Modeling digital I&C systems for PRA with Coloured Petri Nets

Gilles Deleuze, Nicolae Brinzei

MODELING DIGITAL I&C SYSTEMS FOR PRA WITH COLOURED PETRI NETS

Gilles Deleuze
EDF R&D
1 Avenue de Gaulle, 92141 Clamart, France.
gilles.deleuze@edf.fr

Nicolae Brinzei
CRAN - CNRS UMR 7039, Université de Lorraine
2 Avenue de la Forêt de Haye, 54518 Vandoeuvre-lès-Nancy, France.
nicolae.brinzei@univ-lorraine.fr

ABSTRACT

The object of the article is the estimation of dependability and other probabilities of interest for digital systems, e.g. protection system of nuclear plants. The system under study is composed of four divisions, all with identical hardware. Colored Petri Nets are used because of their capability to model complex digital systems and assess their dependability. The Atwood model is also implemented into the CPN model. It represents Common Cause Failures that are contributing to the residual risk of unavailability. Assumptions related to hardware reliability and system logic, maintenance and repairs are taken into account in the model that is dynamic. We explain in this article how the Atwood model can be modified to "direct" non-lethal CCF on certain parts of the system and take into account the different possible origins of CCF. This extension permits to avoid the assumption of uniform distribution of non-lethal shock on the components and to represent some benefits of diversity and separation between divisions.

Key Words: I&C Systems, PRA, Colored Petri Nets

1 PROBABILISTIC MODELING OF LARGE DIGITAL SYSTEMS

1.1 Specific Issues

Digital Instrumentation and Control systems (I&C) systems have a key role for regulation and safety of nuclear power plants. Their characteristics are a large number of more or less similar components, a high level of redundancy and a complex logic of vote. Because of the system design, and because digital components are more reliable than the analog or electromechanical systems they replace, the impact of independent failures are limited, and Common Cause Failures represent the largest part of failure risk. Also, as most of the functions are protective actions, they are in waiting mode; failures may be present and undetected for a long period of time, even in digital systems which have improved failure detection capabilities.

1.2 Common Cause Failures

A CCF can occur in operational or on demand modes and affect groups of identical or similar redundant components having the same function and operating under comparable conditions. The so-called Alpha Factor and Beta Factor models are the most widely used model for taking into account CCF within various types of systems in nuclear power plants [9] and, more generally, in power systems [3]. The Beta Factor model implies the failure of whole set of components when a common cause event occurs. This definition

is used when the system is composed of only a few components. However when the system is composed of dozens of identical or similar components, the assumption of failure of whole set of components, when a CCF occurs, is very conservative. Thus, the concepts of partial and lethal shocks of Binomial Failure Rate model, defined by Atwood, are very well adapted to represent the potential effects of stress factors on electronic hardware.

1.3 Atwood Model

In this section, we introduce the Atwood model [1]. It that takes into account independent failures, and CC F failures due to shocks that affect all or only some components. Two kinds of shock failures are defined: lethal shocks and partial (or non-lethal) shocks. In a large redundant systems with N components, a shock is assumed to be non-lethal when it affects k components among N with $1 \leq k < N$. Each component has then a conditional probability ρ of failure. A shock is lethal when it affects all components. Individual failures, non-lethal and lethal shocks are assumed to follow independent processes. The occurrence frequencies of shocks (noted μ for non-lethal shocks and ω for lethal shocks) are assumed to be constant. For a specific component in a group of N components, the total failure rate is given by:

$$\lambda_{TOT} = \lambda_{IND} + \omega + \mu . \sum_{k=1}^{N} \binom{N-1}{k-1} \rho^{k} (1-\rho)^{N-k} \quad (1)$$

λ_{IND} is the rate of independent failures. The capability to represent CCF implies the use of three parameters (μ, ρ, ω), whatever the size of the CCF group is. The default values usually used to estimate these parameters are:

$\alpha = \frac{\mu}{\lambda_{TOT}} = 0{,}405$ (rate of non-lethal shocks),

ρ = 0,2 or 0,33 or 0,5 (conditional probability of component failure in a non-lethal shock),

$\beta_{letal} = \frac{\omega}{\lambda_{TOT}} = 5.10^{-3}$ (rate of lethal shocks).

2 SYSTEM UNDER STUDY – DESCRIPTION AND ASSUMPTIONS

The system under study is a protection system, composed of four divisions of identical hardware. It is a pa rt of the defense in depth of a nuclear power plant.

2.1 System Architecture

This system contains four identical divisions. They are physically separated, where each division is composed of five processing units (APU), as shown in figure 1. The APU 0, 1 and 2 compose the subsystem A (SSA). The APU 3 and 4 compose the subsystem B (SSB). A control function, there is implemented twice, in an APU of SSA and in an APU of SSB, with different inputs and treatment. Their outputs must be identical in the normal operating mode (functional diversity).

For the I&C signals of interest for PSA, two kinds of electronic modules, C1 et C2, are used by each APU. Each APU contains one C1 module. The APU 0 and 1 contain four C2 modules, and the APU 3, 4 and 5 contain three C2 modules. These electronic modules are used for reception, processing and emission of signals. Groups of APU (GAPU) are defined: one group contains all APUi (i [0,4]) of the four divisions.

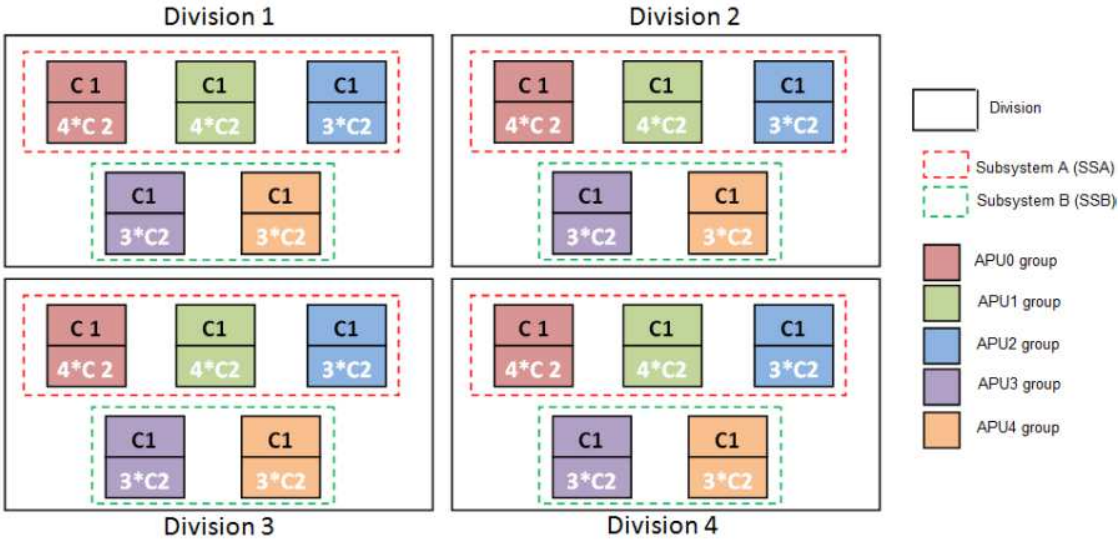

Figure 1: Architecture of the case study I&C system

2.2 Assumptions for the electronic modules

The modules of an APU are considered as a series system. When a failure is detected by a self-test (SA), the detection time is considered null. When a failure is not detected by a self-test (NSA), then it is detected offline during a periodic test. For a given division, these periodic tests take place for every period of 18 months. So every 6 months, one division among four is tested during the periodic tests. After the periodic tests, the failed modules are repaired. According to the supplier of electronic modules, the coverage rate of self-tests is 100%. To be more conservative; we added to the model the non-detected failures by self-test (NSA failures) in order to take also into account the errors due to operation; e.g. parameters setup or installations of modules different than the nominal conditions specified. Thus the coverage rate (a) drops to 85%. The total failure rate of the modules remains identical ($\lambda_{IND} = \lambda_{SA} + \lambda_{NSA}$). The rates of detected failures (λ_{SA}) and non-detected failures (λ_{NSA}) are adjusted by the equations:

$$\lambda_{SA} = a.\lambda_{IND} \text{ and } \lambda_{NSA} = (1-a).\lambda_{IND} \quad (2)$$

2.3 Assumptions for system states and logic

The hazardous event is the unavailability of an I&C signal. The occurrence of this hazardous event is based on the voting logic of the APU:

- An APU fails when a module C1 or C2 fails,
- A group of APU (GAPU) fails when 3 out of 4 APU fail (2oo4),
- A subsystem (SSA or SSB) fails when a GAPU failed,
- The system fails when two subsystems fail (1oo2).

We assume that the mission time of the protection system is ten years, and it becomes as good as new after being retrofitted during the decennial maintenance operations of the nuclear plant. System unavailability can occur anytime during the ten years. During this time interval, the system may recover without being as good as new, with some electronic modules still in fail state.

3 SYSTEM MODELING USING COLORED PETRI NETS

3.1 Benefits of Petri Nets for this modeling

The model should be able to represent the dynamic sequences of states of large digital systems and assess dependability figures. Markov chains or Petri Nets have this capability. The β-factor model has already been integrated in Markov chains [8] and in the classical Petri Nets [11]. The main drawback of these models is the combinatorial explosion of their size when the modeled system is large. To remediate this drawback, we used the Colored Petri Nets (CPN) type [6], [7]. It is a discrete-event modeling language combining the capabilities of Petri Nets with the capabilities of a high level programming language. The main difference is that the CPN tokens can have different colors representing data types (e.g. Boolean, integer or more complex data structure).

Hierarchical CPN. Furthermore, individual CPN models can be hierarchically related to each other in a formal way, i.e. with a well-defined semantics. CPN model hierarchy is realized through substitution transitions. The idea is to associate a transition to a more complex CPN (a module), which gives a more precise and detailed description of the activity represented by the substitution transition (represented by a double rectangle, e.g. in figure 2). The places connected to a substitution transition transmit a given marking from a high level (level of substitution transition) to a low level (level of module) and vice versa. CPN concept of hierarchy allows us to propose a modular modeling approach for a complex system, based on generic modules that can be instantiated as often as needed.

Timed CPN. Additionally, the probabilistic dependability assessment requires to take account of the time dependence of the system. In a timed CPN, the time is given by a global clock. In addition to their color, the tokens contain a time value, also called a time stamp. When a transition is enabled, it is fired and changes the time stamps of tokens which are deposited in its output places. In these places, the tokens remain frozen and cannot be used to enable other transitions until the current model time (given by the global clock) is smaller than their time stamps. As soon as the time stamp of the tokens is greater than or equal to the current time model, these tokens can enable other transitions which are instantly fired. In other words, the time stamp describes the earliest model time from which a token can be used. This permits to represent periodic tests, failures and repairs events.

3.2 Drawbacks

Low readability of Petri Nets. This general drawback of Petri Nets is reduced by using hierarchical CPN.

Difficulty of verification. A Monte-Carlo simulation can be done for a partial verification of the model, by comparing two parameters estimation of Atwood model: an analytical, and a Monte-Carlo simulation from the CPN [2]. A more exhaustive verification can be done by a state space method. The idea is to compute all reachable states and state changes of the CPN model and to represent them as a directed graph, where nodes represent states and arcs represent events. From a constructed state space, it is possible to check a large set of questions concerning the behavior of the system, such as absence of deadlocks, a possibility to be able to reach a given state. This formal verification of a CPN has been done for some specific safety properties of I&C systems [10].

4 MODELING OF THE SYSTEM UNDER STUDY BY CPN

We used a modular approach. The high level CPN model (figure 2) is composed by the following modules:
-CCF generation (left box)
-System representation (center box)
-State system description (right box)
Thus, each of its divisions is modeled by means of a substitution transition (into center box) at the high level of the system, in the Figure 2.

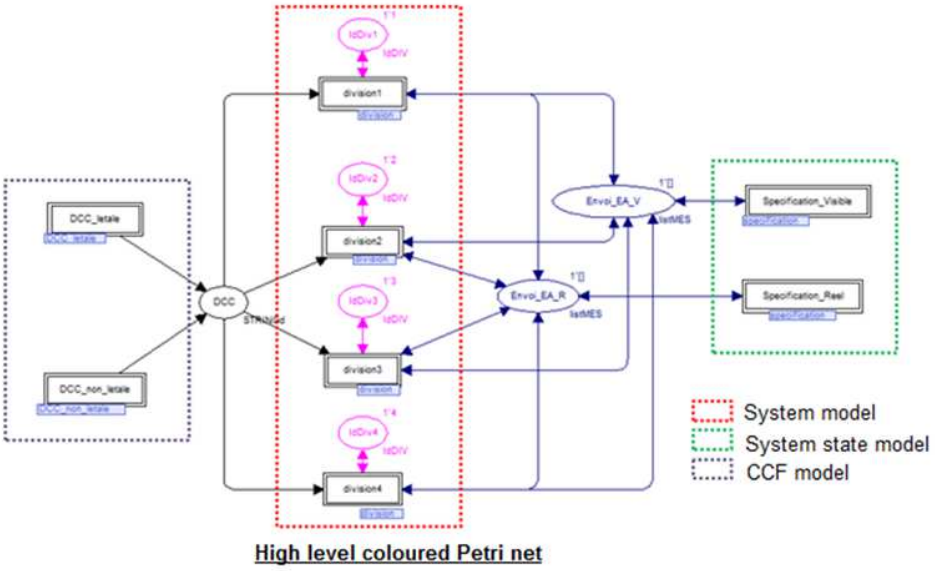

Figure 2: High level colored Petri net of the I&C system.

The state of an APU is determined by the state of its modules (available or unavailable). Once the state of a module changes, the new state of APU is sent to the specification that determines the state of the whole I&C system. The CCF are transmitted to the APU and to the modules by means of CPN places (socket places).

An electronic module has 3 possible states: *operational*, *failed and non-detected*, *under repair*. It fails after one of 4 events:

- independent failure detected online by a self-test
- independent failure detected offline in periodical-tests
- non-lethal CCF detected online and lethal
- non-lethal CCF detected offline in periodical tests

The repair time is calculated using an exponential function. As soon as the module is repaired, its state changes immediately to the *operational* state. The next occurrence of the independent failures detected online and offline are also calculated. The models of electronic modules are generic. Only the numerical values of parameters (failure and repair rates) are different between different types of modules.

4.1 System state modeling

Using the information about the state (*available/unavailable*) of the five APU, it is possible to determine the state of the I&C system using a dedicated part of the CPN. The system state is represented by a token whose color is composed of five Booleans, each of them representing the state of one APU. The different configurations on the transitions guards define the conditions of availability/ unavailability of the system.

The whole CPN model has 685 transitions and 504 places. Although the model size is large, the use of hierarchy and colors concepts have resulted in a modular and readable model obtained through the instantiation of generic templates. An equivalent classical Petri net model for the same I&C system would have several thousand places and transitions.

4.2 Lethal CCF modeling

Lethal CCF are modeled by a dedicated part of the CPN, it corresponds to the substitution transition *DCC_letale* of the figure 2. The firing of a transition determines the occurrence time of the lethal shock using an exponential function. A lethal CCF affects N components of the system and is always detected online. Thus, N temporized tokens are issued with a color indicating a detected failure state. A transition generates the next occurrence time of a lethal shock.

4.3 Non-lethal CCF modeling

Non-lethal CCF are modeled by a dedicated part of the CPN, it corresponds to the substitution transition *DCC_non_letale* of the figure 2. A place contains the number of electronic modules N in the system. The firing of a transition set the number of electronic modules N of the system in the place and set N tokens in another place. The transition is fired N times. A random value is drawn, using the uniform distribution. If the value is lower than conditional probability ρ of the Atwood model, the module is shock sensitive. The firing of a transition determines the occurrence time of the non-lethal shock using an exponential function. At the same time, it specifies if it is detected or not by a self-test, from a random value drawn using the uniform distribution. If the value is lower than the coverage rate of self-tests, the failure is detected. The firing of a transition assigns the occurrence time of CCF and the variable characteristic of failure detection to each token of the system that is shock sensitive. A transition removes the tokens representing modules that are not shock sensitive. A transition generates the next occurrence time of a non-lethal shock and redefines the number of modules, which are shock sensitive.

5 EXAMPLES OF PROBABILISTIC ESTIMATIONS

5.1 Probabilistic measures of interest

The timed hierarchical CPN using an Atwood CCF model may compute safety measures of interest for PSA like the probability of failure on demand (Pfd), the spurious rate and the probabilistic parameters for CCF (Beta Factors, Alpha Factors…). Another measure is the MTFF (Mean Time To First Failure). Note that spurious frequency is a relevant measure of interest, that just requires a different CPN modeling or a complement to the CPN modeling used here to estimate Pfd.

This simulator may be used for various purposes. In [2], we explain how it can be used to assess the difference between the *observed Pfd*, taking into account undetected failures, and the *real Pfd* that could be estimated with a perfect knowledge of the failure conditions. We explain in this article how the Atwood model can be modified to "direct" non-lethal CCF on certain parts of the system and take into account the different possible origins of CCF. This extension permits to represent some benefits of diversity and separation between divisions.

5.2 Oriented CCF propagation.

Atwood model assumes that each element of a CCF group has the same failure probability (ρ) due to non-lethal shocks. This is consistent with the basic assumption of similarity of elements in a CCF group. However, practically, in the case of a large CCF group, this assumption of same failure probability due to a shock is questionable. Indeed, in the Atwood model, a shock can be considered as an external stress, and the failure probability ρ represents the vulnerability of the elements of the CCF group to the stress. Practically, in the case of a large redundant digital system, structural features imply that vulnerabilities are not identical among similar hardware elements of a CCF group: physical or electrical separations, connection to different networks, diversity of applicative functions implanted in the hardware, differences in operations…. A first solution may be to split the large CCF groups in smaller groups for which the similarity assumption is relevant. However, this may be difficult to handle without a significant increase in the size of the model. We propose here to use the potential of a CPN modeling to introduce small differences

of behavior under shocks between the components inside a CCF group. In other words, we modify the generation of non-lethal CCF for simulating the asymmetries in their propagation, so-called *"Oriented CCF"*.

We present here a simple example. We assume that some nonlethal shocks affect a CCF group of N electronic modules with identical hardware belonging to the system. We assume that as an average, a non-lethal shock affects the modules with a conditional probability p. The expected number of affected elements is N.p. We consider that practically the system is built from two subsystems, A and B, using the same hardware, but having differences in term of software and using their own networks. Thus, the set of N components can be divided in two sub-sets SSA (for subsystem A) and SSB (subsystem SSB), containing respectively N_A and N_B components, such as $N_A + N_B = N$. Let be x_A (respectively x_B) the probability that a component of SSA (respectively SSB) is affected, given that a non-lethal shock occurred. Using mathematical expectation, we have:

$$N_A . x_A + N_B . x_B = N.p \quad (3)$$

We define CCF proportion affecting SSA (respectively SSB) as x_A (resp. x_B) such as $p_A + p_B = 1$. The parameters p_A and p_B permit to set the level of dissymmetry between the subsystems in term of CCF propagation. Thus, we can estimate x_A and x_B:

$$x_A = N.p. p_A / N_A \quad (4) \text{ and } x_B = N.p. p_B / N_B \quad (5)$$

x_A and x_B are affected to the CPN tokens of the modules of each subsystem, to represent respectively the different vulnerabilities of SSA and SSB modules.

Table 1 shows the results in term of repartition of failure combinations and MTFF (Mean Time to First Failure), for three types of asymmetry. 10,000 chronicles of 10 years are simulated. A chronicle ends at the first occurrence of a system failure. The conditional probability of failure of a module in a non-lethal shock is $\rho = 0,2$. The frequency of non-lethal shocks is arbitrary fixed at one shock per year, i.e. $\mu = 1.14 \cdot 10^{-1}$ /hr. Lethal shocks are not simulated. The sum of failures combinations is equal to the total number of chronicles (10000) for a given CCF orientation.

Table 1: Repartition of failure combinations and MTFF, for three types of asymmetries

	CCF Orientation (SSA) p_A	**0.1**	**0.2**	**0.3**	**0.4**
	CCF Orientation (SSB) p_B	**0.9**	**0.8**	**0.7**	**0.6**
	Total number of failures situations	10000	10000	10000	10000
System unavailability is due to …	**… CCF**	**9404**	**9723**	**9787**	**9823**
	… combination of independent detected failures	3	0	1	1
	…combination of independent un detected failures	21	9	9	6
	… combination of detected and undetected independent failures	77	46	42	37
	… combination of CCF and independent detected failures	8	6	1	1
	… combination of CCF and independent undetected failures	487	216	160	132
	Relative MTFF	1	0,58	0,44	0,39

We observe that MTFF increases with the asymmetry. This is logical, given the assumption that the system is available even if one subsystem fails (1oo2 logic). Also, independent failures combinations without CCF are very unlikely causes of system failure, due to the high level of redundancy. Independent failures detected offline lead more easily to system failure than the ones detected online by around one order of magnitude.

6 CONCLUSIONS

In this article, we have presented how to use efficiently Colored Petri Nets (CPN) to model a digital I&C system. This approach has been applied to a representative case of protection system of a nuclear power plant. The simulation, based on a CPN mode,l and assumptions of the Atwood model for CCF, permit to estimate various probabilistic parameters, useful for PSA. This CPN model allows the inclusion of combinations of independent failures, lethal and non-lethal CCF, and propagation asymmetry of non-lethal defects. It allows to release the assumption regarding the uniform distribution of non-lethal shocks all of the components and to take into account the benefit of diversity between the system parts. Also, as the Atwood model may not be a fully satisfactory representation of CCF in digital I&C, the next step could be to represent the various modes of CCF as described in [5], [4] .

7 ACKNOWLEDGMENTS

The authors thank Alexander Wigg from EDF SEPTEN for his support.

8 REFERENCES

[1] *Estimators for the Binomial Failure Rate Common Cause Model*. C. L. Atwood, Report No.EG6-EA-5112. March 1980.

[2] *Common cause failures modelling by means of coloured Petri nets for dependability assessment of a control system of nuclear power plant*. N. Brinzei, G. Deleuze, N. Villaume, J.F. Petin. ESREL 2014 European Safety and Reliability Conference. Wroclaw, September 2014.

[3] Bricman-Rejc, Z., M. Cepin, & A. Sitdikova. *Estimating common-cause failures parameters within power system reliability analysis*. European Safety and Reliability Association, ESREL 2013, Amsterdam, pp. 2841–2846.

[4] *A taxonomy for the FMEA of digital I&C protection systems*. H. Bruneliere, G.Deleuze, N Thuy, C.Smidts, PSA 2013, Columbia.

[5] *Failure modes taxonomy for reliability assessment of digital I&C systems for PRA*. OECD/AEN WGRisk Task DIGREL. 12 january 2014.

[6] *Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use* (Volume 1), Volume 1. Jensen, K.. Springer Verlag (1997).

[7]. *Coloured Petri nets: modeling and validation of concurrent systems*. Jensen, K. & L. Kristensen .Springer-Verlag New York Inc (2009).

[8]. *Analysis of common cause failures in complex safety instrumented systems*. Technical note. Lilleheier, T. (2008).

[9] *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*. NUREG/CR-5485. A. Mosleh, D. M. Rasmusson, F. M. Marshall, 1998.

[10] B. Pinna, G.Babykina, N.Brinzei, J.-F. Petin. *Deterministic and stochastic dependability analysis of industrial systems using Coloured Petri Nets approach*, ESREL 2013, European Safety and Reliability Conference. Amsterdam, pp. 2969–2977.

[11]. *Make your Petri Nets understandable: Reliability block diagrams driven petri nets*. Signoret, J.-P., Y. Dutuit, P.-J. Cacheux, C. Folleau, S. Collas, & P. Thomas. Reliability Engineering and System Safety 113 (2013), pp61–75.