MATHEMATICAL METHOD FOR MODELING AND VALIDATING OF SAFETY INSTRUMENTED SYSTEM DESIGNED ACCORDING TO IEC 61508 AND IEC 61511

Reinaldo Squillante Júnior, reinaldo.squillante@usp.br
Diolino J. dos Santos Filho, diolinos@usp.br
Escola Politécnica da Universidade de São Paulo, São Paulo, SP, Brazil
Luis Alberto M. Riascos, luis.riascos@ufabc.edu.br
Universidade Federal do ABC, Santo André, SP, Brazil
Fabrício Junqueira, fabri@usp.br
Paulo E. Miyagi, pemiyagi@usp.br
Escola Politécnica da Universidade de São Paulo, São Paulo, SP, Brazil

Abstract. *Safety Instrumented Systems (SIS) are designed to prevent and / or mitigate accidents, avoiding undesirable high potential risk scenarios, assuring protection of people's health, protecting the environment and saving costs of industrial equipment. Standards such as ANSI/ISA S.84.01; IEC 61508, IEC 61511, among others, guide different activities related to Safety Life Cycle (SLC) design of SIS: mathematical methods are strongly recommended for desired safety integrity level (SIL). In this context, this paper considers control algorithm development and validation and proposes a mathematical method for modeling SIS including diagnostic and treatment of critical faults based on Bayesian networks (BN) and Petri nets (PN). This approach considers diagnostic and treatment for each safety instrumented function (SIF) including hazard and operability (HAZOP) studies in the equipment or system under control. It also uses Bayesian network (BN) and Behavioral Petri net (BPN) for diagnoses and decision-making and the interpreted Petri net (PN) for the synthesis, modeling and control to be implemented by Safety Programmable Logic Controller (PLC) as a layer of risk reduction separated from the Basic Process Control System (BPCS). Finally, a case study of a natural gas compression station considering diagnostic and treatment of critical faults is presented.*

Keywords: *Safety Instrumented System, Critical Fault diagnosis, Critical Fault Treatment, Bayesian networks, Petri net*

1. INTRODUCTION

Nowadays, new control strategies need to be considered for industries to remain competitive in a globalized market, covering aspects such as cost, quality, delivery time, production flexibility and more (Chen and Dai, 2004). Additionally, industrial processes are becoming more complex due to dynamic and technology, among other factors. Simultaneously, organizations have focused on policies to achieve and demonstrate people's safety and health, environmental management system and controlling risks. Additionally, Industries should be consistent with their policies and objectives according to the standards of Occupational Health and Safety Assessment Services (OSHAS18001, 2007) and (ISO14001, 2004) respectively.

In this context, any industrial system, as modern and innovative as can be, could be considered to pose a serious risk to people's health,the environment and to the costs of industrial equipment, in the event that a failure fails to be diagnosed and treated correctly (Sallak *et al.*, 2008). Although many studies have been presented for diagnosis and treatment of faults, a review of fault-tolerant reconfigurable control system can be found in (Zhang and Jiang, 2008), yet accidents still occur. The reason for that is that firstly, there is an intrinsic feature of combinatorial explosion of possible states in discrete event systems (DES) and higher dependency on the number of independent devices in the system. Thus, studies that aim to diagnose and treat faults are inserted at this level of complexity that relies on restricting its state space for the control and treatment of a particular class of faults.

Experts indicate that the solution to this problem involves the application of a layer of risk reduction which is called safety instrumented systems (SIS) that are specifically designed to perform functions that maintain a process in a safe state when any risk is detected, ensuring the integrity of people, equipment and avoids environmental impacts (Summers and Raney, 1999). In this sense, some safety standards such as ANSI/ISA S84.01-1996 (ANSI/ISA-SP, 1996), IEC 61508 (IEC, 1998), IEC 61511 (IEC, 2003a) among others, guide different activities related with a SIS Safety Life Cycle (SLC), such as design, installation, operation, maintenance, tests and others (Lundteigen and Rausand, 2009).

The term risk defines a metric for quantifying injury, environmental damage and economic losses; in reference to both probability of a fault occurrence and magnitude of the injury or loss (Bell, 2005). According to IEC 61508 the term "failure" is defined as an abnormal condition that can cause a reduction or loss of the ability of a functional unit.

Here, failures are classified into two groups: (a) non-critical faults that define risks to be "tolerated" and therefore automatically recovered by the Basic Process Control System (BPCS); hence, the industrial process can be regenerated in a controlled way to a normal state of operation. And (b) critical faults that define unacceptable magnitude of risks and must be either prevented or mitigated in order to avoid a catastrophic scenario, which may cause human fatalities and environmental damage. Therefore, the industrial process should be placed into a safe state via the degeneration of the process by layer of risk reduction or SIS. "Figure 1" shows the architecture of BPCS and SIS for processes.

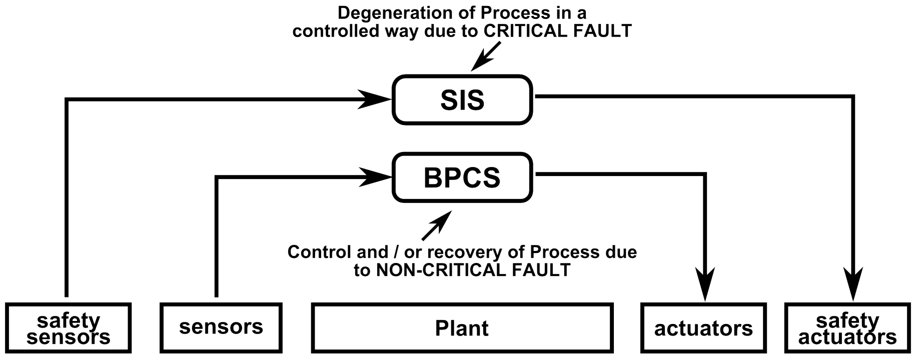

Figure 1. Architecture of Basic Process Control System (BPCS) and Risk Reduction Layer (SIS) for a Process

According to safety standard IEC 61508, the description of faults is made from the identification of safety instrumented functions (SIF). In this sense, a SIF describes a critical fault that should be diagnosed and treated by SIS. A SIS implements one or more SIF through: (a) one or more sensors, (b) one or more devices that perform a control (i.e.: electric, electronic and programmable electronic equipment (PES) such as safety programmable logical controller) and (c) one or more actuators. For each SIF a parameter called safety integrity level (SIL) is defined (Stavrianidis and Bhimavarapu, 1998). This parameter is a measure of safety for components and /or systems. SIL reflects what end users can expect from a device and /or system in a safety function; in case of fault, the process will be recovered in a safe way (Faller, 2001).

Standard IEC 61508 recommends the development of each SLC based on formal methods. In the literature, several authors addressed the considerations of SIS from different points of view; for example, from the standpoint of control hardware, design of SIS and methodologies for the determination and assessment of the SIS and SIL. Bobbio *et al.* (2001) presents an approach using Coloured Petri net and Bayesian networks for SIL definition. Seixas de Oliveira (2008) presents a cost analysis based on SIL definition. In Dutuit *et al.* (2008), a hybrid approach using Petri net and MonteCarlo is presented to quantify the reliability of SIS. Kannan (2007) proposes the use of Bayesian networks to create a risk probability model of a plant and / or process and uses this model in the design phase of SIS. Recently, Lundteigen and Rausand (2009) considered reliability, availability, maintenance and safety in the design and integration of SIS life cycle of security defined by IEC 61508.

There are no works in the literature that address control algorithm development and validation for SIS based on a mathematical method. According to considerations of IEC 61508 and IEC 61511 standards, steps should be implemented and formally verified by analysis and / or tests before the final validation of SIFs and SIS is installed.

A mathematical method for modeling and validating SIS is proposed here in, addressing the control algorithm development in compliance to IEC 61508 and IEC 61511 standards. This approach considers diagnostic and treatment for each safety instrumented function (SIF) including hazard and operability (HAZOP) studies in the equipment or system under control. For modeling critical faults diagnosis, Bayesian network (BN) and Behavioral Petri net (BPN) are suggested. For modeling critical faults treatment, interpreted Petri net (PN)is suggested, since this approach is based on dynamic system behavior, as oriented by occurrence of discrete events, according to discrete event dynamic systems (DEDS)(Miyagi, 2007). Additionally, coordination modeling is used to link each treatment model to a corresponding diagnostic model. Also, for these coordination models, interpreted Petri net is suggested. The mathematical model generated will allow the validation of the control algorithm by providing a computational resource ensuring the SIL specification according to IEC 61508. Finally, these models can be translated to any language defined by IEC 61131-3 in accordance to IEC 61511 standard (IEC, 2003a) and implemented by Safety Programmable Logic Controller (PLC) as a layer of risk reduction separated from Basic Process Control System (BPCS).

This paper is organized as follows: in Section 2, the fundamental concepts for Bayesian network (BN), Behavioral Petri Net (BPN) and Petri net (PN) are introduced. In Section 3 a mathematical method for diagnosis and treatment of critical faults in SIS is presented. In Section 4, a case study of a natural gas compression station considering modeling of diagnosis and treatment of critical faults is presented by applying the method. Finally, in the Section 5, presents the conclusion.

2. FUNDAMENTAL CONCEPTS

This section introduces fundamental concepts of Bayesian Network (BN) and Behavioral Petri Net (BPN) for critical faults diagnosis. Additionally, it introduces Petri Net (PN) for coordination and treatment of critical faults.

2.1 Bayesian Network (BN)

Initially, a model for critical fault diagnosis should be constructed from causes to effects (i.e: if we are sure about the cause of the problem, we can identify which effects are produced by it). But, in the diagnostic reasoning (instead of predictive reasoning), causes should be diagnosed based on the monitored effects (i.e: which the most probable cause is based on the observed effects). In this context, three procedures should be distinguished: (a) the construction of cause -> effect structure from knowledge and / or BN learning algorithms; (b) conversion from the obtained cause -> effect structure to Behavioral Petri Net (BPN) and (c) the utilization of the structure for modeling the critical fault diagnostic.

The Bayesian Network (BN) provides a method of reasoning used to represent partial beliefs under conditions of uncertainty (Pearl, 2000). A Bayesian Network *BN = (G, CP)* is composed of the network structure *G* and the conditional probabilities *(CP)* as shown in "Fig. 2". A direct acyclic graph (DAG) represents the graphical structure *G*, where each node of the graph (depicted by a circle) is associated to a variable *Xi*, and each node has a set of parents *pa(Xi)*. A Bayesian network is acyclic because no cyclic process can be represented. The relationship among variables and their parents (depicted by *arcs*) represents the cause -> effect relationship. The conditional probabilities *(CP)*, numerically quantify this cause -> effect relationship (Murphi, 2007).

Fire	Smoke	θ_{slf}
true	true	.90
false	true	.01

Fire	Tampering	Alarm	θ_{alf}
true	true	true	.5000
true	false	true	.9900
false	true	true	.8500
false	false	true	.0001

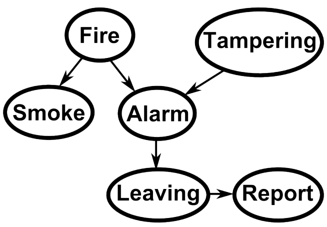

Figure 2. A Bayesian network with some of its conditional probability tables *(CP)*

A Bayesian network is a structure that graphically models relationships of probabilistic dependence of cause-effect considering a group of variables. Bayesian networks have been extensively applied for fault diagnosis (Lerner *et al.*, 2002), (Chien *et al.*, 2002). A Bayesian network allows the combination of human expert knowledge of the process under observation and probability theory for the construction of a diagnostic structure; nevertheless, both are recommended for the construction of a "good" Bayesian network (Riascos *et al.*, 2007). Thus, the construction of a structured Bayesian Network can be accomplished from either database from process or domain knowledge.

2.1.1 Learning the Bayesian Network structure

There are some methods for constructing Bayesian networks from learning the network structure and parameters. One method is largely subjective, which reflects one's own knowledge or the knowledge of others (typically, perceptions about causal influences) and then captures them into a Bayesian network. Another method for constructing Bayesian networks is based on learning them from database, such as medical records or student admissions data (Darwiche, 2010). In this context we are concerned about applying the learning of the Bayesian networks structure.

In the last decade, many Bayesian network structure learning algorithms have been developed. These algorithms generally fall into two groups, **search & scoring**- based algorithms and **dependency analysis**- based algorithms. An overview considering advantages and disadvantages of these algorithms can be found in (Cheng *et al.*, 1998). Here the dependency analysis - based algorithm was chosen to construct a Bayesian network from both database and/or domain knowledge. The tool used is the Bayesian Network Power Constructor (BNPC). This tool can be found in (Cheng, 1998).

2.2 Petri Net (PN)

Since it was presented in 1962 by Carl A. Petri, the Petri net (PN) has been considered as a powerful tool for modeling, analysis and design of DEDS. This tool allows a graphical and mathematical description of the system. In this way, the PN is a communication tool among people related with the project, allowing an easy interpretation, clear identification of the states and actions. The PN provides the possibility of dynamic representation of the system and it is structured, at many levels of abstraction. PN can represent processes with synchronism, concurrent, causality, conflict, share resources and normal situations in productive systems (PS). The mathematical support of PN is useful for performing the formal tests of the dynamic properties of the system. This is especially useful in applications in which security is a relevant factor. It is assumed that the reader is familiar with the basic concepts of PN and the formal definition, rules of execution and formalization of the dynamic properties of the PN as detailed in (Murata, 1989) and (Peterson, 1981).

2.2.1 Interpreted Petri net

As mentioned in section 1, our proposal is to use PN as a tool for modeling coordination and treatment of critical faults in a SIS design. Hence, an extension of PN called interpreted Petri net is used. In Peterson (1981), interpreted Petri net is defined as a tool which is associated with either an interpretation or meaning to their *places* and *transitions*; representing something real which aims to modeling (i.e.: safety sensors and safety actuators). Otherwise, a non-interpreted PN shows no meaning to their *places* and *transitions*, being an abstract representation.

2.2.2 Behavioral Petri Net (BPN)

Although diagnostic models have been created through structures in BN, they can be transcribed into an IEC language; and converted in to the same PN formalism. In Portinale (1997) an extension of PN to represent fault diagnosis is proposed, which is defined as Behavioral Petri Net (BPN). BPN is an ordinary PN with an additional OR-*transition* to model fault propagation among multiple paths by considering a set of observations about a process. BPN is a type of PN that models a diagnostic process since no cyclic process has to be represented. In this context, the process of a Bayesian network (BN) can be represented through a BPN. If two effects are independent of a cause based on database, then an OR-*transition* is considered, but if the two effects are dependent, i.e: both effects take place when a cause is present, then the AND-*transition* is considered. In "Figure 3", (a) A BN with three variables is depicted (*X1* is the cause, *X2* and *X3* are the effects), (b) an equivalent BPN with OR-*transition* is depicted; (c) an equivalent AND-*transition* is depicted.

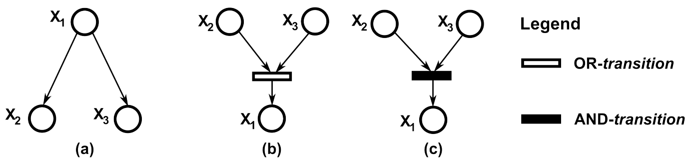

Figure 3. Bayesian network and equivalent BPN models with *transitions*

3. PROPOSAL OF A MATHEMATICAL METHOD

The proposal of a mathematical method for modeling and validating control algorithm for SIS design based on BN, BPN and PN, the initial idea of which was introduced in (Squillante Jr *et al.*, 2010), is presented in "Fig. 4".

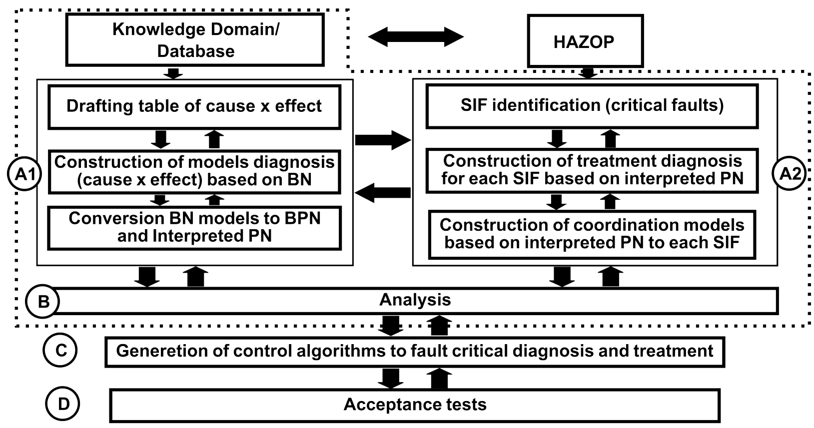

Figure 4. Mathematical method for critical fault diagnosis and treatment in SIS design

The method defines four steps: (A) modeling, (B)analysis, (C) generation of control algorithms and (D) acceptance tests. The modeling step is divided into two complementary stages: (A1) critical fault diagnosis and (A2) critical fault treatment and coordination. The Step (B), analysis, is performed to both verify if some PN properties for critical fault diagnosis, treatment and coordination integrated models are met and validate integrated models in compliance with specification. The liveness, safety, conservativeness and reachability properties should be verified for SIS applications. The Step (C), generation of control algorithms, is performed to convert verified models into a language recommended by standard IEC 61131-3 (IEC, 2003b) and accepted by IEC 61511 (IEC, 2003a) for implementation in a Safety PLC. Finally, Step (D), acceptance tests, are performed in accordance to IEC 61511, to validate if a control algorithm for each SIF complies with the specifications.

3.1 Description of the proposed mathematical method

The steps applied in the proposed mathematical method are described below:

3.1.1 A1 - Critical Fault Diagnostic modeling

Step 1 - Drafting cause-effect table:

In this step, a table that lists the causes (critical faults) defined for each SIF is built, and effects are observed by sensors when these faults occur. The criterion for the construction of this table can be: (a) based on domain knowledge (i.e: in which the relationship between the variables is established by a human operator) and / or (b) based on database obtained from either field experiments or record of past operations.

Step 2 - Construction of model diagnosis (cause -> effect) based on BN

The cause -> effect table obtained from step 1 is used for constructing the BN model. The construction of this model can be performed by using either knowledge or learning BN algorithms. Once the initial structure of BN from cause -> effect is obtained, it is strongly recommended to apply some restrictions from knowledge to improve the network structured.

Step 3 - Conversion from BN model into BPN model and Interpreted PN model

Although the BN models represent a structure that relates the causes of the critical faults with the effects to be monitored by sensors, in the diagnostic reasoning, causes should be diagnosed based on the monitored effects. Additionally, these diagnosis models based on BN must be implemented into a Safety PLC and should thus be converted into PN to make this possible. In this context, firstly diagnosis models should be converted from BN into BPN that are representative mathematical graphical models widely used for fault diagnosis (Luo *et al.*, 2005) and then BPN models are converted into interpreted PN. Finally, interpreted PN model should be transcribed into IEC languages.

3.1.2 A2 - Critical Fault Treatment and Coordination modeling

Step 1 - SIF identification (critical faults)

From hazard and operability (HAZOP) studies, a report is generated and SIFs and SIL are identified for the system under observation. For each SIF, important data are obtained as SIL; that includes initializing events (sensors) and actions (actuators) to be performed by SIS to prevent and / or mitigate such critical faults.

Step 2 - Construction of Treatment Model for each SIF based on interpreted PN

An interpreted PN model is built based on information obtained from each SIF , as shown in the previous step. It ensures that the Safety PLC takes appropriate actions to prevent and / or to mitigate undesirable risks in the system. The goal of each SIF is verified based on dynamic behavior of PN models at the end of this step.

Step 3 - Construction of Coordination model based on interpreted PN to each SIF

A coordination model based is built based on interpreted PN. Once a critical fault is diagnosed by the diagnostic model, the coordinator accounts for calling their respective treatment model to be run, taking actions to prevent and /or to mitigate risks. This model should be designed so as to be robust against the occurrence of spurious failures that may unduly de-energize final elements and produce unwanted system downtime.

3.1.3 B - Analysis

In this step, the models of critical fault diagnosis, treatment, and coordination are integrated to compose the SIS. It is strongly recommended to verify the "best" properties for the resulting model. This procedure should be performed by simulating through computational tools (e.g.: HPSim (Anschuetz, 2001)) to verify such properties. As previously mentioned, the properties of liveness, safety, conservativeness and reachability should be verified for SIS applications. Thus, it complies with the IEC 61511 standard which defines the term "verification" as a demonstration activity for each phase of de SLC from analysis and / or tests specified for the inputs; the outputs should meet the requirements defined for the particular phase. Next, integrated models should be validated in compliance with specifications. This procedure should also be performed by computational tools (e.g.: HPSim (Anschuetz, 2001)).

3.1.4 C - Generation of control algorithms for fault critical diagnosis, coordination and treatment

The critical fault diagnosis, coordination, and treatment PN models, should be converted into control algorithm based on the IEC 61131-3 language and accepted by IEC 61511 such as (a) Ladder Diagram, (b) Function Block Diagram and (c) SFC (Sequential Function Chart). Many works have been published about methods for converting PN models into algorithms based on IEC 61131-3 languages as detailed in (Wightkin *et al.*, 2010) (Thapa *et al.*, 2005) (Music *et al.*, 2005).

3.1.5 D - Acceptance Tests

After the implementation of the control algorithms in a Safety PLC, acceptance tests are performed via commissioning and start-up activities. According to the IEC 61508 / IEC 61511 standards, one of the Safety Life Cycle (SLC) steps is related to final testing of commissioning and start-up procedures. The main goal is to "validate" if these algorithms comply with the system requirement specification. This step is in accordance with IEC 61511 standard that define "validation" as a demonstration activity that SIF and SIS met requirements after installation.

4. CASE STUDY

To illustrate the method proposed, a case study for critical fault diagnosis and treatment in a natural gas compression station is presented. To evaluate the proposed approach, one SIF obtained from HAZOP is considered. Natural gas is a mixture of highly flammable hydrocarbons. This application is used here as an example due to high risk of this process.

4.1 Process Description

The natural gas station has one or more natural gas supply lines, called suction, from a gas pipeline which transports this natural gas. At the station entrance, natural gas goes through filter equipment before being compressed by the turbo-compressor machine. A portion of this gas is directed to an utility unit. The utility unit accounts for controlling the gas temperature and pressure for use in the compression station, such as fuel gas for the turbo-compressor machine, gas heaters and gas power generators. After the natural gas is compressed by turbo-compressor machine, it is sent back to the gas pipeline through discharge lines, called headers. “Figure 5” shows a Process and Instrumentation Diagram (P&ID) of supply lines for natural gas (suction 1 and 2).

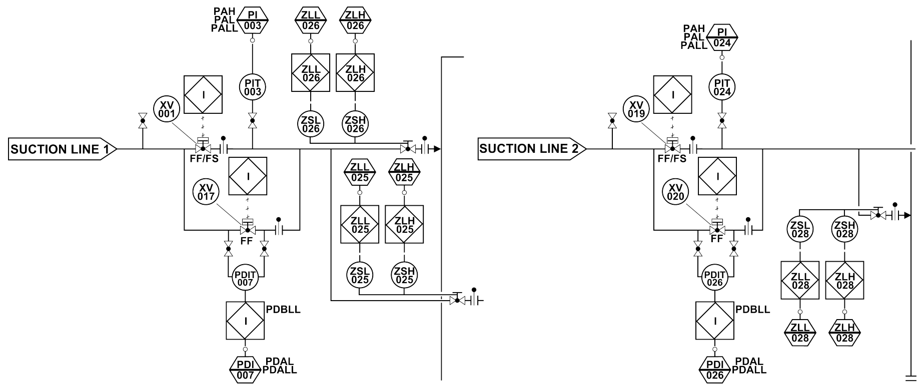

Figure 5. P& ID of Suctions lines 1 and 2 at the entrance of the natural gas compression station

“Figure 6” shows a P& ID of discharged headers for gas natural pipeline.

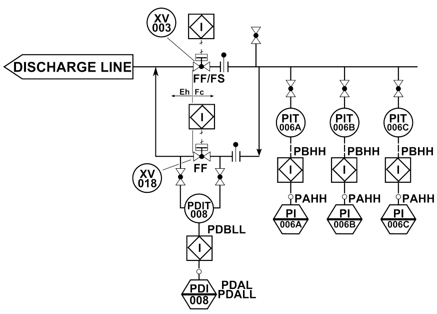

Figure 6. P& ID of Discharge headers for natural gas pipeline

4.2 Application of the proposed method

4.2.1 A1 - Critical Fault Diagnostic modeling

Step 1 - Drafting cause-effect table

The implementation of this step is based on the knowledge about the system, in which variable relationships are established. The cause -> effect table is presented in “Table 1”. In it, all values are binary (e.g.: 0 = Off , 1 = On); except the first column, which defines the number of knowledge cases for a specific SIF-01. The second column defines the critical failure (e.g.: Very High Pressure on Discharge Header) considered for the SIF under study and the remaining columns represent the values of the sensor states observed when the critical failure occurred. PSHH-006A, PSHH-006B, and PSHH-006C are binary states based on thresholds for the very high pressure observed via sensors PIT-006A, PIT-006B and PIT-006C, respectively installed in the discharge header as shown in "Figure 6".

Table 1. Cause -> effect table.

Case	Very High Pressure on Discharge Header	PSHH-006A	PSHH-006B	PSHH-006C
1	1	0	1	1
2	1	1	0	1
3	1	1	1	0
4	1	1	1	1

Step 2 - Construction of the model diagnosis (cause -> effect) based on BN

"Figure 7" shows the SIF-01 diagnosis model generated by applying a learning algorithm BNPC as described in section 2.1.1 ,and based on "Tab. 1" obtained in step 1.

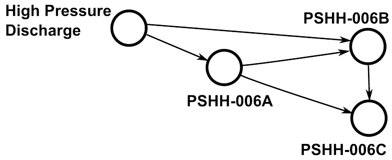

Figure 7. Diagnosis Model for SIF-01

Step 3 - Conversion from BN model into BPN model and Interpreted PN model

"Figure 8" shows the SIF-01 Diagnosis Model based on the Interpreted PN.

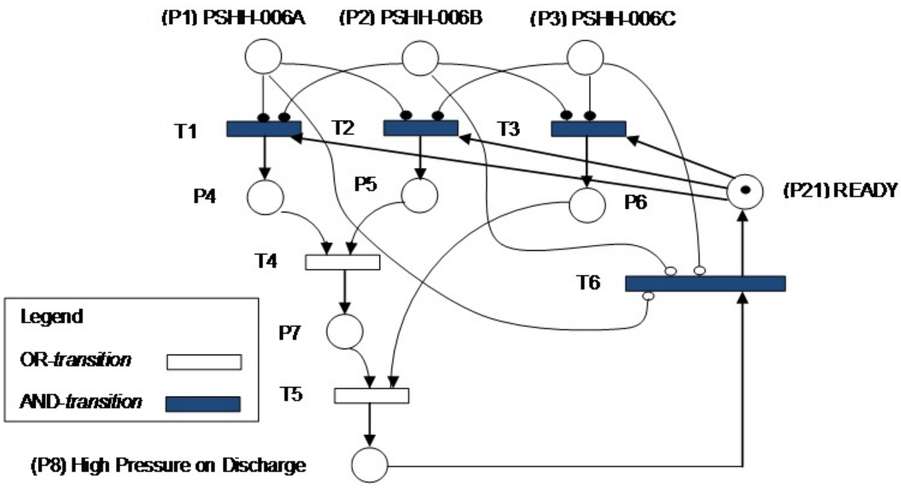

Figure 8. SIF-01 Diagnosis Model based on the Interpreted PN

4.2.2 A2 - Critical Fault Treatment and Coordination modeling

Step 1 - SIF identification (critical faults)

From the risk analysis report in a real situation, 13 SIF's were obtained. Here, SIF-01 is considered as shown in "Table 2".

Step 2 - Construction of the Treatment Model for each SIF based on Interpreted PN

In this step, the treatment model should represent the action to be taken by the SIS when the SIF-01 is diagnosed. The action should be close valves XV-001/017/019/020 (suction lines 1 & 2), close valves XV-003 / 018 (discharge header), and send the shut down command to the turbo-compressor. "Figure 9" and "Table 3" shows the treatment model for SIF-01.

Step 3 - Construction of Coordination Model based on the Interpreted PN for each SIF

"Figure 10" and "Table 4" shows the SIF-01 Coordination Model based on the Interpreted PN.

Table 2. SIF-01 - Very High Pressure on Discharge Header

SIF-ID	Description	Consequences of failure on demand	SIL	Input	Output
01	Very High Pressure on Discharge Header	Possible damage to the discharge header; uncontrolled leakage; excessive vibration and loud noise	3	Sensors PIT-006A/ 006B/ 006C with 2oo3 voting	Close valves XV-001/ 017/ 019/ 020/ 003/ 018 and shut down turbo-compressor

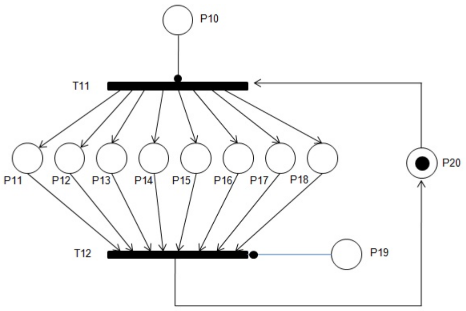

Figure 9. SIF-01 Treatment Model based on Interpreted PN

Table 3. Elements of SIF-01 Treatment Model

Place	Transition	Description
P10		Diagnosed Cause: Very High Pressure on Discharge Header
P11		Close valve XV-001
P12		Close valve XV-017
P13		Close valve XV-019
P14		Close valve XV-020
P15		Close valve XV-003
P16		Close valve XV-018
P17		Shut down command to turbo-compressor
P18		Alarm in Man Machine Interface (MMI)
P19		Acknowledge of Alarm from MMI
P20		Ready
	T11	If (P10 == 1) AND (P20 ==1) > T11 is fire
	T12	If (P11==1) AND (P12==1) AND (P13==1) AND (P14==1) AND (P15==1) AND (P16==1) AND (P17==1) AND (P18==1) AND (P19==1) > T12 is fire

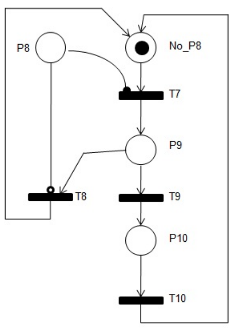

Figure 10. SIF-01 Coordination Model based on Interpreted PN

4.2.3 B - Analysis

The models for diagnosis, coordination and treatment were integrated and simulated using the tool HPSIM (Anschuetz, 2001). Firstly, the liveness, safety, conservativeness, and reachability properties were successfully verified. Next, the integrated models were validated in compliance with requirements by using the HPSim tool. In this step, the validation

Table 4. Elements of SIF-01 Coordination Model

Place	Transition	Description
P8		Diagnosis: Very High Pressure on Discharge Header generated from BPN model
No-P8		Place that indicate SIF-01 No Fault state
P9		Enable calling of SIF-01 Treatment Model
P10		Call SIF-01 Treatment Model after delay time (DT)
	T7	If (P8==1) AND (No-P8==1) > T7 is fire
	T8	If (P9==1) AND (P8==0) > T8 is fire
	T9	If (P9==1) AND (DT >= Preset time) > T9 is fire
	T10	After the call Treatment Model returns to the place No-P8

is conducted, via combinations of known critical fault and verifying that the actions taken are in accordance with the specifications.

4.2.4 C - Generation of control algorithms for fault critical diagnosis, coordination and treatment

The models for fault critical diagnosis, coordination and treatment were converted into a control algorithm based on IEC 61131-3. The language used is the Ladder Diagram.

4.2.5 D - Acceptance Tests

The control algorithms were tested on-line in a safe simulation environment based on the Siemens PLC technology (e.g.: S7-300F, where "F" means Fail Safe) and then the control algorithms were validated in compliance with technical requirements.

5. CONCLUSION

A procedure for generating models that allow performing an off-line analysis based on HPSim tool and further on-line analysis for complying requirements is obtained.

A method for Safety Instrumented System (SIS) design, addressing the critical fault diagnosis and treatment applying mathematical method was introduced.

The method suggests the construction of critical fault diagnosis, treatment and coordination models from formal methods with some formalism such as PN, to further implement them in a Safety PLC through algorithm control based on the IEC 61131-3 language.

Addressing critical fault diagnosis modeling, the BN formal method was introduced to model the cause -> effect construction and further conversion into BPN (e.g: Petri net from knowledge and reasoning diagnosis). Addressing critical fault treatment and coordination modeling, the interpreted PN formal method was introduced for modeling the system dynamic behavior for SIS taking appropriate actions to prevent and / or to mitigate unwanted risks.

The proposed method was applied in a case study of a gas compression station. The case study demonstrates that the proposed method is effective for the development of SIS designed according to IEC 61508 and IEC 61511.

6. ACKNOWLEDGEMENTS

The authors would like to thank FAPESP, CNPq and MEC/CAPES/PET for the financial support to the present project.

7. REFERENCES

Anschuetz, H., 2001. “Hpsim copyright ©1999-2001”. http://www.winpesim.de.
ANSI/ISA-SP, 1996. “Application of safety instrumented systems for the process industries”.
Bell, R., 2005. “Introduction to IEC 61508”. In *Proceedings of ACS Workshop on Tools and Standards*. Sydney, Australia.
Bobbio, A., Bologna, S., Ciancamerla, E., Giuliana Franceschinis, G., Rossano Gaeta, R., Minichino, M. and Portinale, L., 2001. “Comparison of methodologies for the safety and dependability assessment of an industrial programmable logic controller”. pp. 411–418.
Chen, C. and Dai, J., 2004. “Design and high-level synthesis of hybrid controller”. In *Proc. of IEEE Intern. Conf. of Networking, Sensing & Control*.
Cheng, J., 1998. “Belief network (BN) powerconstructor”. http://webdocs.cs.ualberta.ca/ jcheng/bnpc.htm.
Cheng, J., Bell, D. and Liu, W., 1998. “Learning Bayesian networks from data: An efficient approach based on information

theory". Technical report, Dept. of Computing Science - University of Alberta - Canada.

Chien, C.F., Chen, S.L. and Lin, Y.S., 2002. "Using Bayesian network for fault location on distribution feeder". *IEEE Transactions Power Deliv.*, Vol. 17, pp. 785–793.

Darwiche, A., 2010. "What are Bayesian networks and why are their applications growing across all fields?" *Communications of the ACM*, Vol. 53, pp. 80–90.

Dutuit, Y., Rauzy, A. and J., S., 2008. "Asnapshot of methods and tools to assess safety integrity levels of high-integrity protection systems". In *Proc. of IMechE*. Vol. 222.

Faller, R., 2001. "Project experience with IEC 61508 and its consequences". *Lecture Notes in Computer Science*, Vol. 2187, pp. 200–210.

IEC, I.E.C., 1998. "Functional safety of electrical / electronic / programmable electronic safety-related systems (IEC 61508)".

IEC, I.E.C., 2003a. "Functional safety - safety instrumented systems for the process industry sector - part 1 (IEC 61511)".

IEC, I.E.C., 2003b. "Programmable controllers - part 3: Programming languages".

ISO14001, I.O.f.S., 2004. "International standard for environmental management systems".

Kannan, P.R., 2007. "Bayesian networks: Application in safety instrumentation and risk reduction". *ISA Transactions, Elsevier Ltd*, pp. 255–259.

Lerner, U., Moses, B., Scott, M., McIlraith, S. and Koller, D., 2002. "Monitoring a complex physical system using a hybrid dynamic Bayes net". In *in Proc. 18th Conf. on Uncertainty in AI (UAI-02), Edmonton, Canada*.

Lundteigen, M.A. and Rausand, M., 2009. "Architectural constraints in IEC 61508: Do they have the intended effect ?" *Reliability Engineering and System Safety*, pp. 520–525.

Luo, J., Tu, H., Pattipati, K., Qiao, L. and Chigusa, S., 2005. "Graphical models for diagnosis knowledge representation and inference".

Miyagi, P.E., 2007. *Controle Prográmavel - Fundamentos do controle de sistemas a eventos discretos*. Editora Edgard Blucher LTDA, Sao Paulo, SP.

Murata, T., 1989. "Petri nets: Properties, analysis and applications". *Proceedings of IEEE*, Vol. 77, No. 4, pp. 541–580.

Murphi, K., 2007. "Bayes net toolbox for Matlab". http://code.google.com/p/bnt/. Last update.

Music, G., Gradisar, D. and Matko, D., 2005. "IEC 61131-3 compliant control code generation from discrete event models". pp. 346–351.

OSHAS18001, 2007. "International standard of occupational health and safety assessment services".

Pearl, J., 2000. "Causality: Models reasoning and inference". In *Cambridge University Press*.

Peterson, J.L., 1981. "Petri net theory and the modeling of systems". Prentice Hall.

Portinale, L., 1997. "Behavioral Petri nets:a model for diagnostic knowledge representation and reasoning". *IEEE Trans. Systems, Man, and Cybernetics (Part B)*, Vol. 27, No. 2, pp. 267–278.

Riascos, L., Simoes, M. and Miyagi, P., 2007. "A Bayesian network fault diagnostic system for proton exchange membrane fuel cells". *Power Sources*, Vol. 165, pp. 267–278.

Sallak, M., Simon, C. and Aubry, J., 2008. "A fuzzy probabilistic approach for determining safety integrity level". Vol. 16, No. 1, pp. 239–248.

Seixas de Oliveira, L., 2008. "Lifecycle cost analysis of alternatives for complying with required safety integrity level (SIL) at a petrochemical plant". In *Proceedings of CCPS Health and Safety Conference*. Buenos Aires, Argentina.

Squillante Jr, R., Santos Filho, D., Garcia Melo, J.I., Junqueira, F. and Miyagi, P.E., 2010. "Safety instrumented system designed based on Bayesian network and Petri net". In *Proceedings of 8th International Conference on Mathematical problems in Engineering, Aerospace and Sciences (ICNPAA)*.

Stavrianidis, P. and Bhimavarapu, K., 1998. "Safety instrumented functions and safety integrity levels (SIL)". Vol. 37, pp. 337–351.

Summers, A. and Raney, G., 1999. "Common cause and common sense, designing failure out of your safety instrumented systems (SIS)". Vol. 38, pp. 291–299.

Thapa, D., Dangol, S. and Wang, G., 2005. "Transformation from Petri nets model to programmable logic controller using one-to-one mapping technique". Vol. 2, pp. 229–233.

Wightkin, N., Buy, U. and Darabi, H., 2010. "Formal modeling of sequential function charts with time Petri nets." *IEEE Transactions on Control Systems*, Vol. 99, pp. 1–10.

Zhang, Y. and Jiang, J., 2008. "Bibliographical review on reconfigurable fault-tolerant control systems". *Annual Reviews in Control*, Vol. 32, pp. 229–252.