Safety Active Barriers Considering Different Scenarios of Faults in Modern Production Systems

Jeferson A.L. de Souza(✉), Diolino J. Santos Fo, Reinaldo Squillante Jr., Fabricio Junqueira, Paulo E. Miyagi, and Jose Reinaldo Silva

University of São Paulo, São Paulo, Brazil
{jeferson.souza,diolinos,reinaldo.squillante,fabri, pemiyagi,reinaldo}@usp.br

Abstract. Modern production systems, inserted in a context of high competitiveness, in accordance with policies of sustainability and people protection, as well as being integrated with other (smart) systems, makes complexity an inherent factor in any modern production system. Complexity is reflected in hardware, software and labour qualification for both the design and operation of such systems, resulting in the impossibility of (i) the prediction of all achievable states; (ii) the design of all integrated systems, (iii) non-existence of hardware faults and (iv) absence of human operating errors. Depending on the productive process under analysis, different scenarios, considering the combination of operational errors, faults in field components or even faults in system integration can lead to situations of serious risks for the environment, man and facilities. The bow-tie technique can elicit different scenarios of occurrence of faults and their dynamic evolution, by the results of other risk analysis techniques, such as FMEA, FTA and ETA. The concept of Safety Instrumented Systems, along with the concept of Safety Barriers could be a solution for these problems. This paper proposes the use of Petri nets for formal modeling and the generation of control algorithms, by the simplification of several scenarios of faults fault scenarios listed by a team in the process.

Keywords: Modern production systems · Safety Instrumented Systems · Risk analysis · Faults · Scenarios of faults · Safety barriers · Petri nets

1 Introduction

In this first decade of the century XXI many studies have indicated that automation processes are undergoing transformations that have been strongly influenced by the advance of technology and computing resources, becoming increasingly complex due to their dynamic and needed to address issues such as global market competitive production and technology used, among other factors (Chen and Dai 2004; Santos Filho et al. 2000; Wu et al. 2008). Given this new scenario, industrial processes and their control are becoming more and more complex. Additionally, organizations have

L.M. Camarinha-Matos et al. (Eds.): DoCEIS 2017, IFIP AICT 499, pp. 154–164, 2017.
DOI: 10.1007/978-3-319-56077-9_14

focused on policies to achieve and to demonstrate people's safety and health, environmental management system, and the capability in risk management.

In a globalized and competitive environment in which organizations are inserted, it is essential to adopt strategic plans and operational practices that ensure the ability to adapt rapidly and consequent change of the systems-productive but hitherto conceived. The expectation is that in addition to result in a process with effective cost reduction, high product quality and flexibility of production lines, and reduction of new products and delivery development times (Santos Filho et al. 2000; Chen and Dai 2004; Wu et al. 2008), also causes the reduction of environmental impacts of the process. The results of this new scenario are Productive Systems (SPs) that perform highly complex processes (Sampaio 2011; Ferreira et al. 2014) that might not be achievable by conventional production methods (Mazzolini et al. 2011). Because of this complexity inherent in any modern production system, some states, though undesirable, can be achieved, it could be mentioned: the fault states of components, design flaws, or operational errors, including intentional, and environmental events that involve the system. Such occurrences could result, depending on the complexity of the SPs, serious risks to the physical integrity of people, the environment and economic losses resulting from damage to the equipment itself (Sallak et al. 2008). Although many studies have been presented both for diagnosis and for the treatment of faults (Morales et al. 2007; Ru and Hadjicostis 2008; Wang et al. 2008; Zhang and Jiang 2008; Summers and Raney 1999; Sallak et al. 2008; Squillante Jr. et al. 2013; Souza et al. 2014; Souza et al. 2016; Peters et al. 2016) accidents continue to occur. In this context, according to specialists, the use of Safety Instrumented Systems - SIS is a solution to this problem in that aims to reduce the risks associated with SPs by successive risk reduction layers, which can be implemented by safety control systems that operate independently of the Basic System Process Control - BPCS. In general, the role of a SIS is to monitor through security sensors, critical events in the industrial process and indicate alarms or perform preset actions through security actuators, for the prevention of accidents or mitigation of the consequences generated by these events (Goble 1998). SIS are referenced in standards such as IEC 61508 and IEC 61511, that lists the performance requirements and the life cycle for a design of a SIS. However, the standards make no mention of methods for SIS implementation. Another concept that promotes de risk reduction of a SP is that of safety barriers. Safety barriers are defined as any physical or non-physical means used in order to prevent, control or mitigate undesirable events or accidents (Sklet 2006). It may be from human action to a complex logical system. This paper proposes a method for the implementation of SIS, in reference to IEC 61508 and IEC 61511, considering different scenarios of faults, making use of safety barriers both to prevent and to mitigate faults. By associating the occurrence of a fault to an event, and by the fact a fault promotes the change of the process state, scenarios can be modeled by Petri nets (PN). Several isolated models are obtained, representing a great difficulty to implement the control algorithm. The hypothesis lies in the interrelationship of the models that represent the different scenarios of faults, which can result in a considerable simplification both for the good properties verification and formal validation of the algorithm, as well as for control codes transcription. This paper is organized as follows: Sect. 2 presents the Relationship to Smart Systems, Sect. 3 the Fundamental Concepts of some Risk Analysis techniques, Petri nets and Fuzzy Logic.

Section 4 presents the Proposal with partial results, obtained by the application of the method in a gas compression station. Finally, Sect. 5 presents the Conclusion and References.

2 Relationship to Smart Systems

This work has close relationship with smart systems as it proposes a safety control system considering different scenarios of faults, by the use of safety barriers, in reference to IEC 61508/IEC 61511. The work proposes that such barriers be fully implemented by programmable control systems, rather than passive physical barriers or exercised by human activity. The barriers interrelationship characterizes such a system as a "smart system", in line with the event proposal, contributing to the reduction of the inherent risk, presented in any modern production system, with the objective of protecting man, the environment and facilities.

3 Fundamental Concepts

3.1 Risk Analysis Techniques

This section introduces the fundamental concepts of some risk analysis techniques, such as FMEA, FTA, ETA HAZOP and the Bow Tie Diagram. The FMEA technique, described in IEC 60812 (IEC 2006), consists of a detailed and systematic study of possible failures of the components of a system. The failure modes of each component are identified, and a severity level is associated with its effect, and assess the likelihood of their occurrence. The FMEA also discusses actions to prevent, eliminate, mitigate and control the causes and consequences of failures. (Lewis 1995). Another technique used is the Fault Tree - FTA, deductive reasoning methodology described in IEC 61025 (2008) that part of a top event, which is the occurrence of a specific fault in a system, which aims to determine the relationship fault logic components and/or operational human errors that may be associated with the occurrence of the top event. The analysis is done from the construction of a logical tree. In this way, one obtains a graph which can be used to identify all possible causes for the occurrence of a fault (Modarres et al. 2010). The graph enables an analysis of the "top-down", which results in understanding how the event occurred. In the analysis "bottom-up" it has been "why" of the event. The advantage of FTA on the FMEA is that one can have a combination of several elements or multiple failure modes, the graph connected by logic elements such as "and" and "or". The study of operability and risks, or HAZOP (HAZard and OPerability studies) defined in IEC 61882 (IEC 2001) was developed for efficient and detailed examination of the variables of a process having a strong resemblance to the FMEA. Hazop identifies the ways in which the process equipment may fail or be improperly operated. It is developed by a multidisciplinary team, being guided by the application of specific words - words guide - each process variable. Thus, to generate the deviation of operational standards, which are analyzed in relation to their causes and consequences. Event trees (DIN 25419 1985-11) are frequently used in the analysis of sequences of events, including human

activities, that can lead to disasters or undesirable events. The activity is sometimes called cause consequence analysis, and is used more frequently in safety studies. In this analysis, a basic event, resulting from a specific failure of a human equipment or error, called the initiating event, is used to determine one or more subsequent states of possible faults (Rausand 2011; Villemeur 1992). In this way, the ETA considers the action to be taken by the operator or the process response to the initial event. As in FTA, the study is performed through a tree, starting from the initiating event, in order to quantify the probabilities of failure in the system. Explore responses through a single initiating event and lays a path for assessing probabilities of the outcomes and overall system analysis. It may be applied to a system early in the design process to identify potential issues that may arise rather than correcting the issues after they occur. A widely technique for modeling complete accident scenarios, based on the identification of the main "causes" and "consequences", given a top event (TE) or risk. Basically, the principle of this technique is to construct a tree type, called a bow-tie diagram, due to its special shape (Badreddine and Ben Amor 2010). The bow-tie diagram is based on two parts, as shown in Fig. 1. The left side of the diagram represents the fault tree (FT) that defines all the possible combinational logical relationships between the causes of the TE. In addition, the right side of the diagram represents the event tree (ET) that defines all the possible undesired consequences of TE.

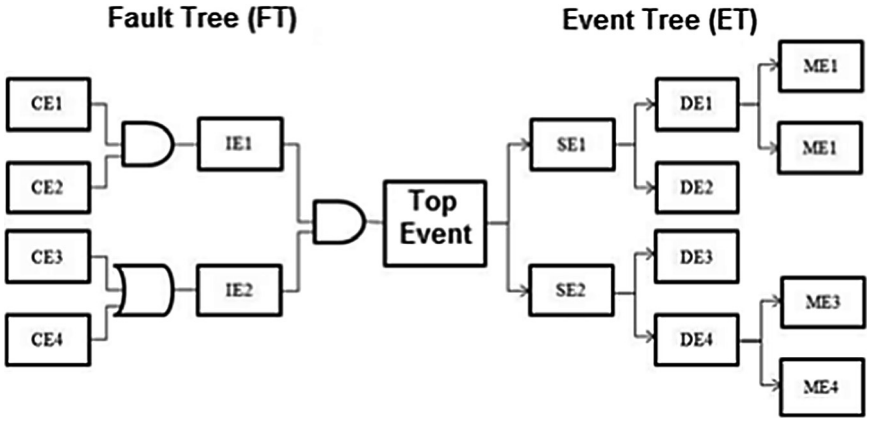

Fig. 1. Example of a bow-tie diagram

3.2 Petri Nets

Petri net (PN) as a graphical tool and mathematics provides a uniform way for model, analysis and design of Discrete Event Systems - SEDs (Adam et al. 1998; Nassar et al. 2008; Zurawski and Zhou 1994), being effective as a description of technical and specification processes (Hamadi and Benatallah 2003; Morales et al. 2007). It provides a representation that can be used both as a conceptual model and functional model of a system that can analyze and validate the operation of the system at each stage of its

development cycle. The PN can also be used as a design tool, allowing for easy interpretation and identification of processes and their dynamic behavior and/or systems being modeled (Nassar et al. 2008). The models based on NP can be used for qualitative and quantitative assessment involving the analysis of the behavioral properties and performance measure, respectively. Moreover, with the development of software simulators (Zurawski and Zhou 1994), has provided tools for editing and analysis of these models. Enables the representation of the system dynamics and structure at various levels of abstraction, according to the with-complexity system (Nassar et al. 2008). It is able to model synchronization process, the occurrence of asynchronous events, competitors and conflict operations, or resource sharing (Adam et al. 1998; Nassar et al. 2008).

3.3 Fuzzy Logic

Fuzzy logic is becoming useful in modeling of nonlinear systems, or when the use of differential equations becomes too complex, or even in processes whose knowledge of the dynamic behaviour is not yet fully understood. Fuzzy systems are based on the human knowledge or a set of rules that are designed to mimic human reasoning in control decisions. Questions like "If … (conditional) So … (consequent)" are formulated process experts in analysis, and control actions are defined from the responses, and in its May-ria, systems multiple inputs to a single output. All rules are processed in parallel, with the consequent be active with its degree of membership in the system output. Unlike Boolean logic, fuzzy numbers are contained in a closed interval 0 to 1, and may take values within this range. The use of fuzzy logic in CPs is referenced in the IEC61131-7 standard, which deals with the conversion of fuzzy logic in implementable language in commercial CPs.

4 Proposal

The proposed method is outlined in the flowchart shown in Fig. 2, and the steps for its implementation, described in the following items 4.1 to 4.5, are built from knowledge of independent experts and/or database obtained from field experiments, record of past operation or computer simulation of plant under study.

To illustrate the proposed method, some results were obtained from a natural gas compression station.

4.1 FMEA – Determination of the Critical Elements

To determine the critical elements of the process under study FMEA is applied as a first evaluation insofar as it associates a level of severity to the occurrence of fault in an isolated and component-centered way, and proposes actions to prevent and mitigate the effects. Faulted components that pose risks to operators, the environment and equipment, besides violating the legislation, receives maximum severity. In the proposed

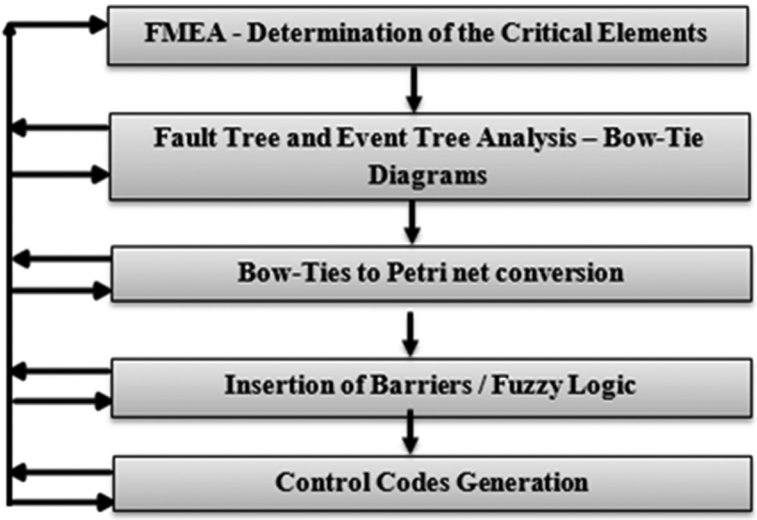

Fig. 2. Flowchart of steps of the proposed method.

method, it is part of the FMEA to associate sensors to detect the occurrence of fault of the critical element, and criteria to confirm the occurrence of failure, such as 2003 voting criteria. Based on the results, a cause/effect matrix is elaborated, in which the lines represent the initializing events of the sensors associated to the occurrence of faults and columns the respective actions proposed for prevention and/or mitigation. Such information is obtained with the assistance of a team of experts in the process under study, according to IEC 61508. Based on the concept of SIS, the Safety Instrumented Functions (SIFs) are listed. An example of cause-effect matrix is presented in Table 1.

Table 1. Example of a cause-effect matrix of a SIF

SIF1 / CAUSES	EFFECTS: STOP TCA	STOP TCB	STOP TCC	STOP TCD	CLOSE XV -001	CLOSE XV -017	CLOSE XV -019	CLOSE XV -020	CLOSE XV -003	CLOSE XV -018	CLOSE XV -005	CLOSE XV -022
PSHH A	X	X			X	X	X		X		X	
PSHH B		X	X		X			X	X	X	X	
PSHH C			X	X	X				X		X	X

4.2 Fault Tree and Event Tree Analysis – Bow Tie Diagrams

The next step consists in analyzing the logical combination of events (or faults) that can lead to the occurrence of a critical fault (or top event), making use of the FT technique. For each top event, the ETA technique represents the evolution of events that follow the occurrence of the top event and which can lead to a catastrophe. The junction of the FTA with the ETA results in the bow-tie diagram, which in turn can be understood as being a fault scenario. The results obtained in the cause-effect matrix certainly aid in the design of bow-ties.

4.3 Bow Ties to Petri Net Conversion

The results from the previous step are isolated bow-tie diagrams, representing scenarios of faults. By associating the occurrence of a fault to an event, and the evolution of the fault to a succession of states, the bow-tie diagrams can be modeled by Petri nets, in which the editing, verification and formal validation properties of the model can be edited and simulated by software, such as PIPE2. An example of a bow-tie diagram obtained in the application example is shown in Fig. 3.

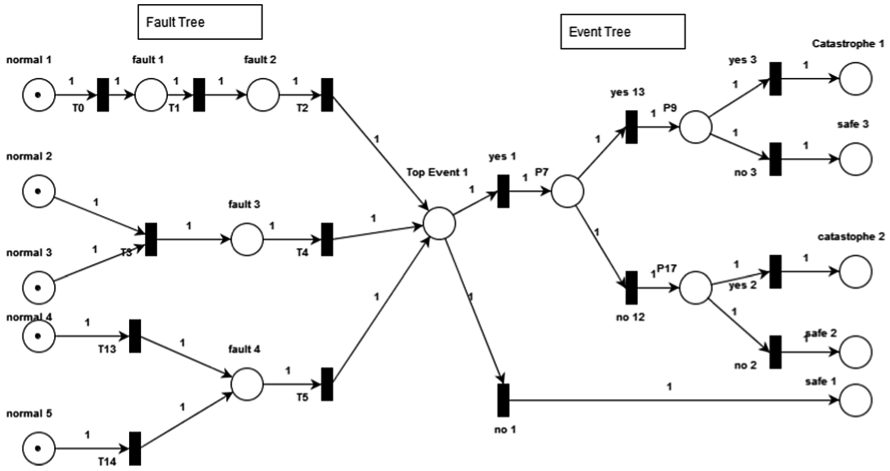

Fig. 3. Example of a bow tie to PN.

It can be observed from the obtained models that places and transitions are common to different bow-ties, so that the graphical representation of PN can contribute to the simplification of the final model, integrating all obtained bow-ties. This step is fundamental to the implementation of the proposed method. After the simplification process, the properties for the formal validation of the obtained model must be verified again.

4.4 Insertion of Barriers/Fuzzy Logic

After the formal validation of the obtained PN model, the next step consists of associating external actions with the PN states, representing barriers to the evolution of fault states. In the proposed method, only the active barriers, associated with a control system, are considered, in which prevention and mitigation actions are associated with actuators. Such actuators can be defined in the initial stages of FMEA and FTA/ETA. N example of a PN model with barriers is show in Fig. 4.

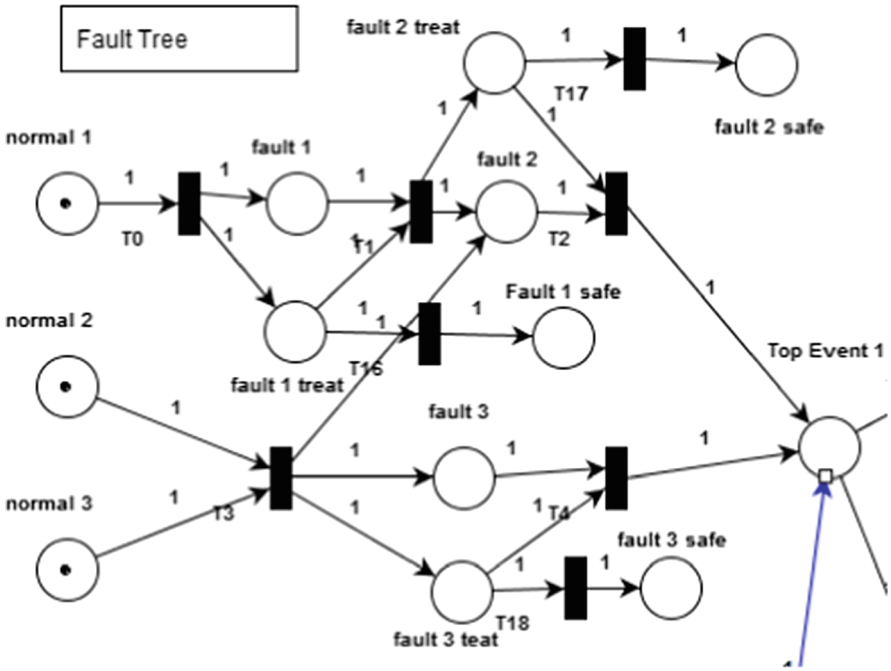

Fig. 4. Example of safety barrier in the PN model.

The advantage of simplifying the models in the previous step is that actuators can be common to different bow-tie actions, which certainly minimizes implementation costs. Another advantage is the property of the encapsulation of functionalities, which represents a great advantage in the design process. In terms of the PN structure, the barriers have the function of inserting deadlocks. Fuzzy logic can help in this process since can define the parameters of the variables associated with the occurrence of a fault, as well as represent an anticipatory action of prevention/mitigation action insofar as the analysis of the temporal increment of the variable can be part of the control action. (Souza et al. 2014) presents the contribution of fuzzy logic to the implementation of a SIS. An example of a fuzzy logic implementation is shown in Fig. 5.

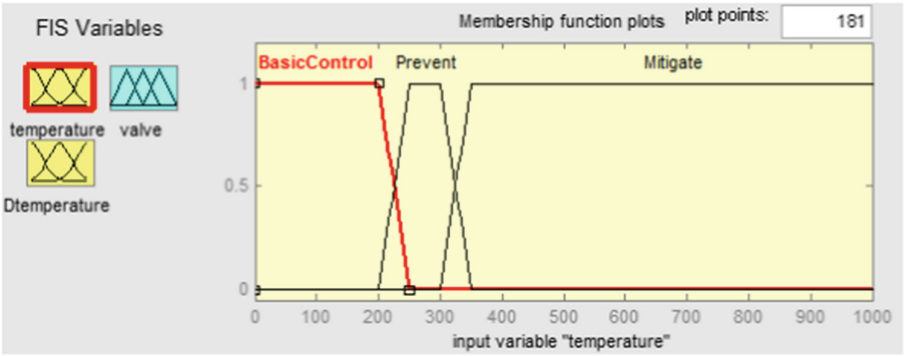

Fig. 5. Example of fuzzy logic implementation. Extracted from (Souza et al. 2014)

4.5 Control Codes Generation

The control codes can be obtained by transcribing PN to Ladder models (IEC-61131-3) or by means of IEC 61131-7, which deals with the conversion of fuzzy logic to Structured Text.

5 Conclusions

The paper presents a method for the implementation of a Safety Instrumented System in modern production systems, inserted in the context of smart systems, by the concept use of Safety Barriers, considering different scenarios of faults. The scenarios are modeled by PN, and the main and the main contribution lies in the interrelationship of the scenario models. It is possible to simplify those models by common initializing events and common actuators, resulting in a greater ease of implementation and control code generation. The proposed method is being applied in a gas compression station and in an oil extraction platform, and the results obtained so far have been quite satisfactory. A limitation of the method are the extensive graphs obtained from the interrelationship of the PN models of the Bow Tie diagrams. A possible solution would be the generation of the models in Colored Petri nets (Jensen 1997) (ISO, IEC 15.909), which would result in more synthetic models, without losing information or complexity of the models, and having as additional benefit the insertion of the fuzzy levels of the associated process variables.

Acknowledgments. The authors would like to thank the Brazilian governmental agencies CNPq, FAPESP, and CAPES for their financial support to this work.

References

Adam, N.R., Atluri, V., Huang, W.: Modeling and analysis of workflows using Petri nets. J. Intell. Inf. Syst. **10**, 131–158 (1998)

Badreddine, A., Ben Amor, N.: A new approach to construct optimal bow tie diagrams for risk analysis. In: García-Pedrajas, N., Herrera, F., Fyfe, C., Benítez, J.M., Ali, M. (eds.) IEA/AIE 2010. LNCS (LNAI), vol. 6097, pp. 595–604. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13025-0_61

Chen, C., Dai, J.: Design and high-level synthesis of hybrid controller. In: Proceedings of IEEE Conference (2004)

DIN 25419: DIN, Event Tree Analysis; Method, Graphical Symbols and Evaluation. Germany (1985)

Ferreira, J.D., Ribeiro, L., Onori, M., Barata, J.: Challenges and properties for bio-inspiration in manufacturing. In: Camarinha-Matos, L.M., Barrento, N.S., Mendonça, R. (eds.) DoCEIS 2014. IAICT, vol. 423, pp. 139–148. Springer, Heidelberg (2014). doi:10.1007/978-3-642-54734-8_16

Goble, W.M.: Control Systems Safety Evaluation & Reliability. ISA - The Instrumentation, Systems and Automation Society, no. 2 (1998)

Hamadi, R., Benatallah, B.A.: A Petri net-based model for web service composition. In: Proceedings of 14th Australasian Database Conference (ADC 2003), Adelaide, pp. 191–200 (2003)

IEC: IEC 60812 - Analysis Techniques for System Reliability - Procedures for Failure Modes and Effects Analysis (FMEA). IEC - International Electrotechnical Commission, Geneva, Switzerland (2006)

IEC: IEC 61025 - Fault Tree Analysis (FTA). IEC - International Electrotechnical Commission, Geneva, Switzerland (2008)

IEC: IEC 61882 - Hazard and Operability Studies (Hazop) - Application Guide. IEC - International Electrotechnical Commission. London, UK, p. 58 (2001). (ISBN 0 580 37625 7)

Jensen, K.: Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use. Springer, Heidelberg (1997)

Lewis, E.E.: Introduction to Reliability Engineering, 2nd edn. Wiley, Hoboken (1995)

Mazzolini, M., Brusaferri, M., Carpanzano, E.: An integrated framework for model-based design and verification of discrete automation solutions. In: Proceedings 2011 9th IEEE International Conference on Industrial Informatics, Milan, pp. 545–550 (2011)

Modarres, M., Kaminskiy, M., Krivstov, V.: Reliability Engineering and Risk Analysis: A Practical Guide. CRC Press, Boca Raton (2010)

Morales, R.A.G., Garcia Melo, J.I., Miyagi, P.E.: Diagnosis and treatment of faults in productive systems based on Bayesian networks and Petri net. In: IEEE International Conference on Automation Science and Engineering (Case 7), pp. 357–362 (2007)

Nassar, M.G.V., Melo, J.I.G., Miyagi, P.E., Santos Filho, D.: Modeling and analysis of the material entry flow system in a pickling line process using Petri net. In: ABCM Symposium Series in Mechatronics, vol. 3, pp. 444–453 (2008)

Peters, B., Perez, P., Soares, J., Thomaz, D.: Risk analysis and management based on the performance of safety barriers: case study: fixed platform Polvo A. In: IBP Rio Oil & Gas Expo and Conference, Rio de Janeiro, RJ (2016)

Rausand, M.: Risk Assessment: Theory, Methods, and Applications, 1st edn. Wiley, Hoboken (2011)

Ru, Y., Hadjicostis, C.: Fault diagnosis in discrete event systems modeled by Petri nets with outputs. In: Proceedings of 9th International Workshop on Discrete Event Systems, Goteborg, Sweden (2008)

Sampaio, L.R.: Validação Visual de Programas Ladder Baseada em Modelos. Dissertação de Mestrado - Universidade Federal de Campina Grande, Campina Grande (2011)

Santos Filho, D.J.: Aspectos do Projeto de Sistemas Produtivos. Tese de Livre Docência - Escola Politécnica da USP, São Paulo (2000)

Sallak, M., Simon, C., Aubry, J.: A fuzzy probabilistic approach for determining safety integrity level. IEEE Trans. Fuzzy Syst. **16**(1), 239–248 (2008)

Sklet, S.: Safety barriers: definition, classification, and performance. J. Loss Prev. Process Ind. **19**, 494–506 (2006)

Souza, J.A.L., Santos Fo, D.J., Squillante Jr., R., Junqueira, F., Miyagi, P.E.: Mitigation control of critical faults in production systems. In: Camarinha-Matos, L.M., Barrento, N.S., Mendonça, R. (eds.) DoCEIS 2014. IAICT, vol. 423, pp. 119–128. Springer, Heidelberg (2014). doi:10.1007/978-3-642-54734-8_14

Souza, J.A.L., Santos Filho, D.J., Miyagi, P.E., Silva, J.R., Moscato, L.A., Squillante Jr. R., Sicchar, J.R.: Coloured Petri nets for implementation of safety instrumented systems in critical production systems. In: CLCA 2016 17th Latin American Conference on Automatic Control, 2016, Medellin. Proceedings Book, pp. 27–33. Universidad EAFIT, Medellin (2016)

Squillante Jr., R., Fo, D.J.S., Souza, J.A.L., Junqueira, F., Miyagi, P.E.: Safety in supervisory control for critical systems. In: Camarinha-Matos, L.M., Tomic, S., Graça, P. (eds.) DoCEIS 2013. IAICT, vol. 394, pp. 261–270. Springer, Heidelberg (2013). doi:10.1007/978-3-642-37291-9_28

Summers, A., Raney, G.: Common cause and common sense, designing failure out of your safety instrumented systems (SIS). ISA Trans. **38**, 291–299 (1999)

Villemeur, A.: Reliability, Availability, Maintainability and Safety Assessment, vol. 1 and 2, 1st edn. Wiley, Hoboken (1992)

Wang, X., Chen, G., Xie, Y., Guo, Z.: Fault detection and diagnosis based on time Petri net. In: Proceedings of 8th International Conference on Electronic Measurement and Instruments, Beijing, China (2008)

Wu, B., Xi, L.-F., Zhuo, B.H.: Service-oriented communication architecture for automated manufacturing system integration. Int. J. Comput. Integr. Manuf. **21**(5), 599–615 (2008)

Zhang, Y., Jiang, J.: Bibliographical review on reconfigurable fault-tolerant control systems. Ann. Rev. Control **32**, 229–252 (2008)

Zurawski, R., Zhou, M.: Petri nets and industrial applications: a tutorial. IEEE Trans. Ind. Electr. **41**, 567–583 (1994)