A DYNAMIC FAILURE EVALUATION OF A SIMPLIFIED DIGITAL CONTROL SYSTEM OF A NUCLEAR POWER PLANT PRESSURIZER

J.M.O. Pinto, jpinto@nuclear.ufrj.br
P.F. Frutuoso e Melo, frutuoso@nuclear.ufrj.br
Universidade Federal do Rio de Janeiro, Av. Brigadeiro Trompowsky – CT, Rio de Janeiro, Brazil

P.L.C. Saldanha, plsaldanha@gmail.com, pedroabeu@gmail.com
Associação Brasileira de Ensino Universitário-UNIABEU – Nova Iguaçu, Rio de Janeiro, Brazil

Abstract. *Given the increasing use of digital systems in nuclear power plants, a specific approach to reliability and risk analysis has been required. The digital system reflects many interactions between hardware, software, process variables, and human actions. At the same time, the software, does not have a reliability approach as well-defined as the one existing for the other physical components of the system. Then, its reliability analysis is still under development due to difficulties arising from the complexity, flexibility and interactions present in such systems.The traditional approach of using fault trees is static and does not approach the dynamic interactions in such systems, such as delays in capture and processing information, memory, logic loops, system states, etc. It is necessary to find a reliability methodology that takes into account these issues without violating the existing requirements concerning safety analysis, such as: ability to distinguish between common-cause failures, availability of relevant information to users, like minimal cut sets, and failure probabilities as long as the possibility of incorporating the results into existing probabilistic safety assessments (PSA).One approach is to trace all the possible errors of the digital system through dynamic methodologies. The DFM (Dynamic Flow-graph Methodology) is one of the methodologies that better meets the requirements for modeling dynamic systems. It discretizes the most relevant variables of the analyzed system in states that reflect their behavior, sets the logic that connects them through decision tables and finally performs a system analysis, aiming, for example, the root causes (prime implicants) of a given top event of failure. Three aspects have been addressed, the modeling of the system itself, the incorporation of results to probabilistic safety analyses and identification of software failures.To illustrate the DFM, a simplified digital control system of a typical PWR pressurizer has been considered. The DFM has been effective in modeling the interactions of the various components of a digital system. Through the prime implicants, it allows the visualization of the system possible states, failed or not. Its deductive analysis allows an efficient study of failures. Its inductive analysis can be used for the mitigation of failures found in deductive analyses and for the verification of system specifications. The results have shown that the methodology provides an efficient failure analysis of a digital system exhibiting all possible interactions between its components. It also provides an efficient way for developing Failure Modes and Effects Analyses (FMEA) for these systems, as well as fault trees that can be incorporated into existing PSAs. Moreover, DFM identifies failures strictly related to software, thus improving its reliability.*

Keywords*: Digital Systems, DFM, Software, Probabilistic Safety Analysis*

1. INTRODUCTION

The Risk Informed Decision Making (RIDM) for the process of regulatory decision-making represents a philosophy by which the results and decisions from risk assessment are considered along with deterministic approaches to establish requirements that better direct the attention of licensees and regulatory bodies to plant design and operation consistent with their responsibility for the safety and health of the public.

The RIDM extends and improves the deterministic processing as it is an integrated and structured decision making where all the insights and requirements that relate to safety or regulatory actions are considered to arrive at a decision (reconciliation deterministic and probability). Techniques such as Probabilistic Safety Analysis (PSA) can be used to ensure compliance with these principles.

Most nuclear plants have already PSAs for assessing the potential vulnerabilities of accident initiators from the point of view of RIDM, usually performed for supporting plant operation, maintenance, and licensing.

The development in the area of instrumentation and control (I & C) has been very fast over the past 30 years. Digital I & C with improved performance have been adopted in various industry sectors. The I & C system in a nuclear plant performs several tasks, which are carefully and formally structured, allowing each role of I & C to be identified with their goals of safety and control.

I&C systems, analog and digital, monitor, manage and protect critical equipment and processes of the plant to ensure that the plant operates safely and reliably. I&C systems carry out different tasks to perform these functions. Analog systems perform instructions through hardware, while digital systems perform their functions through software.

The current guidance regarding the evaluation of digital upgrading projects remains largely deterministic and does not take advantage of PSA: a method that meets all requirements for modeling the reliability of digital I & C systems

has not yet been defined (Guarro *et al*. 2007). Methods for identifying failure modes of digital equipment, and modeling their effects and estimate their probabilities are still under development (Aldemir *et al*, 2006).

Research has been made to model the reliability of the new I & C Digital designs. One of the approaches to estimate the reliability of digital I & C is the use of dynamic methods. This work focuses on the assessment of the dynamic methods to incorporate the results into an existing PSA, in particular the Dynamic Flowgrafic Methodology (DFM).

The experience accumulated and reported in the literature indicates the Dynamic Flowgraph Methodology (DFM) - (Guarro *et al.* 2007) as the one that meets the most the requirements mentioned. The description of the interactions between the control system and other subsystems, as well as the process variables beyond the possibility of results incorporation into existing PSAs, makes this method more credible. It has already been used, for instance, to model dependencies between digital control systems and human errors (Guarro *et al.* 2009), failures of control systems in nuclear power plants (Yau *et al.* 2008), and failures in spatial digital control systems (Guarro *et al*. 1995).

Garrett and Apostolakis (2002) studied an approach to validate the safety requirements of digital systems based on DFM to do risk analysis. It is an approach developed for modeling and analyzing integrated hardware and software components of a system. The objective of the methodology is complementary to traditional approaches, which generally follow the philosophy of separating reliability analysis of hardware and software. These assessments can be used to identify unknown risks in the reactor control system. The method has been successful in identifying unknown failure mechanisms.

This paper presents an application of the DFM (Dynamic Flowgraph Methodology) to a digital control system proposed for current nuclear power plant pressurizers. The study presents the DFM modeling of the control system and its interactions with the controlled process. Three features discussed in the literature were taken into account in the analysis: system modeling from a holistic point of view, the considerations of dynamic interactions, and the incorporation of the failure analysis results to an existing PSA (Probabilistic Safety Assessment). The results have shown that the methodology provides an efficient failure analysis of a digital system exhibiting all possible interactions between its components. It also provides an efficient way for developing Failure Modes and Effects Analyses (FMEA) for these systems, as well as fault trees that can be incorporated into existing PSAs. Moreover, DFM identifies failures strictly related to software, thus improving its reliability.

2. THE DYNAMIC FLOWGRAPH METHODOLOGY

The model builds a causality and temporal network among its elements. Such elements are described below (Aldemir, 1987, Guarro *et al.* 1996):

1. Process Nodes (PN) - Represent the main physical continuous or discrete variables of the system. These variables are discretized in a number of states that reflect their behavior. The number of states can vary according to the system complexity.
2. Causality Edges (CE) – Elements that connect the process nodes showing the causality relationship among them in a qualitative way.
3. Transfer Boxes (TB) - Represent the functions, continuous or not, that relate the model variables. Demonstrate the causality relationship through decision tables. Decision tables are constructed through the empirical knowledge of the system, equations or simulations.
4. Transition Boxes (TT) – Take into account the variables dynamics through the definition of the time step which is the necessary interval of time for a variable to assume a certain value, according to other variables. It is used to describe software functions and clocks processing, for instance.
5. Condition Nodes (CN) – These are conditions of the process nodes.
6. Condition Edges (CO) - Connect the condition nodes to the transfer boxes or transition boxes. Similar to the causality edges.

The first step in building a DFM model consists in choosing the main elements of both the physical and control systems. They will become the process nodes of the model (PN). The discrete behavior of these variables is represented by the condition nodes (CN). The next step is to define the states of the variables that reflect their behavior. Then, these variables are connected to the transfer boxes (TB) and transition boxes (TT), reflecting the time and causality relationships between them. All the possible states combinations of the model variables are described through the decision tables, each one associated with its respective TB /TT.

At the end of the model building, the analysis can be carried out in two ways: through a deductive analysis, which consists in establishing a top event and tracking of all the smallest possible combinations of the parameters states that lead to it, or through an inductive analysis, which consists in the definition of starting events and analysis of their consequences. The first is used in failure analysis and resembles the process carried out in the construction of fault trees. The second is used in conjunction with the results of deductive analysis to reproduce failures found in the system and subsequent mitigations. It can also be used for the FMEA preparation.

The analysis consists in finding all the possible combinations of states present in the model tables, making simplifications when needed, and taking as a starting point the given top event (initial condition).

DFM works with the concept of prime implicants. These are logical representations similar to multivalued minimal cut sets found in fault trees (Guarro *et al*. 1996, Garret & Apostolakis, 2002, Yau *et al*. 1998). They also have a causality relationship similar to the results found in Failure Mode and Effects Analysis (FMEA).

The prime implicants represent the minimum combinations of the variables states sufficient to cause a top event of interest. The union of all those prime implicants is equivalent to the top event. Therefore, they can be used to represent the various states in which the system can be found (Yau *et al*. 1998).

Examples of DFM methodology and its details can be found in Guarro *et al*. (1995, 1996).

3. DFM MODELING FOR THE CASE STUDY

The case study system is based on a typical Westinghouse designed 626 MWe PWR pressurizer, which is responsible for maintaining the plant pressure. It is an electrically heated pressure vessel with zones containing steam and water. During the operation, the pressure is maintained at 157 bar by the heaters in the water zone. If the pressure drops due to variations in load or for transients reasons, heaters will come into operation one by one, providing steam in the respective zone, and consequently, increasing pressure. This process continues until the pressure reaches the nominal value of 157 bar. If the pressure increases, the group of sprays is demanded, condensing the steam and relieving pressure. These sprays inject water from the reactor cold leg.

If the pressure does not decrease (to about 166 bar), a relief valve is activated releasing steam into the relief tank. Finally, if the pressure reaches the design limit (around 175 bar), safety valves are activated, with the reactor already shut down, in order to ensure the system integrity.

The case study system contains the same philosophy of operation implemented by a control software in a microprocessor, sensors and actuators (a digital system), but with some simplifications and assumptions in the controlled plant.

The control system consists in heaters, sprays, a relief valve with one pilot valve and a safety valve with one pilot valve. The group of heaters and sprays work together. The failure modes considered for each component are: Failure On and Failure Off for the group of heaters and sprays, Failed High and Failed Low for the level sensor and Fail Opened and Fail Closed for the valves.

Figure 1 illustrates the proposed digital system. Table 1 summarizes the system control logic.

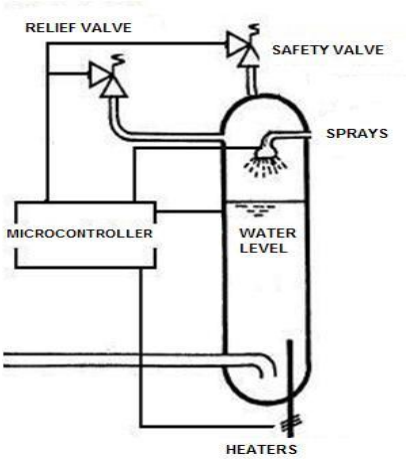

Figure 1. Proposed digital system

Table 1. System control logic

Pressure	Heaters	Sprays	Relief Valve	Safety Valve
Very Low	On	Off	Closed	Closed
Low	On	Off	Closed	Closed
Lower	On	Off	Closed	Closed
Normal	Off	Off	Closed	Closed
Higher	Off	On	Closed	Closed
High	Off	On	Opened	Closed
Very High	Off	On	Opened	Opened

The case study system has four mechanisms of pressure control triggered by a microprocessor that runs a control logic through a software. These actuators: heating control, spraying control and the two valve controls are the key parameters of the control system, and therefore they will become the process nodes (PN) in the DFM model. The pressure is the key parameter of the controlled process and therefore it will also become a PN. The states into which these variables are discretized are shown in Tab. 2. As the failure modes of components are to be considered, condition nodes (CN) must be defined in the model and associated to their respective process nodes. According to the considerations made in the previous section, one can establish the condition variables shown in Tab. 3.

Table 2. Model process nodes

Process Node (PN)	**State**
Pressure	Very High (169 – 175 bar)
	High (166 – 169 bar)
	Higher (160 – 166 bar)
	Normal (156 – 160 bar)
	Lower (148 – 156 bar)
	Low (140 – 148 bar)
	Very Low (131 – 140 bar)
Relief valve	Opened
	Closed
Safety Valve	Opened
	Closed
Heaters	On
	Off
Sprays	On
	Off

Table 3. Model condition nodes

Condition Node (CN)	**State**
Sensor State	Failed High
	Normal
	Failed Low
Heaters State	Failed On
	Normal
	Failed Off
Sprays State	Failed On
	Normal
	Failed Off
Relief Valve State	Failed Opened
	Normal
	Failed Closed
Safety Valve State	Failed Opened
	Normal
	Failed Closed

The next step consists in interconnecting the model variables through the transfer boxes and transition boxes. Each of these elements has an associated decision table showing the causality relationship that exists between the variables. Tables 4 and 5 represent, respectively, the transfer box (TB) decisions that control the group of heaters and relief valve logic of action. They were drawn up by inspection from the system control logic. Table 6 illustrates part of the main decision table of the model associated with the only transition box (TT) that exists. This table shows the change in pressure due to the performance of the control mechanisms and it has been obtained through simulation.

Table 4. Model CTA 1

Sensor State	Pressure	Heaters
Normal	Very High	Off
	High	Off
	Higher	Off
	Normal	Off
	Lower	On
	Low	On
	Very Low	On
Failed Low	-	On
Failed High	-	Off

Table 5. Model CTA 2

Sensor State	Pressure	Relief Valve
Normal	Very High	Opened
	High	Opened
	Higher	Closed
	Normal	Closed
	Lower	Closed
	Low	Closed
	Very Low	Closed
Failed Low	-	Closed
Failed High	-	Opened

Table 6. Model CTR 1

Pressure	Heaters	Sprays	Relief Valve	Safety Valve	Pressure
Very Low	Off	Off	Closed	Closed	Very Low
	Off	Off	Closed	Opened	Very Low
Low	Off	On	Opened	Opened	Low
	On	Off	Closed	Closed	Lower
Normal	On	Off	Opened	Opened	Lower
	On	On	Closed	Closed	Lower
Very High	On	On	Closed	Opened	Lower
	On	On	Opened	Opened	Normal

The DFM model provides a quantitative analysis of the results from the state probabilities of its variables. Using the failure data from IEEE (1984) and the probability distribution estimated for the pressure, these probabilities were estimated as described below and are shown in Tab. 7.

To control devices in continuous mode, one year of operation time in a nuclear power plant has been considered in the unreliability computation. For control devices in demand mode, one demand of operation has been considered. Generic failure modes for each device have been considered. The pressure probabilities in each state were calculated from the probability density function in each interval.

Table 7. Model variables probabilities

Variable	State	Probability
Level Sensor	Failed High	0.033
	Failed Low	
Heaters	Failed On	0.018
	Failed Off	
Sprays	Failed On	0.046
	Failed Off	
Relief Valve	Failed Opened	0.004
	Failed Closed	
Safety Valve	Failed Opened	0.007
	Failed Closed	
Pressure	Very High	< 10E-166
	High	< 10E-96
	Higher	< 10E-14
	Normal	9.0 10E-1
	Lower	9.2 10E-2
	Low	< 10E-81
	Very Low	< 10E-295

4. ANALYSIS OF THE DFM MODEL

The DFM model can be analyzed in two ways: through a deductive approach, consisting in defining a top event of interest and tracking the causes that have led to it, or by an inductive approach, where initial conditions are given and their consequences are searched for. For the system failure analysis, the deductive mode is more appropriate. In the present system, the top event "Pressure Very Low", representing one of the failures in the pressurizer control and later reactor trip, is one of the top events of interest.

For this analysis, the toolset DYAMONDA ® that has been made available by ASCA ® Inc was utilized (Guarro *et al.* 1996). In the analysis of "Pressure Very Low", one searches the smallest number of combinations of the key variables states in the system, or prime implicants, that lead to the failure top event, by using the toolset sentence:

• Pressure Very Low @ t = 0

where t = 0 is a toolset notation, indicating that the top event occurs at the end of the analysis time. The results are 32 prime implicants. But, assuming that the analyst has some information about the plant status before the analysis, these latter can serve as boundary conditions. Assuming that the information consists of a proper work of the level sensor and heaters off and running, the results are the prime implicants shown in Tab. 8.

Table 8. Prime Implicants for “Pressure Very Low”

P=1.0609E-06
Pressure was Normal at time -1
Sensor State was Normal at time -1
Heaters State was Normal at time -1
Safety Valve State was Failed Opened at time -1
Relief Valve State was Failed Opened at time -1
Sprays State was Failed On at time -1

For prime implicant number one, failures in the valves and sprays lead the pressure to "Very Low". Not even the fact that the level sensor is in "Normal", as is the group heaters, allows an increase of pressure to compensate the drop provided by other mechanisms.

Here again, t =- 1 indicates any time before the performance of any of the control devices. It can be seen through the probability value associated with the prime implicant that its occurrence probability is very low. The probability values are very important due to their use for defining maintenance policies where adequate classifications of the major failures are done.

The DFM deductive analysis allows the visualization of interactions among all system components in a dynamic way considering, for example, the state sequencing. These are important aspects in modeling digital systems. In the prime implicant of Tab. 8, for example, there are interactions between the control system, consisting of sensors, actuators and software (implicit in the logic that drives some decision tables), and controlled process (variable pressure).

Inductive analyses could also be run in the model in order to certify the design of the system and to establish studies of failure modes (FMEA, for example).

Once built, the DFM model can be analyzed several times through its two modes, making it an effective tool in the study of failures and system specifications.

5. INCORPORATION OF THE EXISTING REPORT RESULTS IN THE SAFETY ANALISYS

The replacement of analog loops by digital systems is gradual and several digital systems still coexist with analog systems in various industrial plants. It is therefore necessary that the results of failure analyses of digital systems can be incorporated into existing probabilistic safety analysis reports. Only then it will be possible, for example, to perform uncertainty and importance analyses on these results, such as those carried out for other fault trees.

The results of the DFM meet this requirement. One can incorporate them into a PSA by using a traditional tool in failure analysis, as the SAPHIRE code (Beck *et al*. 2008), for instance. This procedure is illustrated below.

The input data for the SAPHIRE code requires a text file (written in a specific format) with an extension of the kind ".ftl" to be imported. Let us consider, as an example, the results of the top event "Pressure Very Low". The input file would be written as follows:

```
jonathan,pressure_very_low=
pressure_very_low                          or
pressure_very_low_subsystem_1
pressure_very_low_subsystem_2
pressure_very_low_pressurizer
etc
...
pressure_very_low _pressurizer             or
prime_implicant_1

prime_implicant _1                         and
pressure_normal_t-1
heaters_normal_t-1
sensor_normal_t-1
sprays_failed_on_t-1
reliefvalve_failed_opened_t-1
safetyvalve_failed_opened_t-1
```

where "pressure_very_low" is the top event, "pressure_very_low_subsystem1, 2, etc ..." represents the trips of "Very_Low" pressure in the other analog systems and "pressure_very_low_pressurizer" represents the trip of the digital pressurizer control.

Figure 3 illustrates the fault tree generated by the SAPHIRE code with this input data. Once constructed and attached, the fault tree branch for the discussed top event becomes part of the probabilistic safety assessment.

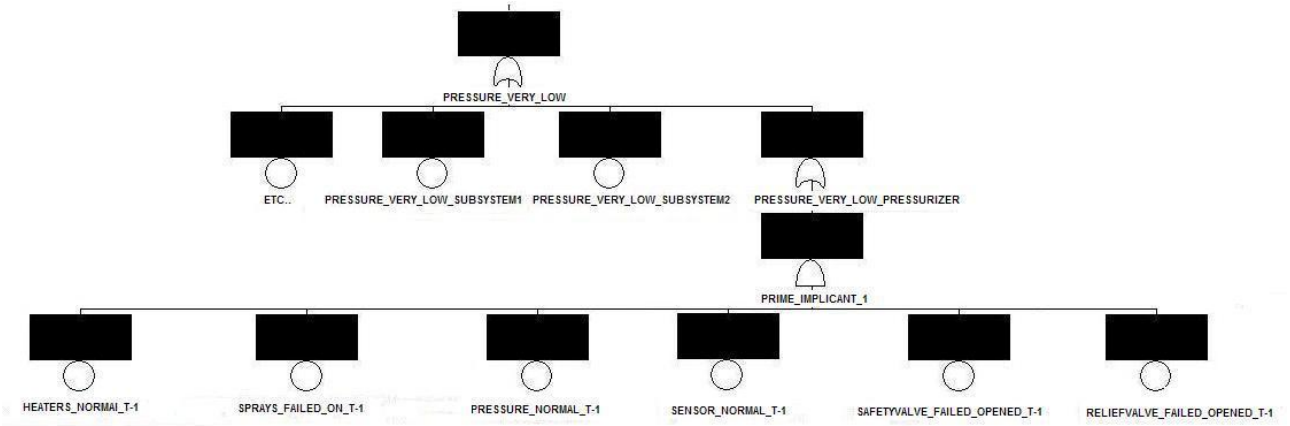

Figure 3. Fault tree branch related to the top event "Pressure Very Low"

6. CONCLUSIONS

This work applied the DFM (Dynamic Flowgraph Methodology) to model the reliability of digital systems. Two concerns in the literature were addressed: the modeling of the system itself and the incorporation of the methodology results into an existing PSA.

Through prime implicants, it allows the visualization of possible system states, failed or not. Its deductive analysis allows an efficient study of failures tracing the causes of a given top event. Its inductive analysis can be used in the mitigation of failures found in deductive analyses and for the verification of system specifications. It can also be used for FMEAs preparation, investigating the consequences of given initial conditions.

A limitation of the methodology is that the knowledge of the whole system both for modeling and for mitigations is necessary. But once built, the system can be analyzed for various failure modes and top events of interest. In the model construction, modularization techniques can be developed to make possible the use of templates and thus simplify the modeling process.

As many digital systems still coexist with analog loops, it is important that the results reported by any methodology can be incorporated into existing PSAs. Only then, uncertainty and importance studies, for example, can be developed for digital systems such as those performed for other systems in failure analysis. Future work on this subject includes the development of computational tools for the automatic inclusion of these results in existing PSAs.

Finally, as the main element of a digital system is the software, and the fact that it does not have a defined reliability approach (Stamatelatos, 2002), it is quite convenient the existence of a tool that enables the verification of faults and subsequent corrections in these elements. The DFM has proved to be a viable alternative through the use of its inductive mode combined with results obtained in the analysis by the deductive mode. In this sense, it is possible to perform several software design tests for debugging purposes. However, one needs full knowledge of the code and the logic involved. Future work will be performed on developing tools that generate inputs to the software using the inductive mode of DFM in order to increase the reliability of these elements with the elimination of programming flaws.

7. REFERENCES

Aldemir, T., 1987, "Computer-Assisted Markov Failure Modeling of Process Control Systems", IEEE transactions on Reliability, R-36, pp. 133-144.

Aldemir, V., Bucci, P., Mangan, L.T., E.A.L., 2006, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plants", NUREG/CR-6901, U.S Nuclear Regulatory Commission, Washington, DC, USA.

Beck, S.T., Wood, S.T., Smith., C.L., E.A.L, 2008, "Systems analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE) Summary Manual", NUREG/CR-6116, U.S Nuclear Regulatory Commission, Washington, DC, USA.

Garret, C.J., Apostolakis, G., 2002, "Automated Hazard Analysis of Digital Control Systems", Reliability Engineering and System Safety, 77, pp. 1-17.

Guarro, S., Aldemir, T., Yau, M., 2007, "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments", NUREG/CR-6942, U.S Nuclear Regulatory Commission, Washington, DC, USA.

Guarro, S., Aldemir, T., Mandelli, D., 2009, "A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems", NUREG/CR-6985, U.S Nuclear Regulatory Commission, Washington, DC, USA.

Guarro S., Yau M., Apostolakis G., 1995, "Demonstration of the Dynamic Flowgraph Methodology using the Titan II Space Launch Vehicle Digital Flight Control Software", Reliability Engineering and System Safety, 49, pp. 335-353.

Guarro, S., Yau, M., Motamed, M., 1996, "Development of Tools for Safety Analysis of Control Software in Advanced Reactors", NUREG/CR-6465, U.S Nuclear Regulatory Commission. Maryland, USA.

IEEE, 1984, "Equipment Reliability Data for Nuclear-Power Generating Stations", New York, IEEE and John Wiley & Sons.

Stamatelatos, M., 2002, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners", chapter 11, NASA, Washington D.C, USA.

Yau, M., Apostolakis, G., Guarro, S., 1998, "The Use of Prime Implicants inDependability Analysis of Software Controlled Systems", Reliability Engineering and System Safety, 62, pp. 23-32.

Yau, M., Guarro, S., 2008, "A Benchmark System for Comparing Reliability Modeling Approaches for Digital Instrumentation and Control Systems", Nuclear Technology, 165, pp. 53-95.

8. RESPONSABILITY NOTICE

The authors are the only responsible for the printed material included in this paper.