Failure Mode & Effect Analysis for Improving Data Veracity and Validity

Ana Elsa Hinojosa Herrera
School of Computing & Mathematical Sciences
University of Greenwich
London, United Kingdom
aehinojosa@ieee.org

Chris Walshaw
School of Computing & Mathematical Sciences
University of Greenwich
London, United Kingdom
C.Walshaw@greenwich.ac.uk

Chris Bailey
School of Computing & Mathematical Sciences
University of Greenwich
London, United Kingdom
C.Bailey@greenwich.ac.uk

Chunyan Yin
School of Computing & Mathematical Sciences
University of Greenwich
London, United Kingdom
C.Yin@greenwich.ac.uk

***Abstract* — Failure Mode & Effect Analysis (FMEA) is a method that has been used to improve reliability of products, processes, designs, and software for different applications, including electronics manufacturing. In this paper we propose a modification of this method to extend its application for data veracity and validity improvement. The proposed DVV-FMEA method is based on engineering features and in addition, provides transparency and understandability of the data and its pre-processing, making it reproducible and trustful.**

Keywords—FMEA, Feature Engineering, Big Data, Data Veracity, Data Validity, Electronics Manufacturing

I. INTRODUCTION

Artificial Intelligence (AI) is recognized as one of the grand challenges to put the UK at the head of the data revolution [1]. In addition, it is anticipated that in the data-driven economy, technology will generate information from analysing big datasets.

With regards the definition of big data the authors in [2] described it using 1C for complexity and 11Vs for: Volume, Velocity, Variety, Volatility, Virtual, Visibility, Vendee, Vase, Value, Veracity, and Validity. In this paper we cover the last 2 Vs of the list.

Failure Mode and Effect Analysis (FMEA) is a method that has been used to improve reliability, testability and safety of hardware designs, processes, products and software, for example [3-6]. The authors in [7] listed different types of FMEA as follows: functional, software (SW), test technology, user, process and design. In electronics, hardware (HW) FMEA has been used to improve electronics reliability [4], and in [9] SW FMEA was used to validate embedded real time systems.

In this paper we extended the usage of the FMEA method to improve data veracity and validity. The proposed extension is illustrated with an electronics manufacturing application.

This article is organized as follows. Section II introduces the data veracity and validity concepts and main causes that commonly affect data quality. Section III discusses the FMEA method and its execution. Section IV and V provide the usage of FMEA for data improvement and its application in production testing data, respectively. And finally, Section VI concludes the article.

II. DATA VERACITY AND VALIDITY

Poor data veracity and validity are two relevant big data challenges. Its improvement is relevant because low quality data could generate inaccurate models and unreliable information, resulting in incorrect data-driven decision taking.

A. Data Veracity

Data veracity is the ability to understand the data and the analytical process applied to a dataset. It covers aspects related to confidence in the dataset or data source, for example data integrity, availability, completeness, consistency, and accuracy and in addition, transparency and clarity in the processes used to generate, improve and analyse the dataset [2, 10, 11].

Low data veracity could impact data-based decision taking and confidence about the data. For example, in an electronic production test if a faulty item is detected by a voltage measurement, but the voltage reading is affected by inaccurate results due to the measurement system, hence the detection of faulty devices would not be accurate. Similar results would be obtained if the voltage measurement is not consistent, or if it is not provided, for instance.

Authors in [12] discuss a general list of causes that frequently affect data veracity:

a) Measurement system limits: For example, equipment calibration, human errors, and non standard measurement processes.

b) Limits of features extraction: This could be evaluated by measuring the precision of correctness and completeness.

c) Data integration limits: In real applications it is useful to gather and combine information from different sources, but sometimes it is challenging due to the diversity of data sources or formats. Authors in [13, 14] discuss challenges and problems of data management and integration. The most common challenges are:

- Scale to adapt the scope of data, including size and its generation velocity.
- Optimization of the unstructured data to reduce data inconsistency when having different data sources.
- Query optimization.

- Integration of data coming from legacy systems to new technology.
- Establishing a support system for updates and errors.
- Extract Load Transform process for big data.
- Uncertainty in the source data to be integrated, in the schema mapping, or in the query transformation, for example.

d) Data ambiguity and uncertainty: In addition to the uncertainty due to data integration there are other sources of data ambuiguity, and for instance authors in [15] discuss this data characteristic in soft data. They state that uncertainty is present in soft data because of ambiguities of natural language, uncertainty related to the information source and low relevance of the information with respect other available information. These three aspects could be adapted to other applications.

e) Data falsification and source collusion: In [16] authors model data falsification attack as a constrained optimization problem with two parameters: efficacy and covertness of the attack. The first parameter is related to the degradation in the detection performance, and the second one is the probability that the attacker will not be detected. In the formulation, the attacker would maximize the attack efficacy while controlling its exposure to the defense mechanism.

B. Data Validity

Data validity refers to data worthiness, which may change over time and during the process under study. For example, data generated before relevant changes in the process is not valid to generate models of the current state, [2]. But there are other applications where historical data is still relevant, for example the history of a long-term credit.

The authors in [17] discussed data staleness for information systems where data is frequently updated. This data freshness characteristic is relevant, for example, in data streaming applications where information quickly becomes obsolete.

III. Failure Mode and Effect Analysis

FMEA is a team work effort that extracts and concatenates domain knowledge or engineering features provided by experts to improve a service, product, software, process, etc. It could be seen as a time-consuming method but if it is correctly applied, may be very useful and time saver because it helps to identify failures, generate and monitor an improvement plan to reduce failure modes occurrence or severity, or to increase its detection.

A. Process to Perform a FMEA

The military standard in [18] contains the procedures to perform a FMEA, the main steps are:

1) System identification: The first step is mapping the system, including the components comprised and its relations.

2) List of failure modes generation: This could be generated in a brain-storming meeting including experts in the product or process under improvement.

3) Causes identification: For each failure mode it is expected to identify one or more root causes. Each cause should be scored based on its occurrence.

4) Effect analysis: In this step the effects of the failures are listed, and each of the effects is scored by its severity.

5) Detection mechanism identification: A list with the available mechanisms that helps detecting the failure modes is generated. In addition, each failure mode should have a score of its detectability.

6) Failure mode prioritization: A long list of failure modes is common. In order to improve the efficiency of this method, the list of failure modes should be filtered based on the Risk Priority Number (RPN), which is calculated by multiplying the scores of severity, occurrence, and detection, as in :

$$RPN = Severity \times Occurrence \times Detection \quad (1)$$

7) Process or Product Improvement: Based on the prioritization and resources available, the next step is to generate and execute an improvement plan, which contains actions to improve the reliability of the product/process under analysis. These changes should reduce the score of severity, occurrence, or detection. Nevertheless, severity score is less frequently reduced.

B. Software FMEA

The authors in [3] customise the FMEA for software failure modes analysis for IPO (Input, Process, Output) processes. The differences with the HW FMEA are:

- In step 1 they identify all the software modules and their input variables.
- In step 2 the list of failure modes covers input variables type, and logic of the SW routines. For example, one failure mode is that a Boolean variable has “True” value, when it should be “False”, and vice versa.
- In step 4 the list of failure effects is related to the effects in the outputs of the software routine.

C. Common Errors

Common errors when executing a FMEA and how to mitigate them are discussed in [7]. The most relevant are:

- The FMEA was generated by one person. It should be generated in a team work environment to comprise the knowhow from the application experts. In addition, the FMEA facilitator should have experience.
- The score system is not known by the team or they are modifying it during its usage. The score system should be developed and agreed before the meeting to avoid biases on the ranking.
- The FMEA is filled as a document and requirement but does not add value to the company. The FMEA is an updatable document, which means that it could be revisited as needed. Furthermore, it could be used as a continuous improvement method.

IV. FMEA FOR DATA VERACITY AND VALIDITY

In Section II the coverage of data veracity and data validity was discussed, as well as the importance of these two big data characteristics and their impact on data-based decision taking. In this section we are going to present the Data Veracity and Validity FMEA (DVV-FMEA) process, which is based on the FMEAs of Section III, but modified for data veracity and validity improvement for big datasets.

1) System identification: The modules identified in the process before using datasets for analysis consist of data generation, data storage, data gathering, and data pre-processing (Fig. 1). Nevertheless, in some applications where data is streaming the storage module could be different.

When working on big datasets which comprise a big quantity of variables, we recommend to group them based on engineering feature or data processes similarities.

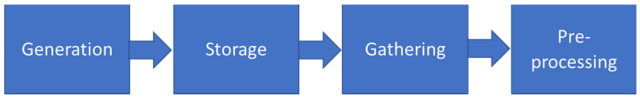

Fig. 1. Data Modules Before Data Analysis

2) List of failure modes generation: We recommend to split the meeting time into the different modules and generate a failure modes list for each of these. The brain-storming meeting(s) should include team members with know-how and expertise in the data process and application.

3) Causes identification: List the causes of failure modes and score them by its occurrence. We recommend to include causes related to:

- Measurement system limits.
- Features extraction limits.
- Data integration limits.
- Data ambiguity and uncertainty.
- Data falsification and source collusion.
- Data staleness.

4) Effect analysis: In this step the effects of the failures are listed, and each of the effects is scored by its severity. We recommend to include impacts to:

- Confidence in the dataset or data source.
- Data integrity.
- Data availability.
- Data completeness.
- Data consistency.
- Data, model or analysis accuracy.
- Execution time or efficiency.
- Ability to replicate results or analysis.
- Data worthiness.

Steps 5 to 7 are the same as in HW FMEA.

We recommend using simple scales for severity, occurrence, and detection scores. For example, a 5 levels scale, such as the Likert scale, which is easy to use when there is no historical data to quantify severity, likelihood or prevention rates (TABLE I).

TABLE I. OCCURRENCE, SEVERITY, AND DETECTION RATING

Rating	*Occurrence*	*Severity*	*Detection*
1	Failure is almost inevitable	Very low or none	Almost certain detection
3	High rate of failure	Low or minor	Remote chance of detection
5	Occasional failures	Moderate or significant	Moderate chance of detection
7	Isolated failures	High	High chance of detection
10	No known failures	Very high or catastrophic	Cannot detect

V. DATA VERACITY & VALIDITY FMEA CASE STUDY

As a case study an opportunity was identified to utilize production test data with the aim of improving the accuracy and efficiency of the testing procedure. More details of this dataset are available in [19].

The proposed DVV-FMEA method was to improve data veracity and validity before doing data analysis.

The experts of the electronic manufacturing and data generation processes took part of the team. The team in charge of building the DVV-FMEA has experience on HW FMEA and the facilitator has experience in this role. In addition, as recommended in Sections III and IV, at the beginning of the first meeting the team agreed to use the scale in TABLE I.

1) System identification: An automated production test sequence called 'p' is run after the assembly of an electronical device for quality assurance purposes. The sequence is comprised by 163 individual tests, an overall test result and other information such as cell number, date, time, temperature, which is useful for analysing the tests conditions. The data generated is stored in a database and in text files for easier accesability. The files are shared in a compressed .zip format, and then the data is pre-processed to tidy it up before using it for data analysis. In this application we are using R scripts for data pre-processing (Fig. 2).

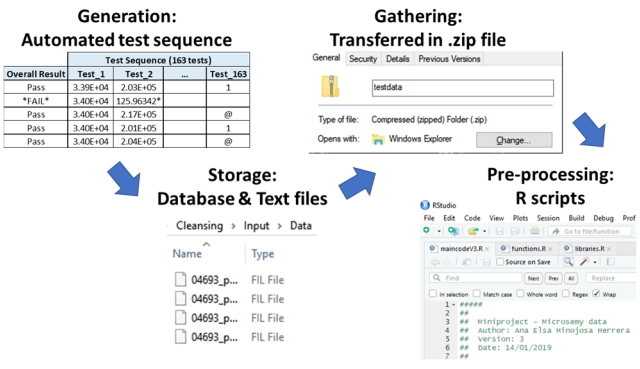

Fig. 2. Production Test Data Modules Before Data Analysis

2) List of failure modes generation: Days before the meeting, the team was asked to think in the data failure modes for each module in (Fig. 2). For each module and relevant variable, group of variables, input or feature was generated

the list of failure modes. Some examples are included in TABLE II.

The failure modes go from incorrect format, incorrect data, ineffective test, inconsistency or not repeatability, for example.

TABLE II. FAILURE MODES

Module	*Input/Variable*	*Failure Mode*
Generation	Overall Result	The overall result is not consistent
Generation	Text File	The file format is not correct
Generation	Test 90	The test was unsuccessful to detect faulty devices
Generation	Test Type	Different to sequence 'p'
Gathering	Dataset	Does not represent the current process conditions
Pre-processing	Data order	The data is not ordered by date-time
Pre-processing	Clean dataset	No clarity of how the data was processed before using it for analysis
Pre-processing	Training/Test datasets	The sampling is not repeatable

3) Causes identification: For each failure mode the root causes were identified and each root cause was scored based on its ocurrence. TABLE III. contains some examples.

The causes of failures comprise human errors in non-automated processes, errors in the software for automated processes, incorrect definition of the test, and missing of standard and robust procedures, for example.

TABLE III. ROOT CAUSES

Input / Variable	*Failure Mode*	*Root Cause*	*Occurrence*
Overall Result	The overall result is not consistent	Human errors in executing the test procedure	7
Text File	The file format is not correct	SW errors in executing the test procedure	1
Test 90	The test was unsuccessful to detect faulty devices	The test does not have a correct upper limit	5
Test Type	Different to sequence 'p'	Files from different test sequences are stored in the same place	5
Dataset	Does not represent the current process conditions	The data is not up to date	5
Data order	The data is not ordered by date-time	The files are not ordered by date-time	10
Clean dataset	No clarity of how the data was pre-processed	No standard process or documentation available	7
Training/ Test datasets	The sampling is not repeatable	No standard process to split the data	10

4) Effect analysis: The effects were identified for each failure mode, and scored by severity (TABLE IV.).

The most common effects for this application are low accuracy of data analysis, missing data to perform analysis, no repeatability of analysis, and low efficiency of the production test procedure for example.

TABLE IV. EFFECT ANALYSIS

Input / Variable	*Failure Mode*	*Failure Effect*	*Severity*
Overall Result	The overall result is not consistent	Low accuracy of analysis	7
Text File	The file format is not correct	Data is not useful for analysis	10
Test 90	The test was unsuccessful to detect faulty devices	Potential test time waste	3
Test Type	Different to sequence 'p'	Low accuracy of analysis	10
Dataset	Does not represent the current process conditions	Low accuracy of analysis	5
Data order	The data is not ordered by date-time	Low accuracy of time series analysis	7
Clean dataset	No clarity of how the data was pre-processed	Results are not repeatable. Low confidence in the dataset and results	7
Training/ Test datasets	The sampling is not repeatable	Analysis or results are not repeatable	7

5) Detection mechanism: For each failure mode the detection mechanisms were identified and scored. Some examples are illustrated in TABLE V.

In the current data process, there are not automated mechanisms that detect the failure modes, but there is information available in the data that could be useful to identify the failure.

TABLE V. DETECTION MECHANISM

Input / Variable	*Failure Mode*	*Detection Mechanism*	*Detection*
Overall Result	The overall result is not consistent	None	10
Text File	The file format is not correct	None	10
Test 90	The test was unsuccessful to detect faulty devices	None	10
Test Type	Different to sequence 'p'	Each record contains the corresponding sequence type	1
Dataset	Does not represent the current process conditions	The date-time is available but not a threshold value	10
Data order	The data is not ordered by date-time	The time stamp is available for each record	1
Clean dataset	No clarity of how the data was pre-processed	Is known that the data pre-processing information is missing	1
Training/ Test datasets	The sampling is not repeatable	Is known that the sampling information is missing	1

6) Failure mode prioritization: The RPN was calculated as in (1). Based on the RPN, the list of +60 failure modes was reduced to 14. Some of them are included in TABLE VI.

The failure mode that has first priority is that the overall test result is not consistent, impacting the effectiveness of the

test but also its efficiency because extra analysis is performed to ensure the good quality of the devices.

In real applications it is very common that the processes change over time, for instance using new raw materials, updates to the design, or improvements to the manufacturing procedures. Hence using out-of-date data to perform data analysis is another relevant failure mode, because the model would not be useful for the current state.

In this application the input variables are the result of individual tests in a sequence that runs in a stop-on-fail scenario. A feature is measured and then compared to upper, lower or both limits to classify faulty devices. The limit definitions are relevant to the accuracy of the tests, but also to its efficiency because in the application one faulty characteristic of the device could be detected by more than one test in the sequence, but the earlier the fault is detected, the shorter the length of the test procedure.

TABLE VI. FAILURE MODE PRIORITIZATION

Input / Variable	*Failure Mode*	*Occ.*	*Sev.*	*Det.*	*RPN*
Overall Result	The overall result is not consistent	7	7	10	490
Text File	The file format is not correct	1	10	10	100
Test 90	The test was unsuccessful to detect faulty devices	5	3	10	150
Test Type	Different to sequence ‘p’	5	10	1	50
Dataset	Does not represent the current process conditions.	5	5	10	250
Data order	The data is not ordered by date-time	10	7	1	70
Clean dataset	No clarity of how the data was pre-processed	7	7	1	49
Training/ Test datasets	The sampling is not repeatable	10	7	1	70

7) Data Process Improvement: Based on the prioritization, some of the actions taken are listed in the TABLE VII.*TABLE VIII.*

Most of the improvements comprise R scripts that pre-process data before its usage for analysis. The scripts detect incorrect data and eliminate it, correct formats, and standardize data pre-process steps to ensure repeatability, consistency, efficiency and confidence. In addition, an analysis of individual test limits was performed to reduce data ambiguity. Here we discuss how the relevance of Test 90 results was improved.

In (Fig. 3) can be seen a strong linear correlation between Test 90 and Test 480. Using 2mA as upper limit for Test 90 there are devices that pass this test but later are identified as faulty devices in Test 480. It was found that all devices that passed Test 480 have Test 90 value ≤ 1.18 mA, and all the devices that fail Test 480 have Test 90 value ≥ 1.40 mA. Hence modifying the upper limit of Test 90 to 1.3 mA this test is able to identify the faulty devices that Test 480 detects. Because Test 480 is after Test 90 in the sequence, by improving Test 90 limits the faulty devices could be identified early and the test procedure execution would be reduced.

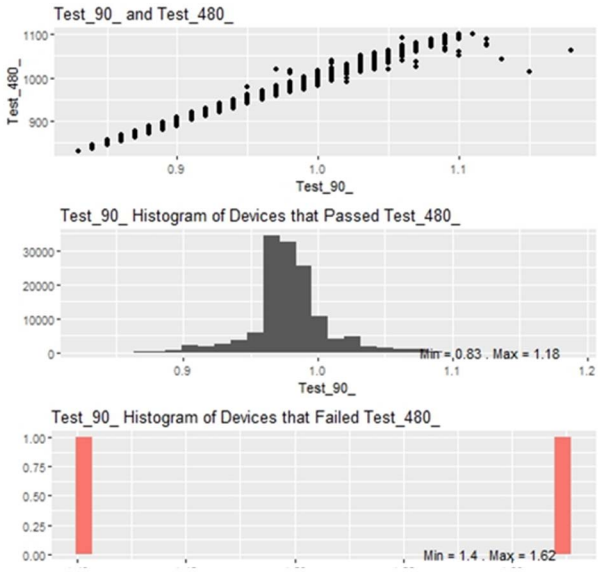

Fig. 3. Production Test Data Modules Before Data Analysis

TABLE VII. DATA PROCESS IMPROVEMENT

Input / Variable	*Failure Mode*	*Actions Taken*
Overall Result	The overall result is not consistent	To write an R script that identifies and eliminates devices that were tested more than one time and the results is different.
Text File	The file format is not correct	To write an R script that identifies and eliminates files with a different format.
Test 10	The test was unsuccessful to detect faulty devices	Using data analysis, to set an upper limit for this test.
Test Type	Different to sequence ‘p’	To write an R script that identifies data from a different test sequence and eliminate it.
Dataset	Does not represent the current process conditions.	Data before 22/03/2016 would not be included, based on the expert’s knowhow about relevant changes in the manufacturing process. To write an R script that identifies data before 22/03/2016 and eliminate it.
Data order	The data is not ordered by date-time	To write an R script that orders the data by time stamp.
Clean dataset	No clarity of how the data was pre-processed	To write an R script that standardize the data pre-processing.
Training/ Test datasets	The sampling is not repeatable	To write an R script that randomly split the data but uses a random seed.

8) RPN recalculation: After implementing the improvements to the data processes, RPN was recalculated.

In TABLE VIII. It can be seen that the risk priority number was reduced by reducing the occurrence of the failure modes or improving the detection mechanisms. For this application a detection and correction of the failure modes was performed from the Generation module, rather than modifying the software of data generation, because of simplicity and efficiency on implementing improvements.

TABLE VIII. FAILURE MODE PRIORITIZATION

Input / Variable	*Failure Mode*	*Occ.*	*Sev.*	*Det.*	*RPN*
Overall Result	The overall result is not consistent	7	7	1	49
Text File	The file format is not correct	10	1	1	10
Test 10	The test was unsuccessful to detect faulty devices	1	3	10	30
Test Type	Different to sequence 'p'	1	10	1	10
Dataset	Does not represent the current process conditions.	1	5	10	50
Data order	The data is not ordered by date-time	1	7	1	7
Clean dataset	No clarity of how the data was pre-processed	1	7	1	7
Training/ Test datasets	The sampling is not repeatable.	1	7	1	7

VI. CONCLUSION

In this paper an extension of the FMEA method was proposed to upgrade data veracity and data validity, two relevant characteristics in the big data paradigm. As discussed, an early identification and mitigation of potential failures in data processes can impact the accuracy of the data-driven models and analysis. Furthermore, investing time and resources to improve data veracity and validity can increase the trust and adoption of the data-based information generated. Another benefit of using DVV-FMEA in early stages of a data analysis project is that as the method is applied, the experts can transfer know-how, data understanding, and business priorities, which are relevant elements of big data and key elements for the success of further analysis.

The DVV-FMEA is presented as a complementary method to improve data veracity and validity, the improvements are driven by feature engineering and expert's know-how rather than on purely data statistics analysis.

The proposed DVV-FMEA method was illustrated using a dataset from production testing of electronical devices. The method applied satisfactory improved the data in terms of veracity and validity. In addition, the improvement of data processing was done efficiently because the prioritization was based on the RPN score. For this application, DVV-FMEA was able to obtain and document know-how of the experts in the electronical manufacturing and data generation processes, which would be useful for further analysis.

ACKNOWLEDGMENT

The authors would like to acknowledge the support from Microsemi Corporation (A Microchip company) for providing the dataset, collaborating with the FMEA elaboration and sharing their domain knowledge with us.

REFERENCES

[1] Department for Business, Energy and Industrial Strategy, Industrial Strategy: Building a Britain fit for the future (November 2017), p 37. Available online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf [accessed 07 February 2019]

[2] R. Patgiri and A. Ahmed, "Big Data: The V's of the Game Changer Paradigm," 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, NSW, 2016, pp. 17-24.

[3] B. Huang, H. Zhang and M. Lu, "Software FMEA approach based on failure modes database," 2009 8th International Conference on Reliability, Maintainability and Safety, Chengdu, 2009, pp. 749-753.

[4] J. Cui, Y. Ren, D. Yang and S. Zeng, "Model based FMEA for electronic products," 2015 First International Conference on Reliability Systems Engineering (ICRSE), Beijing, 2015, pp. 1-6.

[5] G. Yuan, G. Shi, N. Hou and X. Kuang, "The application of FMEA technology in the unstable failure analysis," 2014 10th International Conference on Reliability, Maintainability and Safety (ICRMS), Guangzhou, 2014, pp. 663-665.

[6] H. Zhang, T. Wang, J. Shao, F. Lu and H. Yan, "Advantage analysis of FMEA technique based on EDA simulation," 2015 First International Conference on Reliability Systems Engineering (ICRSE), Beijing, 2015, pp. 1-5.

[7] M. Silverman and J. R. Johnson, "FMEA on FMEA," 2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS), Orlando, FL, 2013, pp. 1-5.

[8] Z. Yuan, Y. Chen and N. Tang, "An integrated method for hardware FMEA of new electronic products," 2016 Prognostics and System Health Management Conference (PHM-Chengdu), Chengdu, 2016, pp. 1-6.

[9] P. L. Goddard, "Validating the safety of embedded real-time control systems using FMEA," Annual Reliability and Maintainability Symposium 1993 Proceedings, Atlanta, GA, USA, 1993, pp. 227-230.

[10] Moyne, J.; Iskandar, J. Big Data Analytics for Smart Manufacturing: Case Studies in Semiconductor Manufacturing. Processes 2017, 5, 39. Available online at: https://doi.org/10.3390/pr5030039

[11] A. F. M. Batista, D. L. da Silva and P. L. P. Correa, "Enabling Data Legitimacy in Data-Driven Projects," 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, 2017, pp. 50-54.

[12] Laure Berti-Equille; Javier Borge-Holthoefer, "Veracity of Data: From Truth Discovery Computation Algorithms to Models of Misinformation Dynamics," in Veracity of Data: From Truth Discovery Computation Algorithms to Models of Misinformation Dynamics , , Morgan & Claypool, 2015, pp.

[13] A. Kadadi, R. Agrawal, C. Nyamful and R. Atiq, "Challenges of data integration and interoperability in big data," 2014 IEEE International Conference on Big Data (Big Data), Washington, DC, 2014, pp. 38-40.

[14] X. HongJu, W. Fei, W. FenMei and W. XiuZhen, "Some key problems of data management in army data engineering based on big data," 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)(, Beijing, 2017, pp. 149-152.

[15] V. Dragos, "Assesment of uncertainty in soft data: A case study" 17th International Conference on Information Fusion (FUSION), Salamanca, 2014, pp. 1-8.

[16] B. Kailkhura, Y. S. Han, S. Brahma and P. K. Varshney, "On covert data falsification attacks on distributed detection systems," 2013 13th International Symposium on Communications and Information Technologies (ISCIT), Surat Thani, 2013, pp. 412-417.

[17] Chayka, O., Palpanas, T., & Bouquet, P. (2012). Defining and Measuring Data-Driven Quality Dimension of Staleness.

[18] Military Standard 1629A, Procedures for Peforming a Failure Mode, Effects and Criticality Analysis, 24 November 1980. Available online at: http://www.barringer1.com/mil_files/MIL-STD-1629RevA.pdf

[19] Hinojosa, A., Stoyanov, S., "Data Driven Predictive Model to Compact a Production stop-on-fail Test Set for an Electronic Device", in Proceedings of the 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE). IEEE Xplore. (In Press)