aerospace

Article

The Impact of Data Injection on Predictive Algorithm Developed within Electrical Manufacturing Engineering in the Context of Aerospace Cybersecurity

Jorge Bautista-Hernández [1,2,*] and María Ángeles Martín-Prats [1]

[1] Department of Electronics Engineering, University of Seville, 41004 Seville, Spain; mmprats@us.es
[2] Department of Electrical Engineering, Airbus Poland, 02-256 Warsaw, Poland
* Correspondence: jorbauher@alum.us.es

Abstract: Cybersecurity plays a relevant role in the new digital age within the aerospace industry. Predictive algorithms are necessary to interconnect complex systems within the cyberspace. In this context, where security protocols do not apply, challenges to maintain data privacy and security arise for the organizations. Thus, the need for cybersecurity is required. The four main categories to classify threats are interruption, fabrication, modification, and interception. They all share a common thing, which is to soften the three pillars that cybersecurity needs to guarantee. These pillars are confidentiality, availability, and integrity of data (CIA). Data injection can contribute to this event by the creation of false indicators, which can lead to error creation during the manufacturing engineering processes. In this paper, the impact of data injection on the existing dataset used in manufacturing processes is described. The design model synchronizes the following mechanisms developed within machine learning techniques, which are the risk matrix indicator to assess the probability of producing an error, the dendrogram to cluster the dataset in groups with similarities, the logistic regression to predict the potential outcomes, and the confusion matrix to analyze the performance of the algorithm. The results presented in this study, which were carried out using a real dataset related to the electrical harnesses installed in a C295 military aircraft, estimate that injection of false data indicators increases the probability of creating an error by 24.22% based on the predicted outcomes required for the generation of the manufacturing processes. Overall, implementing cybersecurity measures and advanced methodologies to detect and prevent cyberattacks is necessary.

Keywords: predictive algorithms; cybersecurity; machine learning; advanced persistent threats

check for updates

Citation: Bautista-Hernández, J.; Martín-Prats, M.Á. The Impact of Data Injection on Predictive Algorithm Developed within Electrical Manufacturing Engineering in the Context of Aerospace Cybersecurity. *Aerospace* **2023**, *10*, 984. https://doi.org/10.3390/aerospace10120984

Academic Editor: Spiros Pantelakis

Received: 18 October 2023
Revised: 6 November 2023
Accepted: 21 November 2023
Published: 23 November 2023

1. Introduction

The latest reports in 2022 from the European Union Agency for Cybersecurity (ENISA) show 586 reported cybersecurity incidents compared to 77 in 2012. Cyberattacks are increasing not only in frequency, but also in complexity, and are affecting organizations worldwide. Safety is an important pillar to protect the overall assets. Risk assessment procedures are likely to define the level of impact, the vulnerabilities, and the affected assets in order to minimize the risk and reach the highest level of safety [1]. This level of safety cannot be achieved in the new digital age since the security protocols are more vulnerable and data privacy can be easily exposed. On the other hand, predictive algorithms, which are developed to perform processes automatically and to reduce costs in organizations, are sensitive to threats such as, for example, data modifications [2]. Thus, data protection is essential in this context. Cybersecurity is needed to ensure the confidentiality, availability, and integrity of data resulting from access to untrusted sources. The aim of this study is to analyze the impact of data modification in order to observe the time increase in electrical harnesses manufacturing and error rate as hazard outcomes of the aerospace predictive algorithm after the dataset has been compromised. The predictive algorithm performance is also shown before and after the event has occurred. Thus, countermeasures to protect the dataset in the cybersecurity context are considered and applied for this purpose.

Algorithms development aims to perform tasks faster, which are designed to enhance safety. Most of them are modeled to replace manual tasks by automation. In aerospace, there are different types of errors which can lead to accidents. Human errors can contribute up to 80% of the total errors [3]. Safety investigations about electrical wiring harness, conducted by authorities, conclude that some aircraft accidents were caused by failures within the electrical installation, resulting from improper design, maintenance, or a combination of them. These errors were mainly created from manual operations generated by humans during different stages of the engineering processes. Traditional methods, related to risk assessment, focus on the identification, analysis, and management of risks. However, they remain obsolete in the new digital world [4,5]. Thus, the use of predictive algorithms applied within the aerospace industry, which aims to prevent failures and decrease errors, is fundamental to maintain aerospace safety at the highest level [6–8]. Technologies, such as machine learning developed within the artificial intelligence, are key to enhance such algorithms [9,10]. Indeed, the new digital age requires more digital sources in order to interconnect processes to overcome the system complexity in the cyber–physical space environment. On the other hand, multiple users not only have access to the digital application, where algorithms are executed and outcomes are displayed, but also they are frequent users on a daily basis. Consequently, data can be compromised. Therefore, it is necessary to protect data using techniques within the framework of the cybersecurity.

The four main categories to classify threat types are interruption, fabrication, modification, and interception in the cybersecurity context. They all aim to develop malicious content in a system. Complex techniques developed by attackers and malware are out of the scope of this paper [11,12].

The new digital environment requires a holistic approach that integrates more automation and system interconnection towards a better analysis of the error creation [13]. The development of predictive algorithms using machine learning techniques aims to connect the cyberspace environment, enable system automation, and prevent error creation during the manufacturing processes in order to maintain aerospace safety at the highest level [14]. Moreover, this environment presents vulnerabilities that affect data privacy. Thus, the need for cybersecurity is essential in this digital domain.

Moreover, in the defense sector, the simulation for data injection could represent a significant risk to the digital assets. The rise of advanced persistent threats (APTs) which are a very highly sophisticated malware is evolving and aims to avoid security measures. Consequently, the attackers often send phishing emails until the first target system gets compromised. Once the malware has been deployed, other intrusive tools can enable the propagation to the internal network. Therefore, data extraction can be conducted, allowing the attackers to steal sensitive information. Thus, all the significant risks are essential for the organization to adopt cybersecurity measures [15]. Additionally, it is important to recognize potential breaches and analyze the consequences in order to strengthen the protection of the digital assets.

Safety and cybersecurity in aerospace have become crucial priorities to be maintained in modern aircraft systems. The increasing systems interconnection and high dependency on software have enhanced the potential threats, leading cybersecurity to be a high priority in ensuring safety [16]. Vulnerabilities in software require focusing on its resilience in order to guarantee system security [17]. The implementation of advanced technology in modern aviation such as autopilot, engines control, air data communication, and electrical power is controlled by software. The flight control of the aircraft has evolved. Software is in charge of the code execution which generates the outputs to control the aircraft. The high level of security, which is required to integrate this system in aerospace, has established that up to 70% of the software development is dedicated to the robustness of the code [18,19]. This process includes the generation of rigorous tasks such as failure detection, isolation, synchronization, reconfiguration in a detected failure, and system control. In this context, any failure that occurs within data or code execution should not be propagated to the aircraft systems [18].

The design of any aviation system is implemented according to the high safety standards, which include guidelines on development, verification, validation, and configuration. Design assurance levels are also established to safeguard the aerospace assets [19]. All these approaches are aligned with the National Institute of Standards and Technology (NIST) within the cybersecurity framework, aiming to enhance security systems. Consequently, safety analysis is of paramount importance to ensure aircraft safety [20].

In this paper, the analysis was conducted after injecting malicious data, which has generated a negative impact on the performance of the predictive algorithms. The motivation to carry out this research was to analyze the impact of cyberattacks, to highlight its importance, and to understand the consequences generated on the engineering processes in the aerospace manufacturing plant. Thus, the performance of the algorithm, after the dataset was compromised, has been the main focus of this study. An assessment of the impact on time and error rate was carried out. Additionally, a detection strategy to detect a potential cyberattack has been set up to protect the algorithm. The hypotheses, which were considered, assumed that the attacker has information on the dataset of the victim and has succeeded to access the system. The following research questions are formulated as follows:

- Can data injection stop the manufacturing of electrical harness?
- Can this event be avoided by the application of proper cyber defense techniques?
- Does the quantity of compromised data affect the efficiency of the algorithm?

The remainder of this paper is as follows: Section 2 presents the structure of the model algorithm developed and the necessity of the contribution of the cybersecurity to the cyber–physical space. Section 3 takes an approach of the inconsistencies generated after data have been injected into the algorithm and shows an analysis of the consequences observed on the outcomes. Also, this Section includes the detection strategy to stop the algorithm operation after data have been injected. Section 4 contains the conclusions and future work.

2. Materials and Methods

The increasing interconnectivity and complexity of the systems requires the use of advanced technologies in cyberspace. The cyberspace environment highly relies on digital applications, which are based on innovative techniques developed within the context of artificial intelligence such as predictive algorithms [21]. Machine learning techniques are used to develop predictive algorithms, which play a relevant role to optimize manufacturing processes, mitigate errors, and enhance safety. At the same time, cyberspace is more vulnerable and exposed to cyberattacks in this new digital environment. Thus, the importance of cybersecurity has been raised as a main priority to maintain the integrity and security of the digital cyberspace [12].

2.1. Predictive Algorithm

The predictive algorithm applies input parameters within the real dataset presented in the 'bill of material' of each electrical harness in a military aircraft. This dataset is used for the creation of the processes necessary to manufacture the electrical harnesses. The experimental data in this case study are the electrical harnesses manufactured and installed in an aircraft. The initialization of the kernel is based on the data from the selected parameters, where the risk matrix function classified each harness and established a different level of probability of error creation during the manufacturing processes. After processing the data, the algorithm outputs show an evaluation of the likelihood of error creation and threats visualization represented by the following elements:

- The automation script: The generation of the automatic processes will avoid human errors which are the main trigger of error creation [22].

- The dendrogram: The hierarchical representation of the dataset can help to establish relationships between different levels of risk by clustering the dataset in groups with similarities [23].
- The logistic regression: The statistical method can be used to model the probability of occurrence using the variables from the risk matrix and to predict the risk of error creation in new harnesses assessment [24].
- The confusion matrix: It is used to evaluate the performance of the classification model used for predictions through the logistic regression method. The true positives, true negatives, false positives, and false negatives provide insights into the performance of the logistic regression model in predicting risk events. Thus, it helps to not only define the performance of the algorithm, but also to detect inconsistences within the dataset. A large amount of true or false negatives can indicate the low performance of the algorithm [25].

Data generation was analyzed and processed through the following algorithm structure, as represented in Figure 1.

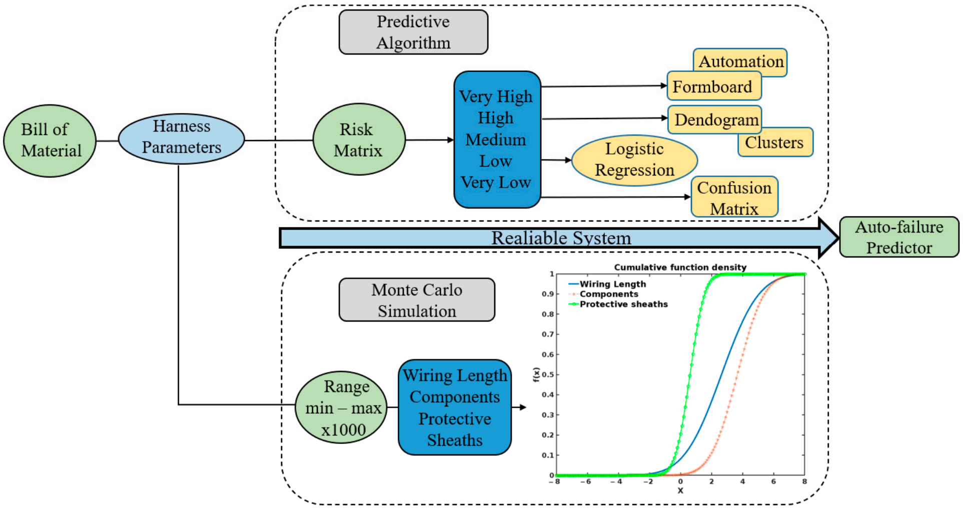

Figure 1. Diagram representation of the structure of the predictive algorithm.

2.2. Risk Matrix

The risk matrix is the mechanism based on the assessment of the electrical harnesses which depends on the following parameters. These input parameters are the number of zones (Z), number of wires (H), and number of electrical components (N) in each harness. The risk matrix function is represented in the following equation:

$$\Phi(\mathrm{Z},\mathrm{H},\mathrm{N}) = \sum_{i=1}^{4} \mathrm{X_i} = \mathrm{X_1(Z)} + \mathrm{X_2(H)} + \mathrm{X_3(N)} + \ \mathrm{X_4(H)} \quad (1)$$

This function is defined with four parameters $\mathrm{X_i}$, which are evaluated on a scale of 1 to 5, with 1 being the simplest geometry and 5 the most complex. These four parameters $(\mathrm{X_1},\ \mathrm{X_2},\ \mathrm{X_3},\ \mathrm{X_4})$ depend on three other parameters, namely, the number of zones (Z), number of wires (H), and number of electrical components (N) present on each electrical harness. $\mathrm{X_1}$ represents the scores assigned due to the complexity of the 3D geometry. $\mathrm{X_2},\ \mathrm{X_3},\ \mathrm{X_4}$ are related to the scores assigned based on the electrical architecture, number of electrical connections, and number of electrical components. They are used as input parameters to define the manufacturing processes of electrical harnesses [14].

2.3. Cybersecurity Context

Cyber defense techniques are crucial to protect systems, data, and networks from threats. The application of cyber defense techniques to the predictive algorithm ensures confidentiality, integrity, and availability of the sensitive data. The analysis of vulnerabilities, anomalies, and countermeasures is an essential strategy to defeat cyberattack scenarios [26].

In the cybersecurity context, the way to compromise data can be presented as follows:

- Data modification: Malicious data can search for specific data within the dataset and modify them to achieve their goals.
- Changing random values: To change data values randomly to cause confusion and make the data less reliable.
- Data deletion: To delete certain information in order to cause significant problems, especially if the deletion of the data is critical to the business or customers.
- Data reformatting: To change the data format in order to make it more difficult to use.
- Insertion of false data: To falsify data into the dataset to deceive users who query it.

In this study, the existing dataset which is used as input data to analyze the algorithm performance, has been compromised. The main consequences related to the error rate within the results after data injection have been analyzed. Data injection was carried out on the predictive algorithm, which is in charge of dataset analysis, patterns identification, and the outcomes forecast for decision making. It is hosted in the internal network within the infrastructure. The provided access is via security protocols which are updated regularly. No external access to the information system is allowed. The predictive algorithm interacts with data sources and means, which comply with security measures. However, the exposure of the system to the attack surface can allow unauthorized users to potentially exploit vulnerabilities and cause the damage [27]. Vulnerabilities within the code and unpatched software can expand the attack surface, amplifying the risk of data breaches. Indeed, a smaller attack surface mitigates the risk and makes the exploitation more difficult and the system more secure [28]. Despite security measures, social engineering attack surface such as phishing can contribute to the enlargement of the surface attack, highlighting the need for more security measures. Thus, the development of detection strategy can significantly reduce an organization from a potential cyberattack [29].

These types of data, which were injected in this study, were linked to the risk matrix function. The experiment was performed at the electrical harness department in the aerospace industry using a dataset related to 157 harnesses installed in a C295 military aircraft. The data were modified by selection of random values within the minimum and maximum of the scalar function risk matrix defined in Equation (1) for each electrical harness. The data affected before and after injection, represented by different levels of the risk matrix function, are presented in Table 1. One hundred and twenty-three harnesses have presented a low-risk matrix, 29 presented a moderate-risk matrix, and 5 of them have presented a high-risk matrix. After data injection, 147 showed a low-risk matrix, 10 showed a moderate-risk matrix, and none of them have presented a high-risk matrix. Overall, 38 (24.22%) harnesses have shown a different risk matrix function after data have been injected.

Table 1. Data affected before and after data injection represented by different levels of the risk matrix function.

Risk Matrix	Before Data Injection	After Data Injection
Low	123	147
Moderate	29	10
High	5	-

3. Results

The real dataset of 157 electrical harnesses, which were manufactured for this type of aircraft, has shown that only 3.18% of the harnesses have presented a high-risk matrix, 18.47% a medium-risk matrix, and most of the harnesses, 78.34%, have presented a low- risk matrix of error creation during the manufacturing processes. However, after the dataset has been modified, 93.63% of the harnesses have shown a low-risk matrix, 6.36% a medium-risk matrix, and none of the harnesses have presented a high-risk matrix. The probability of error creation during the manufacturing processes has increased by 24.22% in comparison with the real dataset scenario. This situation threatens the safety in aerospace. Thus, countermeasures are necessary to be applied and to protect the dataset. Table 2 shows the likelihood of error creation before and after data injection.

Table 2. Likelihood of error creation associated with the risk matrix before and after data injection.

Risk Matrix	Real Data	Injected Data
High	3.18	0
Medium	18.47	6.36
Low	78.34	93.63

Figure 2 depicts the impact of data injection on modifying the real dataset. This event has created a false behavior on the algorithm performance. The risk matrix has established different scores on each electrical harness, changing the probability of error creation. The blue line represents the real dataset associated with the real risk matrix for the experimental dataset and the orange line represents the variation on the risk matrix after data have been injected. This false behavior generated by the data injected is affecting the calculation of the manufacturing time.

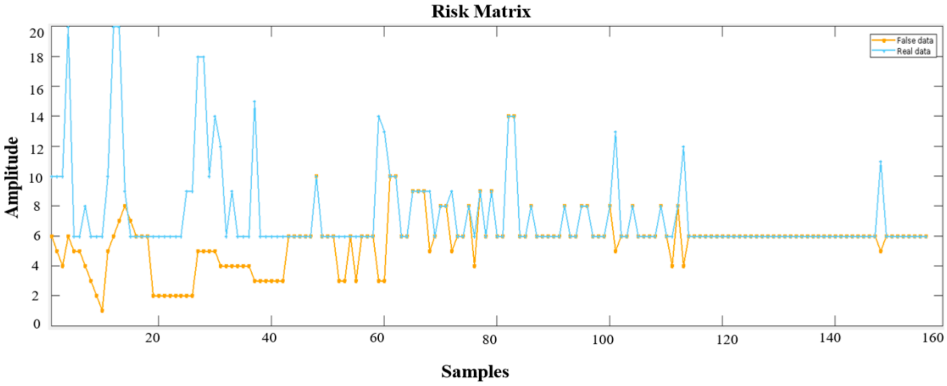

Figure 2. Risk matrix representation of dataset before (real data presented in blue color) and after injection (false data presented in orange color).

Figure 3 shows that the total manufacturing time established for the entire real dataset has decreased from 239.3 h in the green bar to 182.5 h, as represented in the gray bar. The time has decreased by 23.73% after data injection, what has generated a false time calculation. This anomaly can be an indicator of a cyberattack.

The dendrogram is another indicator to analyze the impact of data injection. Figure 4 represents the clusters showing similarities between the dataset and grouping them into families. This situation allows for identifying patterns and improving the decision making. The number of clusters has been increased after data injection from one cluster to three. In the case of real dataset, it is possible to distinguish one family which needs to receive special attention. The groups which were created with similarities are clusters I, J, K and L, M, N, O, P. The rest of the dataset is compact within the main cluster. However, after data injection, the number of clusters has increased to three and the data have been dispersed. After dispersion of the dataset, the following groups are defined from A′ to R′.

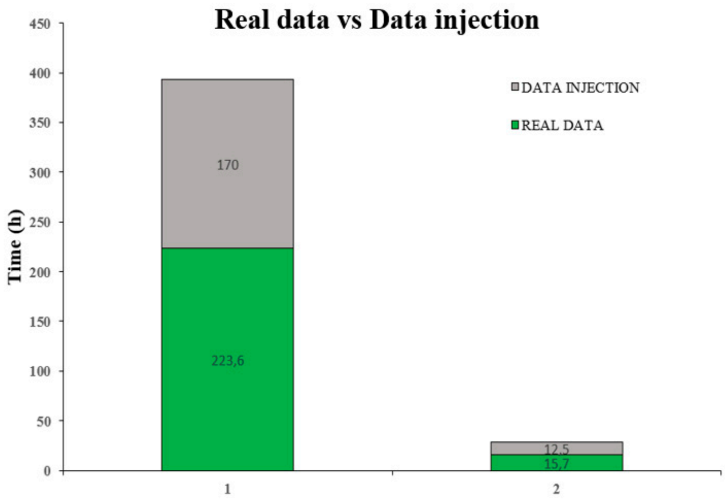

Figure 3. Manufacturing time representation of dataset before (real data presented in green color) and after injection (false data presented in gray color).

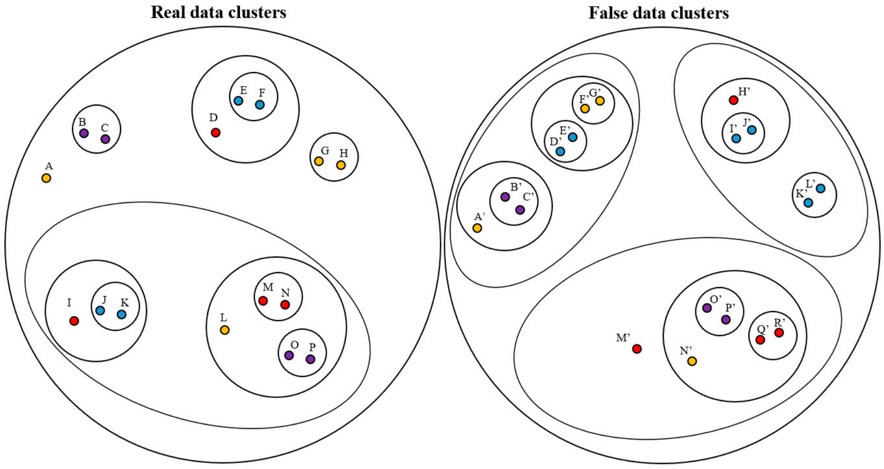

Figure 4. Dendrograms presenting groups of similar data in each node before injection (real data shown on the left) and after injection (false data shown on the right).

The logistic regression shown in Figure 5 represents the best curve fitted to the dataset. The curve shows the probability of error creation (binary dependent variable) versus the risk matrix (independent variable). The blue curve is referred to the real data and the orange curve to the injected data. The probability function associated with the logistic regression is used for new predictions. The decision boundary with real and false data is different after the data have been injected. The risk matrix function presents different values in both situations. Therefore, the model will wrongly predict the new instances. This situation negatively affects the performance of the algorithm. Thus, the algorithm has lost its reliability after data have been injected.

Figure 6 represents the confusion matrix showing the performance of the algorithm. The predictions are labeled as: true negatives (TN), true positives (TP), false negatives (FN), and false positives (FP). After running the simulation with the real dataset, the results are as follows: TN = 26, TP = 6, FN = FP = 0. However, after data have been injected, the results are: $TN' = 1$, $TP' = 3$, $FN' = 0$, $FP' = 27$; the increase in the number of false positives can be observed. This situation indicates a decrease in the performance of the predictive algorithm. Therefore, the classified data can be used as a good indicator for cyberattack detection. The confusion matrix collects all the threat indicators. This early detection mechanism enables a fast reaction and reduces the malicious risk [30].

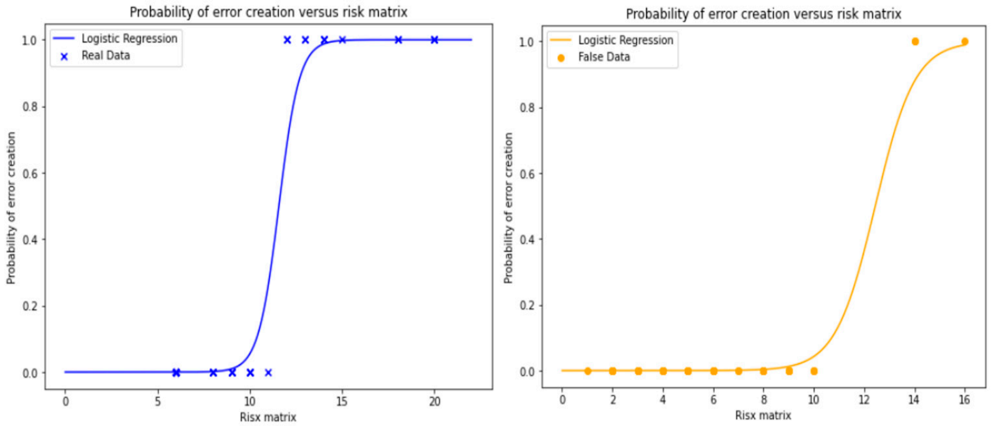

Figure 5. Logistic regression curve before (real data shown on the left) and after injection (false data shown on the right) representing different fittings of the dataset in each situation.

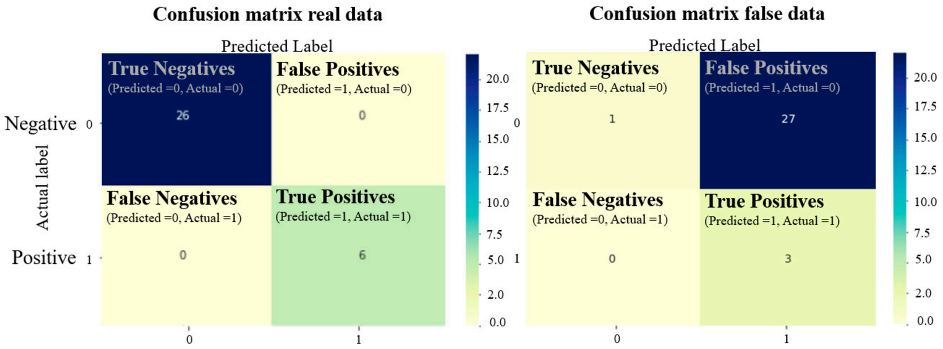

Figure 6. Confusion matrix outcomes model before (real data shown on the left) and after injection (false data shown on the right).

The classifier has changed its performance from 32 correct predictions split between 26 correctly predicted as true negatives and 6 correctly predicted as true positives, while the algorithm was using correct data. However, after data have been injected, there are only four correct predictions split between one correct prediction as true negative and three correct predictions as true positives. There are 27 incorrect predictions as false positives, which involve a decrease in the performance metrics.

Table 3 shows the main outcomes of metrics defined for the algorithm. It shows the impact generated on the performance after data have been injected into the algorithm.

Table 3. Metrics calculation to evaluate the algorithm performance before and after data injection.

Metrics Comparison	Data Real	Data Injection
Precision $=\frac{\text{TP}}{\text{TP+FP}}$	1.0	0.1
Recall $=\frac{\text{TP}}{\text{TP+FN}}$	1.0	1.0
Accuracy $=\frac{\text{TP+TN}}{\text{TP+TN+FP+FN}}$	1.0	0.19
$\text{F}_1=\frac{2\ \text{TP}}{2\ \text{TP+FP+FN}}$	1.0	0.13

The results obtained from the confusion matrix, which compare the metrics using real and false data, are depicted in Figure 7.

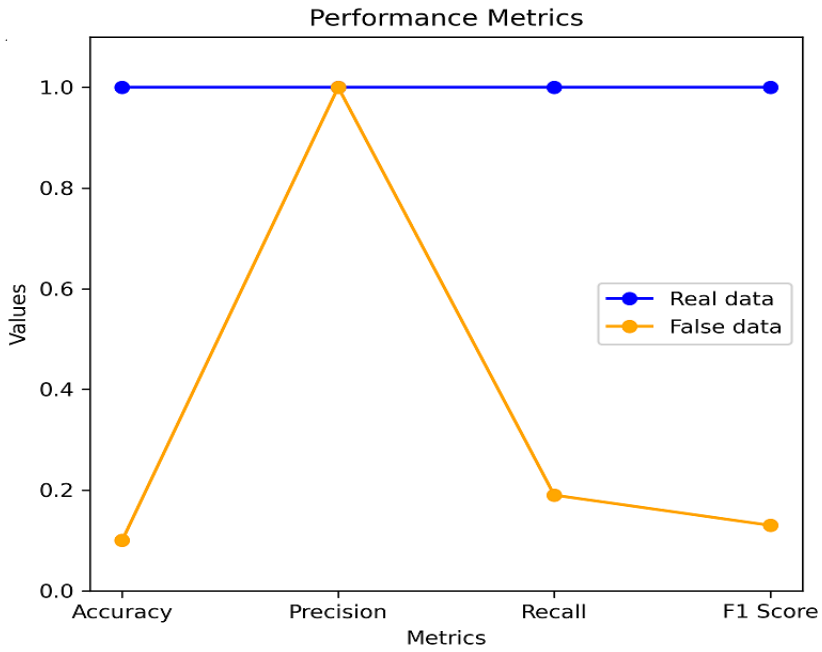

Figure 7. Comparison between accuracy, precision, recall, and F_1 score evaluation metrics between real data (presented in blue color) and false data (presented in orange color).

Overall, data injection compromises the integrity principle based on confidentiality, availability, and integrity of the data [31]. As the attacker can modify the inputs, the detection mechanism is necessary to identify this scenario. This anomaly will affect not only the manufacturing time, but also the risk matrix function Φ, which shows the probability of creating an error during the manufacturing processes. It is critical for the proper performance of the algorithm. Thus, security practises are essential to ensure safety and to protect the algorithm.

The protective mechanism is based on the following detection strategy. The strategy is set up on anomaly detection and monitoring. The implemented mechanism aims to detect the unusual behavior of the risk matrix function defined in Equation (1) in order to identify security breaches. This function depends on four parameters shown in the explicit formula. Indeed, the risk matrix is equal to the sum of those parameters associated with each harness. The scalar function maintains this equality when the real data are used as input of the algorithm. Thus, this condition is fulfilled, allowing the code to continue its execution. However, if this condition is not fulfilled, the code execution will be stopped. Thus, the algorithm will not calculate any outcomes and will not show any false data. This detection strategy is represented in Figure 8.

The model was previously validated using Monte Carlo simulation, which is a method to assess the reliability of the engineering system. The simulation was carried out using the following input parameters: p_1 for wiring length, p_2 for number of electrical components, and p_3 for the protective sheath quantities present in the 'bill of material' on each harness. The Monte Carlo simulation determines the performance of the model for implementation purposes. The baseline run of Monte Carlo simulation was executed 1000 times across a range between maximum and minimum values of meters of wiring length (0.29–2374.79), units of number of components (4–2243), and meters of protective sheath (0.06–22.59) [32].

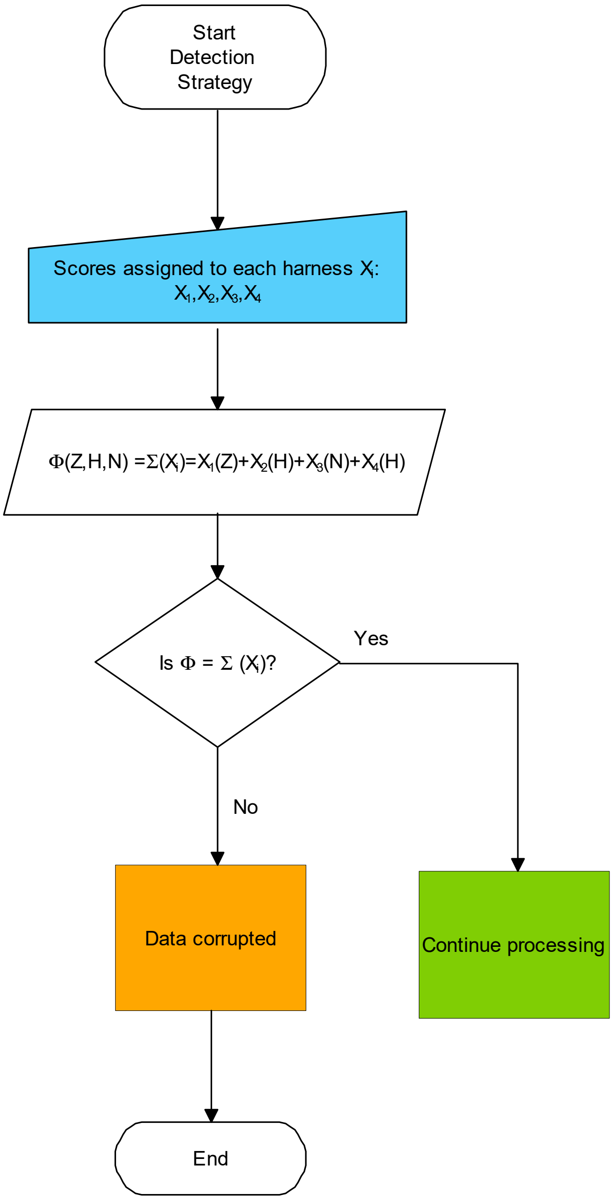
Start Detection Strategy
Scores assigned to each harness X_i: X_1, X_2, X_3, X_4
$\Phi(Z,H,N) = \Sigma(X_i) = X_1(Z)+X_2(H)+X_3(N)+X_4(H)$
Is $\Phi = \Sigma(X_i)$?
Yes
No
Data corrupted
Continue processing
End

Figure 8. Detection strategy to stop the algorithm computation after data have been successfully injected.

The results of the Monte Carlo simulation were evaluated through the cumulative distribution function, which was defined for the three parameters selected. The results showed that the expected values were within a range of high probability of occurrence. After running the simulations, a new outcome was expected to have a wiring length of 2 m, 45 electrical components, and a protective sheath length between 1.49 and 4.48 m within a range of probabilities between 50 and 90%. These results showed that 123 out of 157 (78.34%) of the total electrical harnesses used in the simulation have presented the most common values, which are typical for this type of aircraft.

Moreover, the 1000 runs provide enough evidence to consider the predictive algorithm as a reliable system. Conclusively, the predictive algorithm can be implemented as an auto-failure predictor [32–34].

4. Conclusions

This study was based on the dataset of electrical harnesses, manufactured and installed in a military aircraft. The experimental approach was based on data injection in predictive algorithms, which is necessary to develop manufacturing processes correctly. The main outcomes obtained from the algorithm are the risk matrix, the automation scripts, the dendrogram, the logistic regression, and the confusion matrix, which were developed using machine learning techniques within the artificial intelligence context. The risk matrix brings a state-of-the-art innovation since the aerospace manufacturing processes will be generated from the perspective of failures prevention by using techniques developed within the artificial intelligence context. Traditional methods establish the creation of the manufacturing processes without this consideration, generating failures which can potentially threaten safety in aerospace. This proposed innovative approach leverages the risk matrix, which is the mechanism used to assess the risks based on the likelihood and potential impact. This integrated approach can enhance decision-making processes, and therefore the development of the effective risk mitigation strategies.

The algorithm performance was analyzed before and after data injection. Before the data have been modified, the algorithm had shown a good performance. These results prove the high reliability level of the algorithm. However, the accuracy of the algorithm has been reduced to 19% after data injection. The findings after data have been injected show a negative impact on the performance of the algorithm. Data modification caused the failure of the algorithm performance. Consequently, the algorithm's effectiveness and reliability were compromised as a result of the data modification. After data injection, the risk matrix function has changed, showing that the probability of error creation during the manufacturing processes has increased by 24.22% compared to the real dataset scenario. Security techniques were considered and developed to protect the algorithm and avoid malicious propagation to the outcomes. These techniques are used to secure the correct performance of the algorithm. By prioritizing security measures, the integrity and reliability of the algorithm are maintained, thereby preserving the accuracy and trustworthiness of its outputs. Synchronization of the outcomes is also guaranteed.

Based on the results of this study, it can be concluded that the comparison identified between the algorithm performance before and after data injection has provided valuable insights into the manufacturing processes of electrical harnesses. The study highlights the importance of monitoring the metrics and the discrepancies found within the dataset in order to detect possible cyberattacks. It can also prevent the occurrence of errors and enhance the reliability of the manufacturing processes.

Future work should focus on the analysis of the model variability from another type of aircraft with more extensive datasets. This situation will enable a more comprehensive assessment of the performance of the algorithm across a wider range of aircraft types. Indeed, the use of diverse data will allow this study to further analyze the robustness of the predictive model, enhancing its applicability and reliability in real-world scenarios.

Author Contributions: Conceptualization, methodology, software, analysis, writing, J.B.-H.; methodology review, visualization of Section 3, supervision, M.Á.M.-P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data presented in this study are contained within the article.

Acknowledgments: The authors acknowledge the contributions of the electronic engineering department from Seville University and Airbus Poland for supporting this work with their research facilities and resources.

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

Abbreviations

CIA	Confidentiality, Availability, and Integrity
ENISA	European Union Agency for Cybersecurity
APT	Advanced Persistent Threats
TP	True positives
TN	True negatives
FP	False positives
FN	False negatives
NIST	National Institute of Standards and Technology

References

1. Catteddu, D.; Hogben, G. About ENISA. In *Cloud Computing: Benefits, Risks and Recommendations for Information Security*; ENISA: Attiki, Greece, 2009.
2. Herwan, J.; Misaka, T.; Furukawa, Y.; Ogura, I.; Komoto, H. A proposal for improving production efficiency of existing machining line through a hybrid monitoring and optimisation process. *Int. J. Prod. Res.* **2023**, *61*, 5392–5410. [CrossRef]
3. Atak, A.; Kingma, S. Safety culture in an aircraft maintenance organisation: A view from the inside. *Saf. Sci.* **2011**, *49*, 268–278. [CrossRef]
4. ICAO. *Safety Management Manual, doc 9859*; International Civil Aviation Organization (ICAO): Montreal, QC, Canada, 2013.
5. Barr, L.C.; Newman, R.; Ancel, E.; Belcastro, C.M.; Foster, J.V.; Evans, J.; Klyde, D.H. Preliminary risk assessment for small unmanned aircraft systems. In Proceedings of the 17th AIAA Aviation Technology, Integration, and Operations Conference, Denver, CO, USA, 5–9 June 2017; p. 3272.
6. Jordan, M.I.; Mitchell, T.M. Machine learning: Trends, perspectives, and prospects. *Science* **2015**, *349*, 255–260. [CrossRef] [PubMed]
7. Bozhko, S.; Hill, C.I.; Yang, T. More-Electric Aircraft: Systems and Modeling. In *Wiley Encyclopedia of Electrical and Electronics Engineering*; Wiley: Hoboken, NJ, USA, 1999; pp. 1–31.
8. Casado, R.S.G.R.; Alencar, M.H.; de Almeida, A.T. Combining a multidimensional risk evaluation with an implicit enumeration algorithm to tackle the portfolio selection problem of a natural gas pipeline. *Reliab. Eng. Syst. Saf.* **2022**, *221*, 108332. [CrossRef]
9. Haseeb, M.; Hussain, H.I.; Ślusarczyk, B.; Jermsittiparsert, K. Industry 4.0: A solution towards technology challenges of sustainable business performance. *Soc. Sci.* **2019**, *8*, 154. [CrossRef]
10. Makins, N.; Kirwan, B. *Keeping the Aviation Industry Safe*; EU: Brussels, Belgium, 2020.
11. Jung, B.; Han, I.; Lee, S. Security threats to Internet: A Korean multi-industry investigation. *Inf. Manag.* **2001**, *38*, 487–498. [CrossRef]
12. Su, Q.; Wang, H.; Sun, C.; Li, B.; Li, J. Cyber-attacks against cyber-physical power systems security: State estimation, attacks reconstruction and defense strategy. *Appl. Math. Comput.* **2022**, *413*, 126639. [CrossRef]
13. UK Civil Aviation Authority. *CAP 716: Aviation Maintenance Human Factors (EASA/JAR145 Approved Organisations): Guidance Material on the UK CAA Interpretation of Part 145 Human Factors and Error Management Requirements*; UK Civil Aviation Authority: London, UK, 2006.
14. Bautista-Hernández, J.; Martín-Prats, M.Á. A novel methodology to prevent failures in the manufacturing process using predictive algorithms through machine learning innovations for aerospace. University of Seville: Seville, Spain, 2023; *Manuscript in preparation*.
15. Chen, P.; Desmet, L.; Huygens, C. A study on advanced persistent threats. In Proceedings of the Proceedings 15, Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, 25–26 September 2014; pp. 63–72.
16. Mattei, T.A. Privacy, confidentiality, and security of health care information: Lessons from the recent Wannacry cyberattack. *World Neurosurg.* **2017**, *104*, 972–974. [CrossRef]
17. Bailey, B. *Establishing Space Cybersecurity Policy, Standards, and Risk Management Practices*; Aerospace Corporation: El Segundo, CA, USA, 2020.
18. Kornecki, A.J. Airborne software: Communication and certification. *Scalable Comput. Pract. Exp.* **2008**, *9*, 77–82.
19. Zalewski, J.; Kornecki, A. Trends nad challenges in the aviation systems safety and cybersecurity. *Task Q. Sci. Bull. Acad. Comput. Cent. Gdan.* **2019**, *23*, 159–175.
20. Gallina, B. A model-driven safety certification method for process compliance. In Proceedings of the 2014 IEEE International Symposium on Software Reliability Engineering Workshops, Naples, Italy, 3–6 November 2014; pp. 204–209.
21. Lin, W.; Low, Y.; Chong, Y.; Teo, C. Integrated cyber physical simulation modelling environment for manufacturing 4.0. In Proceedings of the 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, 16–19 December 2018; pp. 1861–1865.
22. Van der Velden, C.; Bil, C.; Yu, X.; Smith, A. An intelligent system for automatic layout routing in aerospace design. *Innov. Syst. Softw. Eng.* **2007**, *3*, 117–128. [CrossRef]
23. Gan, G.; Ma, C.; Wu, J. *Data Clustering: Theory, Algorithms, and Applications*; SIAM: Philadelphia, PA, USA, 2020.

24. Kim, Y.-B.; Jeong, H.-J.; Park, S.-M.; Lim, J.H.; Lee, H.-H. Prediction and Validation of Landing Stability of a Lunar Lander by a Classification Map Based on Touchdown Landing Dynamics' Simulation Considering Soft Ground. *Aerospace* **2021**, *8*, 380. [CrossRef]
25. De Giorgi, M.G.; Strafella, L.; Menga, N.; Ficarella, A. Intelligent Combined Neural Network and Kernel Principal Component Analysis Tool for Engine Health Monitoring Purposes. *Aerospace* **2022**, *9*, 118. [CrossRef]
26. Creado, Y.; Ramteke, V. Active cyber defence strategies and techniques for banks and financial institutions. *J. Financ. Crime* **2020**, *27*, 771–780. [CrossRef]
27. Kovačević, I.; Groš, S.; Slovenec, K. Systematic review and quantitative comparison of cyberattack scenario detection and projection. *Electronics* **2020**, *9*, 1722. [CrossRef]
28. Manadhata, P.K.; Wing, J.M. An attack surface metric. *IEEE Trans. Softw. Eng.* **2010**, *37*, 371–386. [CrossRef]
29. Bordel, B.; Alcarria, R.; Robles, T.; Sánchez-Picot, Á. Stochastic and information theory techniques to reduce large datasets and detect cyberattacks in Ambient Intelligence Environments. *IEEE Access* **2018**, *6*, 34896–34910. [CrossRef]
30. Garcia-Teodoro, P.; Diaz-Verdejo, J.; Maciá-Fernández, G.; Vázquez, E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Comput. Secur.* **2009**, *28*, 18–28. [CrossRef]
31. Li, X.; Liang, X.; Lu, R.; Shen, X.; Lin, X.; Zhu, H. Securing smart grid: Cyber attacks, countermeasures, and challenges. *IEEE Commun. Mag.* **2012**, *50*, 38–45. [CrossRef]
32. Bautista-Hernández, J.; Martín-Prats, M.Á. Monte Carlo Simulation Applicable for Predictive Algorithm Analysis in Aerospace. In Proceedings of the Doctoral Conference on Computing, Electrical and Industrial Systems, Caparica, Portugal, 5–7 July 2023; pp. 243–256.
33. Rao, K.D.; Gopika, V.; Rao, V.S.; Kushwaha, H.; Verma, A.K.; Srividya, A. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. *Reliab. Eng. Syst. Saf.* **2009**, *94*, 872–883.
34. Marseguerra, M.; Zio, E. Monte Carlo estimation of the differential importance measure: Application to the protection system of a nuclear reactor. *Reliab. Eng. Syst. Saf.* **2004**, *86*, 11–24. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.