Toward an Intelligent Distributed Safety Instrumented Systems: Dependability Evaluation

Abdelhak Mkhida, Jean-Marc Thiriet, Jean-François Aubry

Toward an Intelligent Distributed Safety Instrumented Systems: Dependability Evaluation

Abdelhak Mkhida*,*, Jean-Marc Thiriet**, Jean-François Aubry*****

*ENSAM (Ecole Nationale Supérieure d'Arts et Métiers), Meknes BP 4024, Marjane II, Morocco
(e-mail: mkhida@ ensam.ac.ma)
**Joseph Fourier University, GIPSA-Lab (Grenoble Images Parole Signal Automatique UMR 5216 CNRS-INPG-UJF), BP 46, 38402 Saint Martin d'Hères France
(e-mail:jean-marc.thiriet@ ujf-grenoble.fr)
***CRAN (Centre de Recherche en Automatique de Nancy). Nancy-Université CNRS UMR 7039
INPL (Institut National Polytechnique de Lorraine), 2 Avenue de la forêt de Haye, 54516 Vandoeuvre lès Nancy.
(e-mail: jean-françois.aubry@ensem-inpl-fr)

Abstract: In this paper, the modelling and thus the performance evaluation relating to the dependability are studied for structures which have intelligence in the instruments constituting the Safety Instrumented Systems (SIS) in order to determine the contribution of the intelligent instruments in the safety applications. Dynamic approach using Stochastic Petri Nets (SPN) is proposed and the metrics used for the evaluation of the dependability of the Intelligent Distributed Safety Instrumented Systems (IDSIS) refer to two modes of failures mentioned by the safety standards: mode of dangerous failure and mode of safe failure.

1. INTRODUCTION

Safety Instrumented Systems (SIS) have been used for many years to perform safety instrumented functions in the process industries (IEC61511 2003). The SIS are defined as the collection of all safety related sensing elements to determine an emergency situation, all safety related logic solvers to determine what action to take and all safety related final elements to implement the action (Knegtering 2002).

Adding a network communication and intelligent instruments such as intelligent sensors and actuators to the SIS makes this system intelligent. These instruments with a network communication provide several advantages such as integration of diagnosis, cabling reduction, increasing of reconfigurability etc (Lian, et al., 2002).

The problem is to quantify the contribution of the use of the intelligent instruments in the safety loops in compliance with related standards. In safety systems many studies were developed for dependability evaluation. Theses approaches ignore the use of intelligent instruments.

The dependability evaluation of such systems is a difficult task and can concern two approaches: a static approach, and a dynamic approach which takes into account the progressive evolution of system states and functioning modes (Mkhida, et al., 2005) (Dutuit, et al., 1997). The potential application of such systems is very widespread from electronic trippers to some critical real-time systems such as X-by wired cars, drones (Berbra & al. 2007) or aeronautics…

In this paper, we are interested by estimate the metrics that are used in the safety context according to safety standards such as IEC 61508 and IEC 61511. These metrics are the probability of failure on demand (PFD) and the probability of fail safe (PFS).

The methodology used for the dependability evaluation for these systems consists on the structuring and the modelling of these systems; the purpose is to make the verification and analysis by mean of stochastic Petri nets in order to exploit the models.

Modelling is achieved by a stochastic approach using the Stochastic Activity Network (SAN). The SAN is a powerful formalism of the stochastic Petri nets (Moghavar and Meyer, 1984) (Ghostine & al., 2007).

The following sections describe the intelligent distributed safety instrumented systems, how they are modelled and the procedures proposed for their evaluation. The two metrics related to safety performance (PFD & PFS) are calculated. The results are compared, presented and conclusions are drawn.

2. INTELLIGENT INSTRUMENT

2.1 Intelligent Distributed Control Systems (IDCS)

Intelligent or smart instruments have been known for more than two decades. These instruments are more sophisticated than traditional instruments (Mekid 2006).

An intelligent instrument is a component part of Intelligent Distributed Control Systems. These systems are thus composed of smart sensors and actuators with calculations ed by a communication network (generally a fieldbus).

The particularity of a distributed system relates to data exchange between the devices via a communication medium supposed to be a network or a fieldbus. Thereby, the intelligent distributed control system becomes more and more complex and sophisticated, and consequently, makes the design step more difficult (Cauffriez, et al., 2004).

2.2 Structure and functions of an intelligent instrument

The intelligent instruments offer the possibility of a local processing of the information which is distributed on the various entities thus allowing a distribution of the execution of the tasks and appearing a distributed control.

The intelligent instruments are basic instruments that contain microprocessors (Nobes 2004), these instruments meet the following criteria:

- the main purpose of the instrument is to measure or directly control a single process variable,

- these instruments include some flexibility in their use due to parameters that are set by the manufacturer or operator,

- intelligent instruments are not restricted to measurements but also include actuators (valves, motors) and other control equipment.

Intelligent instruments offer considerable lifetime cost reductions. These cover the whole life cycle, including specification, installation, operation, maintenance, decommissioning…

Let us now consider an architecture and functions of intelligent sensor. The architecture comprises the following (Mekid 2006):

- A sensing element that links the external world to a sensor system by generating electrical signal (e.g. voltage, current) with response to physical properties of the environment,

- An interface element for signal conditioning and data conversion. The signal obtained from the sensing element is modified and converted to a discrete time digital data,

- A processing element that includes a microcontroller with an associated memory and software,

- A communication element, which provides a two-way communication between the processing and users.

Various functionalities have been suggested for intelligent sensors. (Robert, et al., 1993) proposed that the intelligent sensors should contain configuration, communication, measurement and validation functionalities. (Meijer 1994) includes three functionalities: compensation, computing and communication. (Tian, et al., 2000) suggested the functions of compensation, validation, data-fusion, and communication. capabilities and communication interfaces. Traditional control systems are connected by analogue current (4-20 mA) and voltage loops whereas IDCSs are connect While (Mekid 2006) propose that what is called an intelligent sensor should have the functions of compensation, processing, communication, validation, integration and data-fusion.

We propose for the generic intelligent instrument (Mkhida, et al., 2007) the functions of measurement, configuration, test, validation, control and communication. Figure 1 illustrates these functionalities.

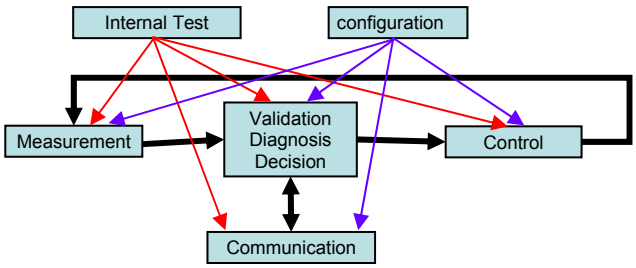

Fig. 1. Functional architecture of an intelligent instrument

3. SAFETY INSTRUMENTED SYSTEMS

Safety instrumented systems are used in many industrial processes to reduce the consequences of process demands on humans, the environment and material assets. Different standards can be used to design safety instrumented systems for process industry like ISA S84, IEC 61508 and IEC 61511 (IEC61508 2000, IEC61511 2003, ISA84 1996). These standards have been developed to ensure that the SIS is designed, implemented and operated according to the specified needs.

3.1 Objectives of a safety instrumented system

The IEC 61511 defines a safety function as : “function to be instrumented by a SIS, other technology safety-related system or external risk, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event”. The Safety Instrumented Function (SIF) is used to describe the safety functions implemented by instrumented technology. The SIS is the physical system implementing one or more SIFs.

The objectives of SIS is to reduce the frequency at which hazard may occur to an acceptable level (Wiegerinck 2002). The safety function only reduces the risk (multiplication: probability x consequences) and never completely eliminates the risk. Some safety functions do not reduce the probability of the consequences.

All combined instrumentation, devices, and equipment that are fulfilling an intended safety function are considered to be part of the safety instrumented systems. The SIS could be composed by a set of safety-related sensing elements, all safety-related logic solver and all safety-related final elements.

3.2 Safety Integrity levels (SIL)

Once the required level of risk reduction to be achieved by the SIS is established, expressed as risk reduction factor(RRF), this level can be translated into the required Safety Integrity Level (SIL) (Knegtering 2002).

IEC 61508 and IEC 61511 split the safety integrity into hardware safety integrity and systematic safety integrity. The safety integrity is split into four discrete safety integrity levels (SILs), SIL1 to SIL4. Each SIL represents a maximum allowed probability of failure on demand of the SIS. SIL4 is the level with the most stringent requirements. To fulfil a specific SIL, the SIL requirements related to hardware safety integrity as well as systematic safety integrity must be met (Lundteigen and Rausand 2006).

To calculate the SIL of a safety function it is required that the complete safety loop from sensor to actuator is considered. Therefore, it is not sufficient to only analyze one subsystem of the safety process, such as the logic solver, and determine the realized SIL.

4. INTELLIGENT SAFETY

The intelligent safety loops (or intelligent distributed safety instrumented systems) enable us to implement safer plants by using the intelligent devices for safety application in compliance with the new IEC 61511 standard.

The concept of intelligent safety is inherent in the use of intelligence within safety instrumented systems. Several manufacturers claim the certification of intelligent products in the applications of safety while launching “smart SIS” but without real justification to the level of the reliability performances. Researchers employ also the term “intelligent safety” in various applications covering nuclear power (Yang, et al., 2005; Chung, et al., 2003; Bae, et al., 2001), railway or transport systems (Farritor and Goddar 2004).

The use of the intelligent instruments in the process industry was facilitated by the increase of the performances in the microprocessors used in industry, in particular in instrumentation. The justification of the use of these instruments in the applications of safety is not completely proven. These instruments have important benefits useful to this type of applications (Nobes 2004).

There is a trend toward the use of intelligent instruments in safety applications. The inherent ability to diagnose failure is the primary reason. The ability of intelligent instruments to reliably measure complex parameters is another.

The incorporation of the intelligence in the SIS leads towards safety intelligence expressed by IDSIS (Intelligent Distributed Safety Instrumented Systems) whose methodology of evaluation is proposed in the following section.

5. MODELLING OF THE SYSTEM BEHAVIOUR

5.1 Modelling approach

The combinatory methods (fault tree, event trees, reliability diagrams) inherent to reliability study of dynamic systems allow us to identify and evaluate the combinations of events leading to the occurrence of another event (Dutuit, et al., 1997). Such combinations do not take into account the order of the events and they exclude any taking into account of time dependency or delays, which can be of high importance in dynamic systems.

The dynamic approach using the Stochastic Petri Nets (SPN or SAN, Stochastic Activity Nets) is proposed to overcome the difficulties mentioned above.

Petri nets, as tools for discrete event simulation are of large use in dependability evaluation. Dynamic changes in the PNs are induced by transition firing. Firing of one or of several transitions changes the net marking. In other terms, it induces a discrete change of states. Thus, dynamic properties of PNs such as parallel firing, successive firing or firing of concurrent transitions may be used to simulate complex events sequences (Vernez, et al., 2003).

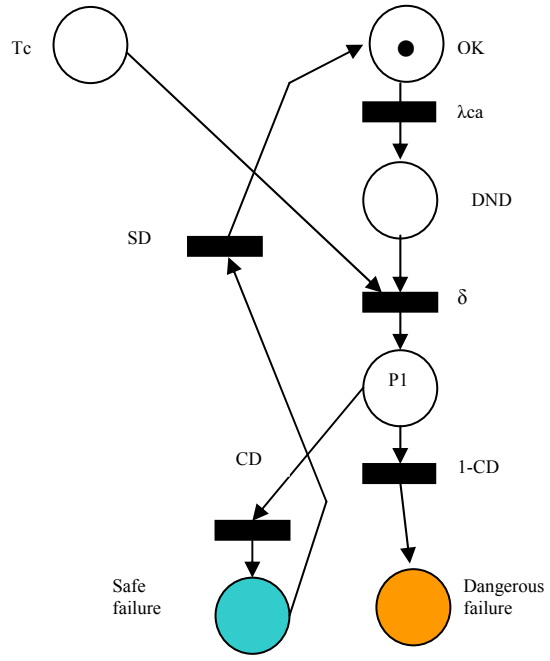

Figure 2 : Example of sensor modelling and its failures

The modelling problem consists in achieving the evaluation of dynamic systems which evolve as a function of the time. SPN give the possibility to model a system in which cooperate discrete-time variables and discrete events, which can occur on stochastic basis. The formalism used for the behavioural modelling will naturally be able to represent these characteristics. The use of this formalism will allow the possibility to represent component failure in interaction with the functional behaviour.

In the present approach, it is assumed that the failure distributions of individual components of a system are given,

and the dependability measures of the stochastic system are sought. Furthermore, the system is assumed to be dynamic (its properties change with time).

5.2 Möbius tool support of SAN

SAN models have been used to evaluate a wide range of systems and are supported by several modelling tools such as Möbius (Deavours, et al,. 2002). The models are developed using this SAN-based tool. Möbius tool consists on the description of the net structure and of the desired performance variables and solutions methods to be used in the evaluation.

5.3 System modelling

In the modelling of the system, the functional and dysfunctional aspects coexist; the failures are divided into safe failures and dangerous failures. A dangerous failure results in an absence of reaction of the safety function. A safe failure results by the setting in a safe position of the system or in an unexpected execution of the safety function. The detection of a safe or dangerous failure, results in a setting into safe position of the system or a forced execution of the safety function. At the beginning, we present SIS without incorporation of intelligent instruments nor communication network. The model of the logic solver is shown in figure 3.

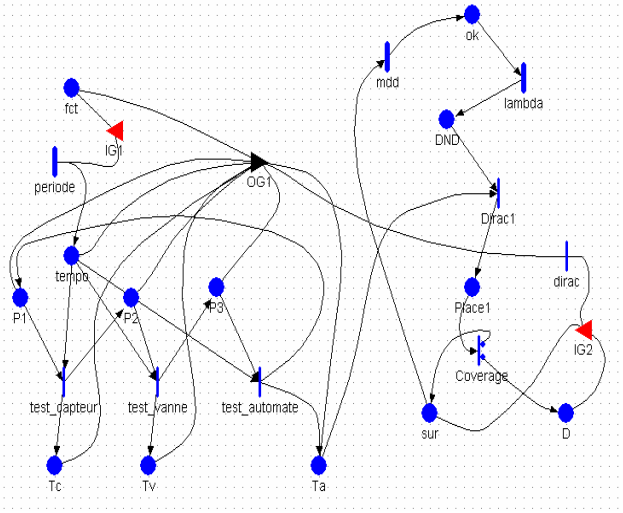

Figure 3: Structure of Logic solver

The model of the logic solver presented figure 3 shows a disposition of two parts, one functional and the other dysfunctional. In the functional part (on the left), the cycles of the logic solver are carried out by a periodic clock (*periode*). The self-tests of the various devices are managed locally according to a policy allocating the same duration of test for the various devices and starting with the test of the sensor (*Tc*), then the actuator (*Tv*) and finally the logic solver (*Ta*). This policy is not the only possible and other policies can be possibly established. For the dysfunctional part, it should be made sure that the token is carried of functional part when the system fails safe or dangerous. The logic solver can be also restored in the event of safe failure and it also has a coverage rate of diagnosis which is inherent to him.

Now, we will be interested in a model of the system with a communication network (*CAN*: *Control Area Network*) and then we will also introduce intelligent instruments instead of traditional instruments. Indeed, CAN protocol is used as a communication architecture for safety critical applications (Carvalho, et al,. 2006). In this article, we focus on CAN while in this study can be extended to other types of communication network.

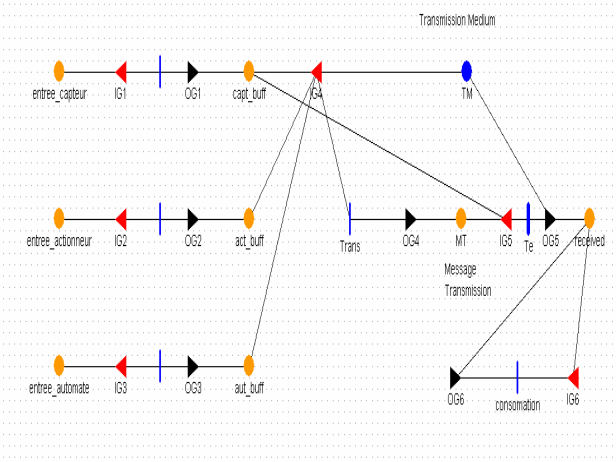

Figure 4 : Network model

This submodel represents the behaviour of the CAN network (Ghostine & al., 2007). The network is made up in this example of three transmitting stations which will be able to send messages on a shared medium (transmission channel). The messages sent are placed in buffer places which are extended places, messages then await the release of the channel to be transmitted towards their destination. The channel access is based on messages priorities. This means that each subscriber will be affected by a priority allowing him or not to send these characteristics via the channel, to avoid the collisions on the channel. The medium (channel) is affected of a delay representing the time of transmission of the messages. The output message of the channel is ready to be sent and it is available in the place *" received "*.

In the intelligent sensor model (see figure 5), the order of test is not transmitted any more via communication network by the logic solver and the functionality relating to the test as well as the other functionalities of the intelligent sensor is treated locally. The modules of test can be requested either when it is necessary, or in a cyclic way, or permanently according to an active monitoring principle (the intelligent sensor has at one's disposal a self-tests). In our model, the intelligent sensor has self-tests in a cyclic way according to the instants of period. The other functionalities are also synchronized by this period.

The model of the actuator does not differ much from that of the intelligent sensor and the dysfunctional parts are similar. It should be noted that the model of the sensor, the actuator and the logic solver are sampled models and information is sent to the communication network periodically.

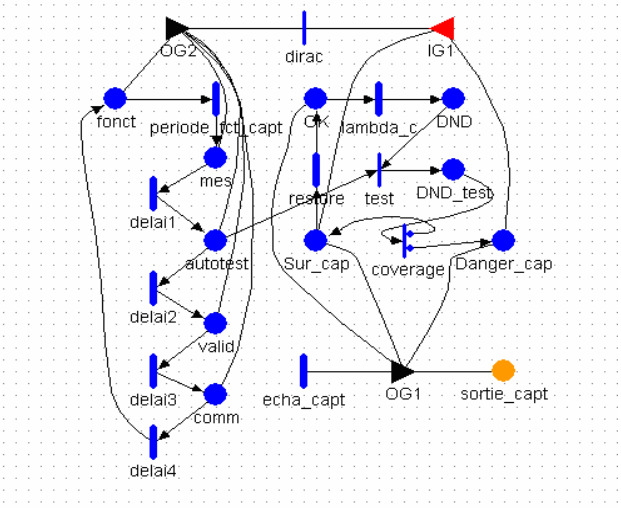

Figure 5: intelligent sensor model

6. RESULTS OF SIMULATION

The procedure used for the calculus of probability of dangerous failures PFD and the probability of safe failures PFS consists of the presence of tokens in the places which describe the safe failures and the dangerous failures for the whole system.

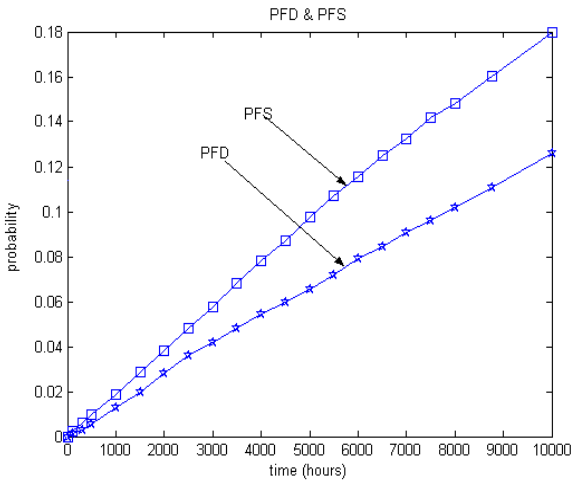

Figure 6: Evolution of PFD and PFS according to time

Figure 6 shows the evolution of PFD and PFS for a 10000 hours duration which is a little higher than one year (8760 hours).

The coverage rate of diagnosis is taken in this example equal to 60% for the whole of the devices. The period of the self-tests operated by the logic solver is selected equal to one hour. I.e., that in compliance with the policy of test chosen, the duration of cycle of the logic solver is 3 hours Also let us note that this duration affects the PFD and PFS when it is changed. For example, for a value of period of test of 1 hour such as it is presented in figure 7, the PFD is 0.113 and the PFS is 0.1604 for a time of 8760 hours mission. While these values apply to one duration of test of the logic solver equal to 2 hours, the PFD passes to 0.107 and the PFS becomes equal to 0.165. It is to show the influence of the frequency of the period of the test of the logic solver on the total performances in safety of the system.

Now, we will be interested in the performance evaluation in safety after the introduction of the intelligent instruments. The results are given for a duration of simulation equal to 8760 hours.

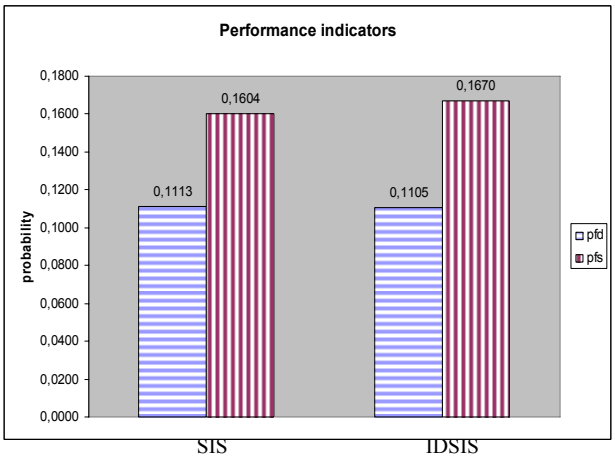

Figure 7: Safety performances for SIS and IDSIS

The evolution of the two metrics (see figure 7) which describe the performances in safety of the studied system show a clear improvement of the probability of dangerous failure according to the addition of intelligence and a weak degradation of the probability of safe failures. Indeed, more there are a high rate of detection by the integrated means of self-tests, more the failure rate weakens and the safe failure rate increases by the means of the dangerous failures which were transformed into some kind of safe failures.

7. CONCLUSION

This paper presents the dependability evaluation of intelligent distributed safety instrumented systems. The performance of these systems is evaluated and compared to the systems without intelligence. The results express the safety performance of these systems, using the particular modelling assumptions made, and the reliability data chosen. Some parameters have a significant impact on the PFD and PFS values, but the accent was put on the contribution of intelligence on the SIS. The setting of the intelligence in SIS improves the PFD but not in a significant way and degrades the PFS slightly. We can say this is the first level of our studies, we have to emphasise the modelling of intelligence in the future model, in order to have a more realistic representation of it.

Special focus was given to the intelligent instruments introduced in the SIS with their failures without counting the failure of network that can influence the performance of safety.

REFERENCES

Bae K.H., H. C. Kim, M. H. Chang and S. K. Sim (2001). Safety evaluation of the inherent and passive safety features of the smart design. *Annals of Nuclear Energy*. **Vol 28**. pp 333-349.

Berbra C., S. Lesecq, S. Gentil, J-M. Thiriet (2007), Diagnosis of a safe networked quadrotor, *ACD'07 workshop on Advanced Control and Diagnosis*, Grenoble, 15-16 novembre 2007.

Carvalho F.C., E.P. Freitas, C.E. Pereira and F.H. Ataide (2006). A time-triggered controller area network platform with essentially distributed clock synchronisation. A *Proceedings Volume from the 12th IFAC Conference*. Saint-Etienne, France. pp, 93-98.

Cauffriez L., J. Ciccotelli, B. Conrard and M. Bayart (2004).Design of intelligent distributed control systems: a dependability point of view. *Reliability Engineering and System Safety*. **Vol 84**. pp, 19-32.

Chung Y.J., S.H. Kim and H.C. Kim (2003). Thermal hydraulic analysis of SMART for heat removal transients by a secondary system. *Nuclear Engineering and Design.* **Vol 225**. pp, 257-270.

Deavours D.D., G. Clark, T. Courtney, D. Dalys, S. Derisavi, J.M. Doyle, W.H. Sanders, and P.G. Webster (2002). The Möbius framework and its implementation. *IEEE Trans. On Soft. Eng*, **Vol. 28**, **no 10**. pp 956-969.

Dutuit Y., E. Chatelet, J.P. Signoret and P. Thomas (1997). Dependability modelling and evaluation by using stochastic Petri nets : application to two test cases. *Reliability Engineering and System Safety*. **Vol 55**, **no 2**, pp, 117-124.

Farritor, S.M. and S. Goddard (2004). Intelligent higway safety markers. *IEEE Intelligent Systems,* **Vol 19 no 6,** pp, 8-11.

Ghostine R., J-M. Thiriet, J.-F. Aubry (2007). Influence of transmission faults on the dependability level of networked control systems: application to a control loop, *8th IFAC Symposium on Cost Oriented Automation, La Havane (Cuba),* 13-15 February 2007,

Haffar M., J.M. Thiriet, E. Savary (2007). Modeling of substation architecture implementing IEC 61850 protocol and solving interlocking problems. *7th IFAC International Conference on Fieldbuses & Networks in Industrial & Embedded systems*, Toulouse, France (November 7-9, 2007), pp. 291-294

IEC61508 (2000). Functional safety of electrical / electronic / programmable electronic safety related systems. IEC, International Electrotechnical Commission.

IEC61511 (2003). Functional safety – Safety instrumented Systems for the process industry sector. IEC, International Electrotechnical Commission.

ISA84 (1996). Application of Safety instrumented Systems for the process industries. ANSI/ISA-S84.01.

Knegtering B., (2002). Safety lifecycle management in the process industries: the development of a qualitative safety-related information analysis technique. *Phd thesis.* Technische Universiteit Eindhoven.

Lian, F., J.R. Moyne and D.M. Tilbury (2002). Network design consideration for distributed control systems. *IEEE Transactions on Control Systems Technology*. **Vol 10(2)**. pp 297-307.

Lundteigen, M.A. and M. Rausand. (2006). Assessment of hardware safety. *Proceedings of the 30th EDReDA Seminar*. Trondheim, Norway.

Meijer G.C.M., (1994). Concepts and focus point for intelligent sensor systems. *Sensors and Actuators A*, **Vol. 41-42**, pp. 183-191.

Mekid S. (2006). Further structural intelligence for sensors cluster technology in manufacturing. *Sensors*, **Vol 6**, pp. 557-577.

Mkhida A., J.M. Thiriet and J.F. Aubry (2007). Modélisation formelle d'un instrument intelligent dans le cadre d'analyse de sûreté de fonctionnement. *Proceeding of 7th Qualita Conference*. Tanger, Morocco.

Mkhida A., P. Barger, J.M. Thiriet and J.F. Aubry (2005). Influence of the control strategy choice on the safety level of the distributed control system. *Proceedings of ESREL (European safety and reliability conference*). Gdansk-Gdynia, Poland.

Movaghar A, and J.F. Meyer (1984). Performability modelling with stochastic activity networks. *Proceddings of the 1984 Real Time Systems*, Symposium, Austin, TX. pp 215-224.

Nobes, T (2004). , Smart instruments in protective measures, Is your product safe? *–IEE Seminar*. pp 67-74.

Robert M., J. M. Riviere, J. L. Noizette, and F. Hermann (1993). Smart sensors in flexible manufacturing systems. *Sensors and Actuators A,* **Vol. 37-38,** pp.239-246.

Tian G. Y., Z. X. Zhao and R. W. Baines (2000). A fieldbus-based intelligent sensor. *Mechatronics*, **Vol. 10**, pp. 835-849.

Vernez D, D. Buchs, and G. Pierrehumbert (2003). Perspectives in the use of coloured Petri nets for risk analysis and accident modelling. *Safety Science,* **Vol 41,** pp. 445-463.

Weiegerinck Jan A.M., (2002). Introduction to the risk based design of safety instrumented systems for the process industry. *Seventh International Conference on Control, Automation, Robotics And Vision (ICARV'02)*. Singapore.S.E.

Yang, S.H., Y.J. Chung and H.C. Kim (2005). Assessment of the MDNBR enhancement methodologies for the SMART control rods banks withdrawal event. *Annals of Nuclear Energy.* **Vol 32**. pp, 1567-1583.