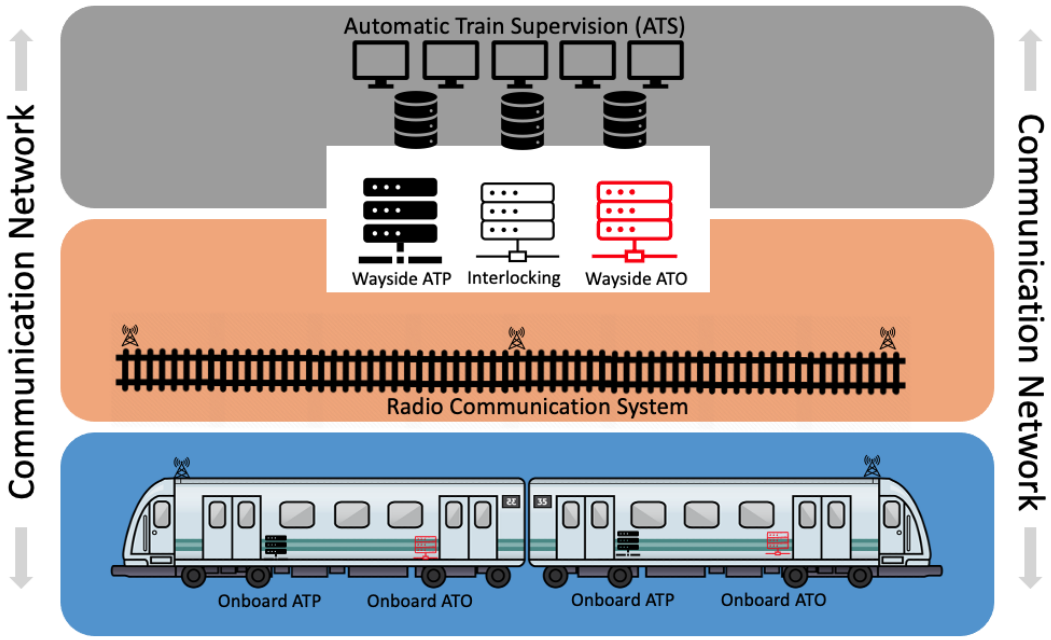

Figure 1. Communications-Based Train Control (CBTC) system architecture.

Further ahead, we succinctly describe the most essential components of a CBTC system, as well as the networked communication between the train and the wayside devices. This network consists of the following three integrated networks: Train onboard network, trackside backbone network, and train-to-trackside network. The first two networks communicate through Ethernet, while the last one generally uses Wi-Fi [24].

Following, we will disciss the major onboard components of a CBTC system: The Vehicle Onboard Computer (VOBC), the onboard ATC, and the Radio Communication System (RCS). Together, these components represent the train onboard network. VOBC is the system responsible for consistently sending train control information to the wayside. This system either includes, or works together with, the onboard ATP, and ATO subsystems of the ATC. ATO is in charge of the train driving functions and ATP takes care of safety-related functions. The ATP subsystem helps avoid collisions when the driver ignores the speed limitations. This system automatically audits and regulates the train speed, and if necessary, uses the brakes. The ATO subsystem is responsible for automating the train operation, which includes starting and stopping the train, acceleration, braking, and stopping accuracy. The RCS stands also as an essential onboard component, having a critical influence on sending and receiving data from the wayside AP. RCS includes software and hardware, radios, and antennas, and its primary function is to establish the communication between the train and the wayside AP.

Regarding the wayside components, the Zone Controller (ZC), which in most cases includes the wayside ATP and ATO subsystems, is responsible for its correspondent zone inside the railway network. The railway network is divided into independent zones, such that each zone constitutes its respective wayside infrastructure. The primary function of a ZC is to prevent trains from colliding inside its zone. The ATP subsystem of a ZC is responsible for all the data exchange with the trains in its zone. This subsystem is also in charge of calculating the movement authority for every train inside its zone. The ATO subsystem supplies the train destination and dwells times to all the trains in its zone.

The Computer-based Interlocking (CI) is responsible for defining routes for trains and controlling signals and switch machines regarding these trains' destinations. The Automatic Train Supervision (ATS) system, which is charged for scheduling and supervising the traffic, is also a trackside component but independent from the ZC [24]. The trackside cells, each one represented by one AP, receive trains' connections through Wi-Fi, and then continuously exchange data for the proper

system's functioning [24]. Urban railway systems are progressively more dependent on unified communications, integrated wireless signals, and computers. This transformation raises crucial cyber-security concerns [23]. In the next section, a risk prevention analysis of the CBTC system is performed, with the main focus on this system's cyber-security concerns.

CBTC Risk Prevention Analysis

As a modern railway control system, the CBTC system contains several network and information components, which requires high cyber-security responsibilities. CBTC's most problematic security issues are cyber-attacks exposure and high-risk vulnerabilities in critical devices [25].

Thus, security measures are required not only to help prevent unauthorized users from intermediate in train-to-wayside communications with their Wi-Fi devices but also to avoid traffic sniffing and signal jamming. Hence, jamming attacks and Man-in-the-Middle (MitM) attacks require primordial attention when considering CBTC security's most relevant concerns. While jamming attacks cause interference into wireless communications [26], MitM attacks may cause, not only traffic sniffing, but also wrong control messages injection, and consequent train derailment and collision [27].

With a jamming attack, the attacker intends to jam the wireless signal to disrupt the communication between the train and wayside ATP. Through the emission of an electromagnetic wave, the attacker confuses the train which is unable to distinguish between the jamming signal and the correct data signal from the wayside ATP. The train perceives the electromagnetic wave as noise, significantly lowering the signal-to-noise ratio (SNR) for the wayside ATP signal. In the worst-case scenario, this may cause a communication failure. If the wireless signal continues to be jammed and consequently the communication disconnected, the train stops for safety [28].

In MitM attacks, the attacker assumes control of the communication between the two network nodes. Depending on the type of the attack, the attacker may replay, drop, or even spoof messages, according to its malicious intentions. As Wi-Fi networks are susceptible to MitM attacks, these can be carried at the data-link layer of the Open System Interconnection (OSI) model, which is the base for the Wi-Fi communication protocol. The Address Resolution Protocol (ARP) spoofing is one of many methods for performing a MitM attack [28].

In our analysis, we consider two different types of MitM attacks, message spoofing and replay attacks. The Message spoofing attack consists of injecting unauthorized packets on a communication assuming a false authorized identity [29]. This attack is a significant threat to the CBTC system, since the attacker can identify himself as a CBTC AP and inject wrong control messages. This attack's consequences may be unexpected abrupt braking, train location loss, train speed control loss, train full stop, train derailment, and train collision. In a replay attack the intruder copies targets' exchanged packets and sends extra copies into the network. This attack generates data overflow and may originate an incoherent system's behavior. In a CBTC environment, the critical consequences may be train stop and train control performance breakdown. The message dropping attack creates a false node inside the network and intentionally drops the received packets. Causing Denial of Service (DoS) to many system nodes and eventually to the entire system. This attack's repercussions to CBTC are the same as the ones jamming attack may cause and change to conventional operation.

As end-to-end data encryption and authentication methods rise as adequate solutions to prevent message spoofing and replay attacks, Melaragno et al. [30] introduce Rail Radio Intrusion Detection System (RRIDS) as a command replay and message corruption detection system. Using a µTime Efficient Stream Loss-tolerant Authentication (TESLA) approach called µTesla, this system highly increases burnout on the intruder, which decreases intrusion efficiency and ramification. The RRIDS makes use of a subset of µTesla, appropriated to CBTC systems, with algorithms built on the originating seed and salt variations. RRIDS also is capable of analyzing Radio Frequency (RF) and detecting real-time threats.

Moreover, preliminary results showed that RRIDS was able to detect replay and message corruption attacks with a 100% success rate, and close to 0% CPU usage, throughout the experience.

Nam et al. [31] proposed an innovative version of the ARP protocol for ARP poisoning prevention. This MitM prevention strategy compensates for the ARP lack of authentication and security consideration, with Internet Protocol (IP)/Media Access Control Address (MAC) mapping retaining until the machine goes offline. The proposed MitM-Resistant Address Resolution Protocol (MR-ARP) uses a long-term IP/MAC mapping table with three fields, IP, MAC, and a timer for checking if the machine is still running. Moreover, uses a Voting-based Conflict Resolution (VbCR) for cases where a node with an empty ARP cache and long-term table may receive first ARP malicious responses. Its solution consists of allowing neighbor hosts to send the correct MAC of the host to the first node, which is trying to communicate with it.

Xie et al. [32] designed a message dropping attack detecting scheme based on node querying after messages exchange. Each sampled node must reply with an authenticated acknowledgment (ACK) where if each bit is 1 means that the node received the message and 0 means it missed the message. The authors ranked all the overlay network nodes with a static balanced tree-structured topology. While this scheme was defined mainly for systems with packet broadcasting and overlay networks, it is possible to adapt its attack detection method of querying every node upon receiving a message to the CBTC urgent concerns. Next, we proceed to our CBTC system risk analysis through our version of the FMEA's RPN calculation.

6. Failure Mode and Effect Analysis Application

In this study, we apply FMEA with our new RPN approach to the CBTC system. Besides being a CPS, CBTC has a vital software component with substantial networked data exchange, which positively contributed to our decision on choosing it. We will divide the FMEA application into **four** steps: System Subdivision, Failure Modes, Causes and Effects, RPN Calculation, and Prevention Actions Recording.

6.1. System Subdivision

Initially, the system is divided into different units. We will focus our analysis on the train to the wayside communication system, once it is the one where the failure modes are more related to our previous CBTC risk prevention analysis. In Table 10, we subdivided CBTC into four main subsystems, and display their main components.

Table 10. System Subdivision.

Subsystems	Components
Local control system	Automatic train supervision (ATS)
Wayside system	Zone Controller (ZC) Computer-Based Interlocking (CI)
Vehicle onboard system	Automatic train protection (ATP) Automatic train operation (ATO) Vehicle Onboard Computer (VOBC) Data Communication System (DCS)
Train to the wayside communication system	Radio Communication System (RCS) Access Points (AP)

6.2. Failure Modes, Causes, and Effects

After performing the system subdivision, a unit is chosen, which will be the "train to wayside communication system" unit. Then, a component from the subsystem is chosen, which will be the RCS component, for which failure modes are identified, together with their causes, and effects. In Table 11, we identify the failure modes for the RCS component and its possible causes, and effects. We do not perform any further evaluation of the AP component because it has the same cyber-related failure modes as the RCS component.

Table 11. Failure Modes, Causes and Effects.

Failure Mode	Failure Cause	Failure Effect
Wrong Control Messages injection (Packet Spoofing)	Message Spoofing Attack	Unexpected abrupt braking Train location loss Train speed control loss Train full stop Train collision Train derailment
Message Dropping (Packet Dropping)	Message Dropping Attack	Train full stop Emergency braking; Change to conventional operation
Signal Jamming	Jamming Attack	Train full stop Emergency braking; Change to conventional operation
Communication Delay (Extensive packet duplication and forwarding)	Replay Attack	Train control performance breakdown Change to conventional operation

6.3. Risk Priority Number Calculation

After all failure modes are identified, with their causes and effects, we calculate the RPN for each failure mode. Since we based our RPN calculation on the possible economic impact of the failure mode, we will be always considering the worst consequences for each case. Starting with the "Wrong control message injection" failure mode, which has the worst possible consequences, we assigned 10 to all its RPN factors. Its train collision and train derailment possible consequences can result in several F and SI, high infrastructure damage, severe environmental contamination, and considerable delays.

The "Message Dropping" and the "Signal Jamming" failure modes have the same consequences since their both preceded by a variation of a DoS attack. We assigned 3 to the SF, 2 to IF and DF, and 1 to the EF. These two attacks train full stop and emergency braking consequences may cause light damage to the track and bogies and low delays. To the "Communication Delay" failure mode factors, we assigned 1 to the all four factors. Despite being a MitM attack, the replay attack intentions are to provoke data overflow on the target, thus from our economic impact perspective, this failure mode has the minimum RPN.

The values displayed in Table 12 are a direct result of consulting the Portuguese railway accident reports [19], where we could find data relative to deaths, serious and light injuries, train, and railway damage , delays, and environmental pollution. Accordingly, all the costs for all possible failure mode consequences were estimated and summed, originating a total cost equivalent for each factor. Then, we provide two RPN calculations, the original and our proposal, to grant an easy comparison between both methods.

Table 12. Risk Priority Number values.

Failure Mode	Social	Infrastr	Environ	Delay	RPN	
	0.5	0.35	0.05	0.1	Original	Our Approach
Wrong control message injection	10	10	10	10	10,000	10
Message dropping	3	2	1	2	12	2.45
Signal jamming	3	2	1	2	12	2.45
Communication Delay	1	1	1	1	1	1

After gathering all the values for the RPN formula, we proceed with the RPN calculation:

- Wrong control message injection:

$$10 \times 0.5 + 10 \times 0.35 + 10 \times 0.05 + 10 \times 0.10 = 10 \quad (2)$$

- Message Dropping:

$$3 \times 0.5 + 2 \times 0.35 + 1 \times 0.05 + 2 \times 0.10 = 2.45 \quad (3)$$

- Signal Jamming:

$$3 \times 0.5 + 2 \times 0.35 + 1 \times 0.05 + 2 \times 0.10 = 2.45 \quad (4)$$

- Communication Delay:

$$1 \times 0.5 + 1 \times 0.35 + 1 \times 0.05 + 1 \times 0.10 = 1 \quad (5)$$

Then, with all the RPN ranks gathered, we conclude that the "Wrong control message injection" failure mode is the one with the highest rank, thus the most dangerous and the first to take into consideration on the next step. Compared to the original method to assess the RPN, the main differences are within the "Message Dropping" and the "Signal Jamming" failure modes, which go from "Very Low" in the original method to "Low" in our evaluation. Besides, a small variation in the social and infrastructure factors, for example from 3 to 5 and from 2 to 4, would not represent any change in the outcome for the original RPN, however it would increase from "Low" (2.45) to "Moderate" (4.15) with our approach, which would be more representative of the severity.

6.4. Prevention Actions Recording

On the Prevention Actions Recording step, prevention actions to the failure modes identified above will be briefly summarized based on our risk prevention analysis section. We will suggest actions based on our CBTC system knowledge and the previous risk prevention analysis.

1. Wrong control message injection
    - Originating seed and salt variation method for authentication.
    - Long term IP/MAC mapping table.
2. Message Dropping
    - Query node after messages are sent.
    - Time communications between two nodes with a limit waitable timer.
3. Signal Jamming
    - Low transmission power deteriorates chances for attacker signal location.
    - Transmission of short pulses on a broad spectrum of a frequency band at the same time.
4. Communication Delay
    - Originating seed and salt variation method for authentication.
    - Long term IP/MAC mapping table.
    - IP/MAC binding allows to prioritize traffic with static IP assignment reservation.

It is necessary to regard all these preventive actions in future analysis. The prevention of failure modes is critical to the system's functioning and the evolution of its risk analysis.

6.5. Discussion

While FMEA is a risk analysis method designed for industry and industrial processes, applying its method to CPS has with some limitations. The subdivision step of the FMEA system made our study faster and more intuitive since we intended to focus on the network communication component of the CBTC system. The quantification of risk through RPN ranks also contributed positively to our study. Identifying which failure mode was the most critical for the system was a fundamental part of the

process. To assess the system from an economic impact point of view, we had to create new parameters to calculate the RPN equivalent, since the traditional parameters were not suitable. The previously mentioned limitations of the standard RPN formula, that consists of the multiplication of all parameters, prompted us to propose a new formula to estimate RPN ranks, which not only consists of the sum of all parameters but also uses assigned weights to each one of the parameters. Regarding our RPN calculation formula, we perfected the weights as the result of several RPN calculation tests. These final weights are the ones that best portray the economic impact of the parameters. Nevertheless, in other studies, the study team may apply different weights to these parameters, and their approach would neither be wrong nor worse. According to our evaluation, the presented values were considered fit to the circumstances of the study case.

In this work, we demonstrated how FMEA can be applied to the CBTC system, more precisely to its network communication component. Other CBTC subsystems will be analyzed as future work because they also have vulnerabilities, and are crucial to the critical functioning of the system. We focused our study on system failures caused by cyber-attacks since these are one of the primary sources of failures in the system. We conducted our analysis to assess the risk through an economic impact perspective, however, we will consider other perspectives of risk analysis in our future work.

7. Conclusions and Future Work

In this paper, we have shown how FMEA behaves analyzing highly critical CPS. The CBTC is a critical system with an extensive software unit and frequent network data exchange that correctly corresponded to our use case necessity. We briefly described this system's functions along with its primordial components.

Regarding CBTC risk prevention, we addressed existing works on MitM attacks and DoS attacks risk prevention. Considering our perspective on the FMEA limitations, we proposed a novel approach to FMEA's RPN estimation that considers social, infrastructure, environmental, and delay costs, concerning our CBTC use case. We also suggested a weighted sum based formula for RPN calculation. We assessed CBTC risk, specifically the Train to wayside communication subsystem risks, through our proposed FMEA version. Our results show that from an economic perspective, the message spoofing attack has the highest risk to the CBTC system. We concluded that the existing risk assessment methods, focused on industrial systems, must be improved to approach CPS risk analysis concerns. For applying the proposed method to another country, the study team must use that country's VPC, CO_2 emission tax value, and accident reports.

In future work, we will apply our method to other CBTC subsystems, such as the CBTC local control system, wayside system, and vehicle's onboard system. Moreover, we intend to assess the risk of aircraft and hydroelectric power systems using other risk assessment methods.

Author Contributions: Conceptualization, B.C.; methodology, J.O., G.C., B.C. and J.B.; validation, G.C., B.C. and J.B.; formal analysis, G.C., B.C. and J.B.; investigation, J.O. and G.C.; writing—original draft preparation, J.O. and G.C.; writing—review and editing, J.O., G.C., B.C. and J.B.; visualization, G.C.; supervision, G.C., B.C. and J.B.; funding acquisition, J.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: This work is supported by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the PORTUGAL 2020 framework [Project InfraCrit with Nr. 039555 (POCI-01-0247-FEDER-039555)]

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lyu, X.; Ding, Y.; Yang, S.H. Safety and security risk assessment in cyberphysical systems. *IET-Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 221–232. [CrossRef]

2. Wu, W.; Kang, R.; Li, Z. Risk assessment method for cyber security of cyber physical systems. In Proceedings of the First International Conference on Reliability Systems Engineering (ICRSE'15), Beijing, China, 21–23 October 2015; p. 4. [CrossRef]
3. Amin, S.; Schwartz, G.; Hussain, A. In quest of benchmarking security risks to cyber-physical systems. *IEEE Netw.* **2013**, *27*, 19–24. [CrossRef]
4. Stamatis, D. *Failure Mode and Effect Analysis: FMEA from Theory to Execution*; ASQ Quality Press, Milwaukee, WI, USA: 2003.
5. Wang, Y.M.; Chin, K.S.; Poon, G.K.K.; Yang, J.B. Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean. *Expert Syst. Appl.* **2009**, *36*, 1195–1207. [CrossRef]
6. Xie, F.; Lu, T.; Guo, X.; Liu, J.; Peng, Y.; Gao, Y. Security analysis on Cyber-Physical System using attack tree. In Proceedings of the 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Beijing, China, 16–18 October 2013; pp. 429–432. [CrossRef]
7. Ruchkin, I.; Rao, A.; De Niz, D.; Chaki, S.; Garlan, D. Eliminating inter-domain vulnerabilities in cyber-physical systems: An analysis contracts approach. In Proceedings of the 1st ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, Co-located with CCS'15, Denver, CO, USA; October 2015; pp. 11–22. [CrossRef]
8. Ali, N.; Hong, J.E. Failure detection and prevention for cyber-physical systems using ontology-based knowledge base. *Computers* **2018**, *7*, 68. [CrossRef]
9. Tay, K.M.; Lim, C.P. Fuzzy FMEA with a guided rules reduction system for prioritization of failures. *Int. J. Qual. Reliab. Manag.* **2006**, *23*, 1047–1066. [CrossRef]
10. Liu, H.C.; You, J.X.; Fan, X.J.; Lin, Q.L. Failure mode and effects analysis using D numbers and grey relational projection method. *Expert Syst. Appl.* **2014**, *41*, 4670–4679. [CrossRef]
11. Wu, J.; Tian, J.; Zhao, T. Failure mode prioritization by improved RPN calculation method. *Reliab. Maintainab. Symp.* **2014**, 5. [CrossRef]
12. Kabak, M.; Özveri, O. The Usage of MCDM Techniques in Failure Mode and Effect Analysis. *J. Econ. Manag. Res.* **2015**, *4*, 94–108.
13. Rezaei, F.; Yarmohammadian, M.H.; Haghshenas, A.; Fallah, A.; Ferdosi, M. Revised risk priority number in failure mode and effects analysis model from the perspective of healthcare system. *Int. J. Prev. Med.* **2018**, *9*, 1–8. [CrossRef]
14. Carpitella, S.; Certa, A.; Izquierdo, J.; La Fata, C.M. A combined multi-criteria approach to support FMECA analyses: A real-world case. *Reliab. Eng. Syst. Saf.* **2018**, *169*, 394–402. [CrossRef]
15. Ciani, L.; Guidi, G.; Patrizi, G. A Critical Comparison of Alternative Risk Priority Numbers in Failure Modes, Effects, and Criticality Analysis. *IEEE Access* **2019**, *7*, 92398–92409. [CrossRef]
16. Spreafico, C.; Russo, D.; Rizzi, C. A state-of-the-art review of FMEA/FMECA including patents. *Comput. Sci. Rev.* **2017**, *25*, 19–28. [CrossRef]
17. Gilchrist, W. Modelling Failure Modes and Effects Analysis. *Int. J. Qual. Reliab. Manag.* **1993**, *10*, 16–23. [CrossRef]
18. Instituto da Mobilidade e dos Transportes, IP. Apuramento de Indicadores Comuns de Segurança (in Portuguese). Technical Report. 2015. Available online: http://www.imt-ip.pt/sites/IMTT/Portugues/TransportesFerroviarios/CaminhodeFerro/GuiasdeApoio/Documents/Guia_Implementa%C3%A7%C3%A3o_ICS_v3.pdf (accessed on 12 August 2020).
19. Gabinete de Prevenção e Investigação de Acidentes com Aeronaves e de Acidentes Ferroviários (GPIAAF) (in Portuguese). Investigation Activities Annual Report—Rail Transportation. Technical Report. 2018. Available online: http://www.gisaf.gov.pt/?lnk=1282ca70-b489-4691-8079-6d8f784788ec (accessed on 12 August 2020).
20. Caruso, M.; Tornaghi, M.; Negro, P. Applicability of the Sustainable Structural Design (SSD) method at Urban/Regional/National Level. *JRC Tech. Rep.* **2017**, *2017*. [CrossRef]
21. Organisation for Economic Co-operation and Development (OECD). Taxing Energy Use 2019: Country Note—Portugal. Technical Report. 2019. Available online: https://www.oecd.org/tax/tax-policy/taxing-energy-use-iceland.pdf (accessed on 12 August 2020).
22. Xu, J.; Chen, L.; Gao, W.; Zhao, M. CBTC Simulation Platform Design and Study. *J. Comput. Commun.* **2015**, *3*, 7. [CrossRef]

23. Chen, B.; Schmittner, C.; Ma, Z.; Temple, W.; Dong, X.; Jones, D.; Sanders, W. *Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective*; SAFECOM 2015 Workshops; Springer: Cham, Switzerland, 2015; pp. 277–290. [CrossRef]
24. Farooq, J.; Soler, J. Radio Communication for Communications-Based Train Control (CBTC): A Tutorial and Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1377–1402. [CrossRef]
25. Wu, W.; Bu, B. Security analysis for CBTC systems under attack-defense confrontation. *Electronics* **2019**, *8*, 991. [CrossRef]
26. Lakshminarayana, S.; Revadigar, G.; Karachiwala, J.S.; Sravana Kumar, S.L.; Hu, Y.C.; Chang, S.Y.; Yau, D.K. Signal jamming attacks against communication-based train control: Attack impact and countermeasure. In Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Stockholm, Sweden, 18–20 June 2018; pp. 160–171. [CrossRef]
27. Li, Y.; Zhu, L. A Bayesian game based defense scheme for CBTC systems under Man-in-the-middle attacks. In Proceedings of the 2019 IEEE Intelligent Transportation Systems Conference, ITSC, Auckland, New Zealand, 27–30 October 2019; pp. 2172–2176. [CrossRef]
28. Kim, S.; Won, Y.; Park, I.H.; Eun, Y.; Park, K.J. Cyber-Physical Vulnerability Analysis of Communication-Based Train Control. *IEEE Internet Things J.* **2019**, *6*, 6353–6362. [CrossRef]
29. Lopez, I.; Aguado, M. Cyber security analysis of the European train control system. *IEEE Commun. Mag.* **2015**, *53*, 110–116. [CrossRef]
30. Melaragno, A.; Bandara, K.R.S.; Fewell, A.; Wijesekera, D. Rail Radio Intrusion Detection System (RRIDS) for Communication Based Train Control (CBTC). In Proceedings of the IEEE International Conference on Intelligent Rail Transportation (ICIRT), Birmingham, UK, 23–25 August 2016; pp. 39–48. [CrossRef]
31. Nam, S.Y.; Kim, D.; Kim, J. Enhanced ARP: Preventing ARP Poisoning-Based Man-in-the-Middle Attacks. *IEEE Commun. Lett.* **2010**, *14*, 187–189. [CrossRef]
32. Xie, L.; Zhu, S. Message Dropping Attacks in Overlay Networks: Attack Detection and Attacker Identification. *ACM Trans. Inf. Syst. Secur.* **2006**, *11*, 1–10. [CrossRef]