System Level Risk Analysis for Immunity in Automotive Functional Safety Analyses

Lokesh Devaraj
HORIBA MIRA Limited
Nuneaton, UK
lokesh.devaraj@horiba-mira.com

Alastair R. Ruddle
HORIBA MIRA Limited
Nuneaton, UK
alastair.ruddle@horiba-mira.com

Alistair P. Duffy
De Montfort University
Leicester, UK
apd@dmu.ac.uk

***Abstract*—At present, automotive functional safety and EMC engineering are largely carried out independently. Current EMC regulations aim to avoid unwanted disturbances by setting appropriate immunity threat levels and emission limits. However, with the rapidly evolving technology and complexity of automotive systems, the limits identified in standards may no longer be appropriate. Hence the identification and assessment of EMC-related risks are becoming increasingly necessary. This paper outlines the tools used to support risk analysis for functional safety and presents initial proposals for a graphical method to better align the analysis of EMC risks and functional safety.**

Keywords—automotive, risk analysis, hazard identification, EMC, functional safety.

I. Introduction

In modern vehicles, the electronics and software components already represent around 40% of the total cost for premium models. Current industry trends towards wider powertrain electrification, increasing wireless connectivity and greater driving automation are set to increase this significantly, as well as resulting in much higher levels of system complexity. Furthermore, many electronic systems already provide safety related functions, and efforts to increase automation will expand the reliance on electronic systems to provide safety-related functions. Risk analysis performed before the production of such systems should reduce the risks associated with potential safety hazards in an efficient and cost-effective manner.

Functional safety (FS) aims to address possible hazards caused by the malfunctioning behaviour of electronic and electrical systems. To ensure FS, the automotive industry has been following ISO 26262 [1] for almost a decade. This and similar standards (e.g. IEC 61508 [2]) aim to identify measures to maintain functional safety in the event of malfunctions that may results from hardware failures, software errors etc. In FS, electromagnetic compatibility is highly recommended to verify the robustness of hardware integration under external stresses. Considerable expertise and technical knowledge in the relevant fields are required to study and analyse all of the safety hazards associated with such systems.

Current EMC regulations aim to avoid unwanted disturbances, by setting appropriate immunity threat levels and emission limits. For the automotive industry these are specified in UNECE Regulation 10 [3]. However, with the rapidly evolving technology and complexity of systems, the limits identified in standards are increasingly questionable.

From the FS perspective, therefore, passing an EMC test should provide sufficient confidence that a system will demonstrate robustness and resilience against all the known, unknown, intentional and unintentional EM disturbances present in the system's target environment. In practice, however, this is not true since the EMC test specification and FS technical safety requirements relating to EMC are not usually aligned.

Hence in order to comprehensively identify the potential risks to FS due to EMI sources, a detailed risk analysis of the system needs to be performed, aligning both EMC and FS engineering in order to ensure that the system is resilient against EM disturbances. The system that is the target for this risk analysis here can either be an entire vehicle, or its lower level sub-systems. For instance, an electronic control unit within a vehicle can be taken as a system for the risk analysis.

In section II, the need to perform a risk analysis for EMI with respect to FS is explained and then the requirements, challenges and limitations to develop a complete risk analysis are discussed. In Section III, the practicality of some of the graphical methods mentioned in [4 - 6], such as Bayesian Networks (BN), the Bow-Tie model (BT), and Binary Decision Diagrams (BDD), are discussed. Finally, with a goal to align EMC to aspects of automotive FS, an enhanced graphical approach is proposed in section IV.

II. Risk Analysis: EMC and Functional Safety

A. Need for EMC Risk Analysis

Both emission and immunity tests are required to demonstrate compliance with legislative requirements. Classic EMC engineering employs a rule-based approach, which often involves expertise in this field along with relevant standards [7] to set the test level. So, from the EMC perspective, if tested function is safety related then higher immunity test levels are applied than for less critical functions. However, no specific risk analysis is performed to address issues that could possibly compromise FS and its requirements [8].

In [9], the lack of a detailed risk assessment for EMC is mentioned in the list of shortcomings for reliance on standard immunity tests. A detailed risk analysis could address issues including:

- ageing, corrosion, wear and tear;
- environmental factors such as vibration, temperature and humidity;
- intra-system emission sources;

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 812790 (MSCA-ETN PETER). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: http://etn-peter.eu/.

- possible conflicts between FS technical requirements and EMC mitigation measures.

A combination of these issues [8] can further leave the system vulnerable to EM disturbances, with potential to fail to provide the expected functionality. Hence the current rule-based EMC approach is considered to be insufficient for satisfying all the FS requirements of the system. Nonetheless, immunity testing is highly recommended in Part 5 of [1] (concerning product development at the hardware level), to demonstrate desired level of robustness to external EM threats under the specified environmental conditions.

B. Risk Analysis for FS

In the concept phase (see part 4 of [1]), hazard and risk analysis (HARA) is performed for an item to derive the safety goals. For the first step in the risk analysis, i.e. the hazard identification, a high-level functional model of the system is constructed (the "item definition"). Those functions that impact on the safety of the stakeholders (i.e. vehicle occupants and other road users in the automotive case) are then identified by constructing a "black box" model. Potential malfunctions are then assessed in terms of their impact on the stakeholders (i.e. the "severity" of the hazard).

The next step is to establish the possible causes of such failures using trees, graphs, tables and other techniques like HAZOP [10], as well as DELPHI and SWIFT [9]. From this it is possible to estimate the likelihood of the hazard occurring. In the automotive context, the likelihood is represented in terms of the "exposure" to the hazard and the "controllability" of the situation for a typical driver. The risk is then determined from the severity and the likelihood.

The notions of risk analysis and risk management are often confused However, risk management also includes risk mitigation, verification, validation and decision making within its scope. According to [11, 12], given an intended use of a device, risk analysis for this device will involve, 1) identification of the hazards and 2) classification of the associated risk(s) for relevant hazardous situations. Assessment of the risks can be qualitative, quantitative or a combination of both. All elements of a system that provide safety related functions, as well as any sub-elements that they depend upon, are within the scope of the risk analysis.

Contemporary FS standards (e.g. IEC 61058, ISO 26262 for road vehicles, and IEC 60601 [13] and ISO 14971 [14] for medical devices) specify *what* needs to be accomplished to ensure freedom from unacceptable risks; but h*ow* it is achieved is not specified, because of the diversity of the systems considered. Hence, a safety analyst is free to utilize any desired tools for their analysis. In Section III, the typical tools that are used to perform a risk analysis for a system is listed. References [15, 16] are good examples for demonstrating some risk analysis methods applied at a system level to mitigate intentional EMI threats.

In FS, the failure mode and effect analysis (FMEA [17]) is a popular tool that has been used for hazard and risk assessment (HARA). FMEA is an inductive tool which has been traditionally used in many industries, especially in the automotive industry to explore the effects or consequences of failures modes occurring in a system. This analytical technique is applied using simple worksheets or tables. The steps for HARA in FS are described using the flowchart shown in the Fig. 1.

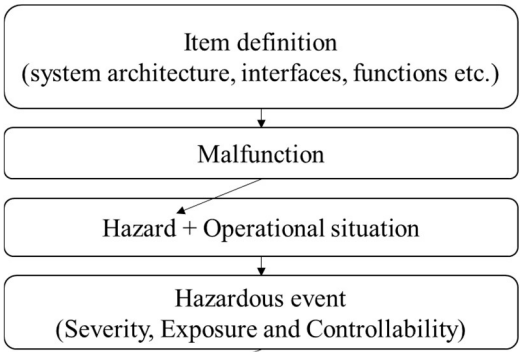

Fig. 1. Flowchart to explain the concept phase risk assessment in ISO 26262.

Furthermore, the hardware and software technical requirements for the mitigation measures needed to reduce significant risks to tolerable levels are given based on the FS risk assessment. These requirements are derived using tools such as fault tree analysis which can be used to identify the causes of a malfunction.

Although EMI is often identified as one of the causes for a possible malfunction, it is commonly assumed to been effectively mitigated by passing the standard immunity tests. Thus, any additional risk associated with EMC is often not adequately considered.

C. Rule-Based to Risk-Based EM Approach

The immunity to electromagnetic disturbances is verified by performing standard immunity tests. These tests are usually carried out to ensure the safe operation of the system in the presence of external EM stresses. However, these tests do not guarantee that the item is free from all possible errors; only that for the given test condition there are no identified functional failures.

Individual equipment testing and the EMC verification for the entire system after integration alone does not assure the safety and security during its entire lifecycle. For e.g. any vehicle on a typical road environment considered as a system includes its driver, passengers, their possessed electronic gadgets, infrastructures in proximity emitting EM fields, other road users etc. In this case, several unknown EM sources and their modulations which were not tested can increase the EM stress levels leading to a malfunction of the safety related element(s) of the system.

The safety of the system is depicted in Fig. 2, using the notions of EM "stress" and "strength" (i.e. immunity) levels. In these diagrams, the overlap of stress and strength circles represent a possible malfunction and the gap between them represents safety. The strength circle depicts all attributes that could possibly reduce the susceptibility of the element (e.g., higher EM immunity threshold, effective shielding, filters, grounding etc.). The stress circle represents all factors that contribute to the EM threat to the element in the system (i.e. EM field strength, frequency, modulation, illumination direction, ageing effects etc.), which could lead to possible malfunction and thus a hazard.

The main reasons for developing a risk-based approach are to prioritize risks and to identify the work needed to assure their mitigation to acceptable risk levels, saving costs from tedious testing over the entire EM spectrum and their modulation and to prevent over engineering.

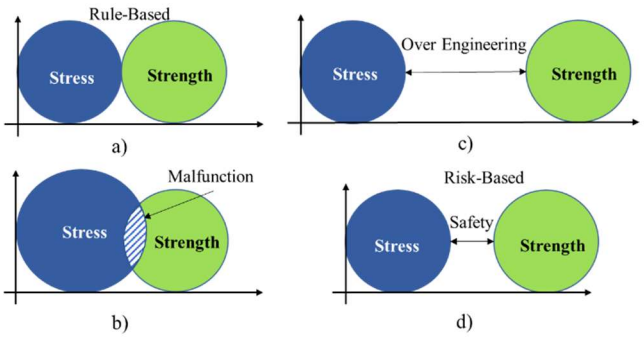

Fig. 2. Pictorial representation of the need for risk-analysis to change the current rule-based approach to a risk-based approach for: a) current rule-based approach; b) emerging malfunctions, if EM sources exceed the EM strength level despite current EMC tests; c) overengineering, if robustness targeting worst-case scenario for the system/component; and d) risk-based approach for adequate safety.

In many cases, the target environment in which the system is to be operated is, to a certain degree, known. However, the susceptibility of the system to all possible or unknown EM disturbances present in the environment is practically impossible to be considered fully. In other words, a risk analysis is necessary to be performed to ensure that all feasible measures were taken to keep the system within the intended operational condition. Methods to include uncertainties in tolerance levels of the system to varying EM environment, hazards and evolving cyber-attacks in the risk analysis can also be considered.

III. Graphical Tools and Techniques

In [9], it is recommended to employ at least one deductive method (bottom-up) and one inductive (top-down) method to improve the coverage of the hazard and hazard assessment. Fault Tree Analysis (FTA [18]) and Event Tree Analysis (ETA [19]) are examples of deductive and inductive methods, respectively.

FTA starts with an undesired top event and propagates lower to find all possible causes for the occurrence of the event as shown in Fig. 3. Using the Boolean logic ETA, an initiating event (e.g. due to EMI) can be traced forward, as shown in Fig. 4, to the consequences it will bring to the system. Generally, the inductive and deductive tools like FTA and ETA are also used to help assess the risks, by estimating the probability of occurrence or by using the statistical data associated with the identified causes and consequences.

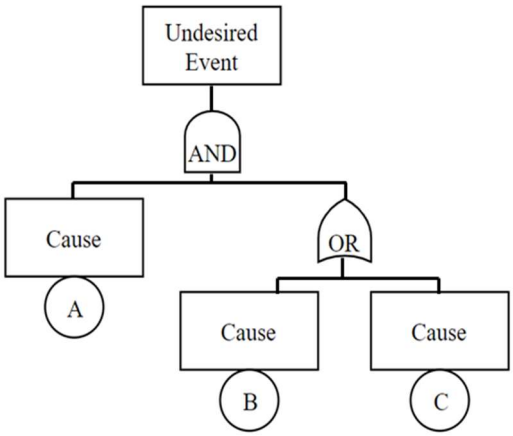

Fig. 3. Top-down (deductive) approach of FTA.

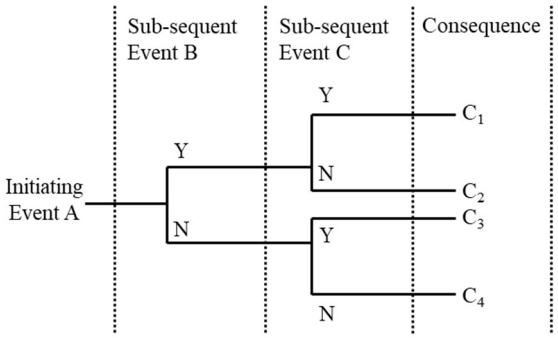

Fig. 4. Bottom-up (inductive) approach of ETA.

To perform a risk analysis using trees, the system under consideration must be defined beforehand. In the real world, the boundaries of a system from the design phase through the entire lifecycle are not necessarily fixed, paticularly for systems such as vehicles, which may be in operation for many years. In addition, to include the effects of unknown EM disturbances and the risk associated with it, trees alone are not sufficient.

Graphs offer the advantage that they can be more effectively used to represent complex networks, which is very much essential for the risk analysis of large systems. In general, a graph consists of several nodes that are interconnected by directed edges to form a network. Hence trees are actually a subset of graphs that are unidirected and acyclic. The trees, being a subset of graphs, can be converted to a graphical representation. An example of such conversion is shown in [20], in which a logical decision tree is converted to a graph called a binary decision diagram (BDD). However, systems like road vehicles have more than one root cause for safety related malfunction, hence tools such as BDD, which uses Boolean logic, have limitations for the current risk analysis.

The Bow-Tie (BT) model mentioned in [6] is one such graphical tool which is be adapted to combine FT and ET from a common pivot node representing an undesired event as shown in Fig. 5. The undesired event for example, can be an item malfunction in FS. This tool is used in risk analysis to determine both cause and consequences for a single event. However, the use of this tool is also limited for complex systems.

A Bayesian Network (BN) is a similar graphical tool that has been widely used in the field of risk analysis and decision making at system level [6, 16, 21, 22]. BN is a directed acyclic graph, in which the nodes can represent any random variable and the arrows inter-connecting these nodes specify the dependence in a probabilistic, deterministic or functional sense. The Boolean relationships used in FT, like AND and OR, can be represented in a BN by assigning a conditional probability distribution table to the node. In [6], this is demonstrated with examples. Further, the general requirements and limitations of Bayesian Networks for risk analysis are described in [23].

Fig. 5. Bow-Tie Model representation.

The BN has a limitation that the nodes connected should have a conditional probability relationship. Nevertheless, the tools like FTA and ETA used in FS can be easily converted for the reuse during risk analysis. Other tools like Petri nets, reliability diagrams, Monte-Carlo simulation, Markov chain, check lists, worksheets, tables etc. (see [9]) have also been used for risk analysis but are not discussed in this paper.

IV. Simple Case Study

Functional safety requiring EMC testing arises if EM disturbances are identified to be the cause for an item malfunction. To demonstrate this, an assumption of an item (sub-system/ECU) to be present within a vehicle (system) is made. The item consists of 1) the pressure sensor (C1), to detect the pressure applied by the driver for vehicle acceleration, 2) the power controller (C2), to control the rotation speed of the motor based on the C1 input, and 3) the internal and external interfaces (denoted by I_1–I_4). In practice, all functions, architecture, interfaces etc., of such an item and its elements should be recorded in the item definition. For simplicity, a single function of the item is taken to derive its associated malfunction, hazard, operational situation and hazardous event (HE) (see Fig. 6). For the HE in Fig. 6, the cause and consequences can be represented using a BT model, as shown in Fig. 7.

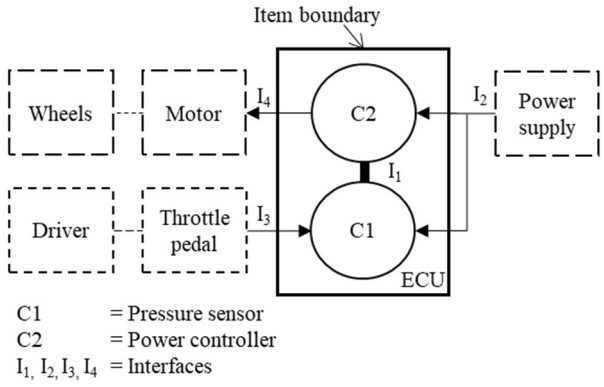

Fig. 6. A simple example to demonstrate the concept phase of FS

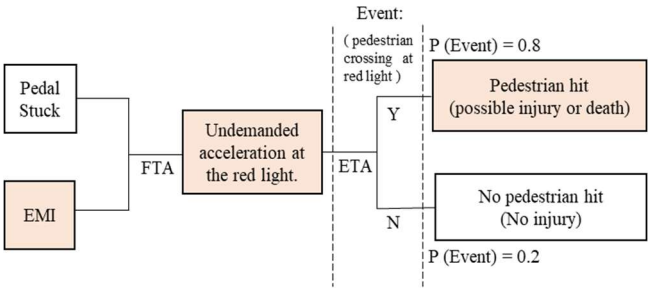

Fig. 7. Hazard analysis using BT model to identify the cause and onsequences of an hazardous event.

However, such graphs are much more complex when multiple operational situations and relevant causes and consequences are associated with the HE. Any cause (e.g. EMI) leading to highly severe and likely consequences needs to be prevented or mitigated to achieve tolerable risks. In Fig. 7, EMI is considered as one of the causes for the HE, which may lead to severe consequences such as injury or death. The FS requirement, in this particular example to prevent the HE will be to subject this safety-related item for EMC testing, with specific EM fields that are found in the operational situation considered. If the specified EMC tests are passed, the hazards due to EMI as a potential cause are considered as being negligible.

However, the risks due to issues listed in Section II.A are not addressed. For example, the effective shielding of the item during EMC testing may degrade due to ageing, posing a potential risk during the operational lifecycle. So, sufficient confidence can only be obtained by performing a comprehensive risk analysis. Alternative solutions to have higher degree of confidence, like increasing the number of tests with varied frequency, amplitude and modulations, or by repeating the tests again would require more time and be very expensive.

V. Proposed Approach for Immunity Risk Analysis

No single tool or method is able to analyse an entire system without limitations. However, the tools currently used in industry (FTA, FMEA, ETA, BN etc.) can be utilized and adapted to carry out risk analysis and to take risk-based decisions for a system. Data available from the hazard and risk analysis done for FS and the tools that were used to identify and classify the associated risk metrics can be reused to construct a new graphical model. A graph for the item used in the case study is shown in Fig. 8, where,

- Nodes are used to represent all the elements composing the system considered. All interfaces, including wired and wireless communication links as well as power supply cables, are represented as separate nodes.
- Edges are used to represent functional dependencies between the attached nodes. Mutually exclusive nodes should not be connected by edges, facilitating the identification of cascaded failures.

This model or network [23] has the elements and their functional dependencies mapped systematically with nodes and edges, respectively.

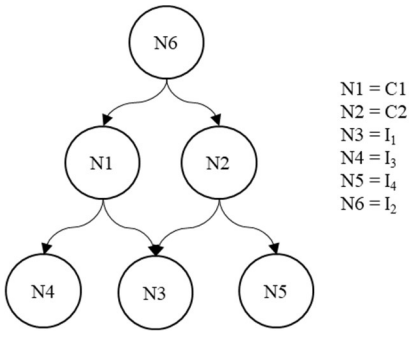

Fig. 8. Graphical representation of the elements and functionalities of the item (ECU) considered in Fig. 6.

For a comprehensive risk analysis several graphs, each representing an item/component within the system, can be connected using edges to complete the system network. For instance, a separate graph representing another item within the system can be connected to N6 of graph shown in Fig. 8, if they have a common power supply. To analyse the system for risks, the nodes in the graph shall be assigned with attributes such as a threshold value for the probability of malfunction, above which the system level risk is greater than tolerable.

Initially with item passing the EMC tests, the probability of malfunction due to EMI, *P(MF)*, is assigned a value zero and the presumed probabilistic threshold value, *T* assigned to each node of the system network will be a value between 0 and 1. Stress factors (like ageing, intra-system emissions, untested EM fields etc.) will increase the value of *P(MF)* to a new value. For the system to have a low risk level against malfunction due EMI, the newly determined probability of malfunction due to the additional stress, $P_{new}(MF)$, when propagated through the network should be less than value of *T* that has been assigned to each node in the graph. By doing this, EM risk due to vulnerability of one or multiple nodes present in the system network can be identified and further analysed to achieve tolerable risk levels.

VI. Conclusion

Several tools are available to support the development of comprehensive risk analyses. However, they all have limitations when it comes to specific applications. This paper proposes a modified graphical approach to improve the analysis of functional safety risks due to EM aspects that are not currently considered in FS. Further work will involve, 1) identifying efficient ways to determine the probability of malfunction due to EM stress and the probabilistic threshold value, 2) designing an application specific software tool to enable risk analysis for addressing EM safety risks.

References

[1] BS ISO 26262:2018: “Road vehicles — Functional safety”, British Standards Institute, 12 parts, Dec. 2018.

[2] BS ISO 61508:2010: “Functional safety of electrical/ electronic/programmable electronic safety-related systems”, British Standards Institute, 7 parts, June 2010.

[3] UNECE Reg10:2012, “Regulation No. 10 – Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility”, Add. 9, Rev. 4, 06/03/2012

[4] Aven, Quantitative Risk Assessment: The Scientific Platform. Cambridge, UK: Cambridge University Press, 2011.

[5] P.V. Varde and M.G. Pecht, Risk-Based Engineering – An Integrated Approach to Complex Systems – Special Reference to Nuclear Plants, Springer Series in Reliability Engineering, SingaporeSpringer, ISBN 978-981-13-0090-5, 2018.

[6] N. Khakzad, F. Khan and P. Amyotte, "Quantitative risk analysis of offshore drilling operations: A Bayesian approach," Safety Science, vol. 57, pp. 108–117, 2013.

[7] BS EN 61000-1-2:2016: Electromagnetic compatibility (EMC). General. Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena," British Standards Institute, Sept. 2016.

[8] K. Armstrong, "EMC testing to achieve functional safety: the IET's new guide," EE-Evaluation Engineering, vol. 49, (1), pp. 42, 2010.

[9] IET, “Guide on EMC for Functional Safety”, 2008. Online: www.theiet.org/factfiles/emc/emc-factfile.cfm.

[10] BS EN 61882:2016, “Hazard and operability studies (HAZOP studies). Application guide”, British Standards Institute, June 2016.

[11] K. Borgeest, EMC and Functional Safety of Automotive Electronics, London, UK: IET, 2018.

[12] D. Flood, F. Mc Caffery, V. Casey, R. McKeever, and R. Peter, , “A roadmap to ISO 14971 implementation,” J. Softw. Process Evol., in press.

[13] IEC 60601-1-2:2014, “Medical electrical equipment – Part 1–2: General requirements for basic safety and essential performance – Collateral Standard: Electromagnetic disturbances – Requirements and tests”, 4th Edition, February 2014.

[14] BS EN ISO 14971:2019, Medical devices. Application of risk management to medical devices”, British Standards Institute, Dec. 2019.

[15] E. Genender, H. Garbe and F. Sabath, "Probabilistic risk analysis technique of intentional electromagnetic interference at system level," IEEE Trans. EMC, vol. 56, (1), pp. 200–207, 2014.

[16] C. Mao and F. Canavero, "System-level vulnerability assessment for EME: from Fault Tree Analysis to Bayesian Networks-Part I: Methodology framework," IEEE Trans. EMC, vol. 58, (1), pp. 180–187, 2016.

[17] BS EN 60812:2006, “Analysis techniques for system reliability. Procedure for failure mode and effects analysis (FMEA)”, British Standards Institute, June 2006.

[18] BS EN 61025:2006 “Fault tree analysis (FTA)”, British Standards Institute, Sept. 2007.

[19] BS EN 62502:2011, “Analysis techniques for dependability. Event tree analysis (ETA)”, British Standards Institute, June 2011

[20] P. Marugán, F.P. García Márquez and B. Lev, "Optimal decision-making via binary decision diagrams for investments under a risky environment," Int. J. Prod. Res., vol. 55, (18), pp. 5271–5286, 2017.

[21] M.K. Jha and A. Keele, "Using Dynamic Bayesian Networks for Investigating the Impacts of Extreme Events, Bayesian Networks," Wichian Premchaiswadi, IntechOpen, 2012.

[22] K.-J. Li , Y.-Z. Xie, Y.-H. Chen, Y. Zhou and Y.-C. Hui, "Bayesian inference for susceptibility of electronics to transient electromagnetic disturbances with failure mechanism Consideration," IEEE Trans. EMC, in press.

[23] P. Trucco and M.C. Leva, "BN Applications in Operational Risk Analysis: Scope, Limitations and Methodological Requirements", IntechOpen, 2012.