Common cause failures modelling by means of coloured Petri nets for dependability assessment of a control system of nuclear power plant

Nicolae Brinzei, Gilles Deleuze, Nicolas Villaume, Jean-François Pétin

Common cause failures modelling by means of coloured Petri nets for dependability assessment of a control system of nuclear power plant

N. Brînzei
Centre de Recherche en Automatique de Nancy, CRAN UMR 7039
Université de Lorraine, Vandœuvre-lès-Nancy, France
CNRS, Vandœuvre-lès-Nancy, France

G. Deleuze
Électricité de France (EDF) R&D Management des Risques Industriels
1, avenue de Général de Gaulle, 92141 Clamart, France

N. Villaume
École Nationale Supérieure d'Électricité et de Mécanique
Université de Lorraine, Vandœuvre-lès-Nancy, France

J.F. Pétin
Centre de Recherche en Automatique de Nancy, CRAN UMR 7039
Université de Lorraine, Vandœuvre-lès-Nancy, France
CNRS, Vandœuvre-lès-Nancy, France

ABSTRACT: This paper presents an approach to assess the effects of common cause failures (CCF) on dependability of digital systems. Independent failures of system components and partial or lethal shocks are considered in a global CCF model, the Atwood model. The Coloured Petri nets (CPN) are used to modelize the digital system and the common cause failures. Based on the CPN, the parameters of Atwood model are estimated analytically and by Monte-Carlo simulation. Thereafter, the Atwood model of CCF is modified in order to represent the dominant failures propagation on some system components in the case of partial shocks. The assessment of system dependability, in the presence of CCF failures, becomes possible. This approach is applied to a representative instrumentation and control system of a nuclear power plant. The system is large with a high level of redundancy.

1 INTRODUCTION

Digital Instrumentation and Control systems (I&C) systems have a major role in the control and protection of nuclear power plants. These systems are characterized by a large size, a high level of redundancy and a complex logic of vote. Although digital systems and their components are more reliable than the analog systems they replace, some characteristics raise specific issues on the modelling and assessment of common cause failures (CCF). 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 β-factor model is the most widely used model for taking into account CCF within all types of systems, like nuclear power plants (US-NRC 1987) and, more generally, in the field of power system (Bricman-Rejc et al. 2013). It involves *the failure of whole set of components* when a common cause event occurs. This model 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.

The concepts of partial and lethal shocks are very well adapted to represent the potential effects of stress factors on electronic hardware. In the next section we introduce the Atwood model of CCF that takes into account independent failures of components and

CCF failures due to shocks that affect all or only some components. For dependability assessment, the CCF model must be integrated within a system model. Also, the system model must integrate the dynamic behaviour of the digital I&C systems. The Markov chains or Petri nets are such types of models and the β-factor model has been integrated in Markov chains (Lilleheier 2008) and in the classical Petri Nets (Signoret et al. 2013). The main drawback of these models is the combinatorial explosion of their size when the modelled system is large. To overcome this drawback, we propose to use the Coloured Petri Nets (CPN) for I&C systems modelling. The section three of this paper develops a CPN model for an I&C system and, also, for the CCF Atwood model. In the same section, firstly, we propose two approaches for parameters estimation of Atwood model and, secondly, we modify this model to represent asymmetry in CCF propagation oriented on some types of components. If for I&C modelled system only the hardware architecture is considered, the oriented propagation of CCF on this architecture takes into account the software and human aspects of functional safety analysis. Section four presents the probabilistic assessment of dependability indicators (PFD, MTTF) or of the impact of the oriented CCF. Finally, some conclusions and future outlook are presented.

2 MODELLING OF COMMON CAUSES FAILURES (CCF)

2.1 *The Atwood model*

The model introduced by Atwood (1980) considers that the system components are subject to two types of failures: independent failures and shock failures. 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 $1 \leq k \leq N$. A shock is lethal when it affects *all* components. In the case of a non-lethal shock, only the failure of some components is considered. Each component has then a *conditional probability p* of failure. Individual failures, non-lethal and lethal shocks are assumed to follow independent processes. The occurrence frequencies of shocks (denoted μ for non-lethal shocks and ω for lethal shocks) are assumed to be constant.

The failure rate of a specific component in a group of *N* elements, due to an independent failure or to a non-lethal shock is:

$$\lambda_1^N = \lambda_i + \mu.p.(1-p)^{N-1} \quad (1)$$

The failure rate of a group of *k* components from *N* with $1 \leq k \leq N$ due to a non-lethal shock is:

$$\lambda_k^{(N)} = \mu.p^k.(1-p)^{N-k} \quad (2)$$

The failure rate of *N* components due to a non-lethal and lethal shock is:

$$\lambda_N^N = \mu.p^N + \omega \quad (3)$$

For a specific component in a group of *N* components, the total failure rate is given by:

$$\lambda_{TOT} = \lambda_{IND} + \omega + \mu.\sum_{k=1}^{N} C_{N-1}^{k-1} p^k.(1-p)^{N-k} \quad (4)$$

The Atwood model is considered representative for the phenomena leading to multiple failures in the large digital I&C systems. It allows to represent CCF affecting only a part of the all components of the system. However, it introduces three parameters to estimate p, μ and ω. The results will be sensitive, of course, to the values used, usually given by expert opinion or by using default values. The default values usually used for these parameters are the following:

- $\alpha = \frac{\mu}{\lambda_{TOT}} = 0.405$: the rate of non-lethal shocks.
- $p = 0.2\ ou\ 0.33\ ou\ 0.5$: conditional probability of component failure in a non-lethal shock.
- $\beta_{letal} = \frac{\omega}{\lambda_{TOT}} = 5.10^{-3}$: the rate of lethal shocks.

Later, in this work, we propose to determine the values of these parameters by two approaches: an analytical one, or a second approach based on results of Monte-Carlo simulations.

2.2 *The Coloured Petri nets (CPN) model*

In order to asses the impact of CCF in the dependability study of digital I&C systems, it is necessary to have a model of this studied system that is able to take into account the system dynamics. A widely used model in the dependability studies of dynamic systems is represented by the Petri nets (Signoret et al. 2013). Since I&C systems are complex and large, we choose to use the coloured Petri nets (CPN) type. CPN (Jensen & Kristensen 2009, Jensen 1997) is a discrete-event modelling language combining the capabilities of Petri nets with the capabilities of a high-level programming language. The main difference between a classical Petri Net and a CPN is that the CPN tokens can have different *colours* representing data types (*e.g.* Boolean, integer or more complex data structure). The formal definition of CPN is as follows.

A Coloured Petri Net is a 9-uplet $CPN = (P, T, A, \Sigma, V, C, G, E, I)$, where:

1. P is a finite set of **places**.
2. T is a finite set of **transitions**, $P \cap T = \emptyset$.
3. $A \subseteq P \times T \cup T \times P$ is a set of directed **arcs**.
4. Σ is a finite set of non-empty **colour sets**.

5. V is a finite set of **typed variables** such that *Type[*ν*]* $\in \Sigma$ for all variables $\nu \in V$.

6. $C : P \rightarrow \Sigma$ is a **colour set function** that assigns a colour set to each place.

7. $G : T \rightarrow EXPR_V$ is a **guard function** that assigns a guard condition to each transition t such that *Type[G(t)]* = Bool, bool standing for Boolean data type.

8. $E : A \rightarrow EXPR_V$ is an **arc expression function** that assigns an arc expression to each arc a such that $Type[E(a)] = Type[C(p)]$, where p is the place connected to the arc a.

9. $I : P \rightarrow EXPR_\emptyset$ is an **initialisation function** that assigns an initialisation expression to each place p such that *Type[I(p)]* $= Type[C(p)]$.

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 modelling* approach for a complex systems, based on generic modules that can be instantiated as often as needed.

Additionally, the probabilistic dependability assessment requires the time evolution of the system. For this, the CPN must take into account the *time* aspect. In a timed CPN (Jensen & Kristensen 2009, Jensen 1997), the time is given by a global clock. In addition to their colour, 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 can not 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.

The following drawbacks can be cited: the low readability (which can be put into perspective by using hierarchical CPN) and the difficulty in verifying a Petri net model. This last drawback can be offset by using a verification of CPN properties. This properties verification is supported by the *state space method*. The basic idea underlying the state space method 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 occurring events. From a constructed state space, it is possible to answer a large set of questions concerning the behaviour of the system, such as absence of deadlocks, a possibility to be able to reach a given state. We have used this formal verification of a CPN to study and validate some specific safety properties of an I&C systems (Pinna et al. 2013), but a Monte-Carlo simulation can be also realized without this type of verification.
In this paper, we propose to integrate the Atwood model into a CPN model of an I&C system. The obtained model allows the assessment of the CCF impact on the system dependability. In order to realize this assessment, in the next section, we introduce a case study coming from a nuclear power plant.

3 CASE-STUDY PRESENTATION AND ITS MODELLING

The studied system is a digital protection system. It is a part of the defence in depth of a nuclear power plant.

3.1 *System architecture*

This protection I&C system contains four divisions, which are strictly identical, see figure 1. These divisions are physically separated. Each division is composed of five "Acquisition & Processing Units" (APU). The APU 0, 1 and 2 represent the subsystem A (SSA). The APU 3 and 4 represent the subsystem B (SSB). The gathering of APU into subsystems takes into account the allocation of control functions of the I&C system. For the same control function, there is one implementation in an APU of SSA and one implementation in an APU of SSB with different inputs and treatment and their outputs must be identical in the normal operating mode.

Different electronic boards *C1* et *C2* are included in each APU. Each APU contains one *C1* board. The APU 0 and 1 contain four *C2* boards, and the APU 3, 4 and 5 contain three *C2* boards. These electronic boards are used for reception, treatment and emission of signals.

A second type of partition is defined: the *groups of APU* (GAPU). A group of APU contains all of the APU i (i [0,4]) of the four divisions.

3.2 *Modelling assumptions*

3.2.1 *Assumptions for the electronic boards modelling*

A constant failure rate is considered for boards.

The *C2* boards of an APU are considered as a series system.

The board failures can be detected by a set of self-tests. When a failure is detected by a self-test (SA),

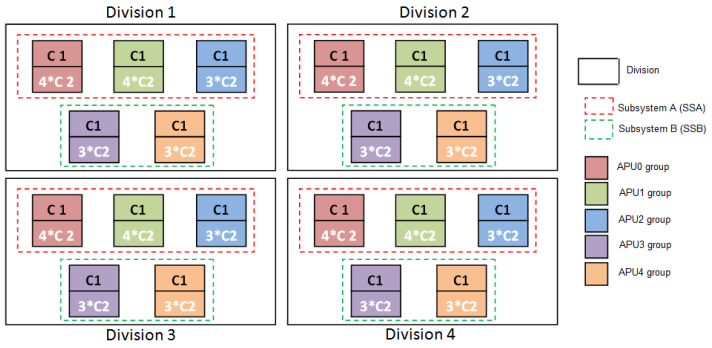

Figure 1: Architecture of the case study I&C system for a nuclear power plant

the detection time is considered null. When a failure is not detected by a self-test (NSA), then it is detected offline during a periodical-test. For a given division, these periodical-tests take place at each 18 months. So every quarter of this period, a division is tested during the periodic tests. After the periodic tests, the failed boards are repaired.

According to the supplier of electronic boards, their coverage rate of self-tests (t_c) is 100% , but this value seems to be ambitious. We add to the model the non-detected failures by self-test (NSA failures) in order to take into account the errors due to operation (different parameters or installation of boards from the nominal conditions specified by the provider). Thus the coverage rate is reduced at 85%. The global failure rate of the boards 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 following equations: $\lambda_{SA} = t_c.\lambda_{IND}$ and $\lambda_{NSA} = (1 - t_c).\lambda_{IND}$.

3.2.2 *Assumptions for global system modelling*

The hazardous event is represented by the failure of the protection I&C system.

The occurrence of this hazardous event is based on the voting logic of the APU:

- An APU fails when a card *C1* or *C2* is failed.
- A group of APU (GAPU) fails when 3 out of 4 APU is failed (3oo4).
- A subsystem (SSA or SSB) fails when a GAPU is failed.
- The I&C system fails when a subsystem is failed (1oo2) *or* when two subsystems are failed (2oo2).

We assume that the mission time of the protection I&C system is ten years. Indeed, this system is retrofitted only during the decennial maintenance operations of the nuclear plant. System unavailability can occur during the ten years. The system changes from unavailable to available state without being as good as new as it is not fully retrofitted on this period of ten years. Some electronic boards may be still failed when the system becomes available.

3.3 *CPN modelling*

We propose to use a modular approach for system modelling. Thus, the CPN model (shown in figure 2) is composed by the following modules:

- CCF generating (blue box)
- System representation (red box)
- State system description (green box)

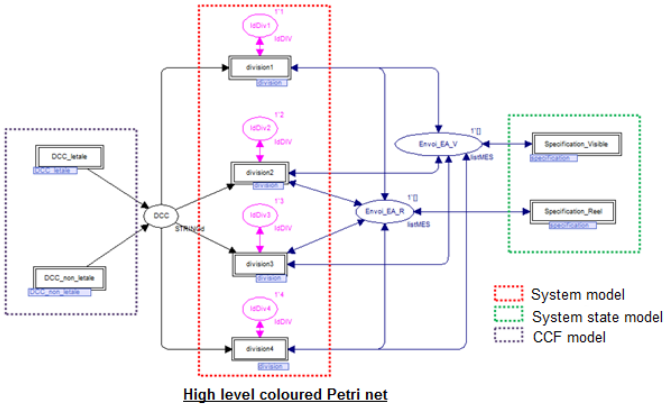

Figure 2: High level coloured Petri net of the I&C system

3.3.1 *CCF generating using Atwood model*

Non-lethal CCF are modelled by the CPN sub-net shown in figure 3. It corresponds to the substitution transition *DCC_non_letale* of the figure 2. The place *Nb-carte* contains the number of electronic boards *N* in the system. The firing of transition *Save* maintains the number of electronic boards *N* of the system in the place *SNb_carte* and set *N* tokens in the place nb_carteu. The transition *proba* is fired N times. The function *defdcc()* draws a random value using an uniform distribution law of probabilities in the interval [0, 1]. If the drawn value is lower than conditional probability *p* the considered board will be shock sensitive. The returned value will be *1*, otherwise *0*.

The firing of *init_temps* transition allows to determine the occurrence time of the non-lethal shock using the function *floor(exponential(!mu)+0.5)* and, in the same time, to specify if it is detected or not by a self-test. This is done using the function *detect()*. This function draws a random value using an uniform distribution law of probabilities in the interval [0, 1]. If the value is lower than coverage rate of self-tests (t_c), the non-lethal shock is detected. In this case the function return the value *1*, otherwise *0*. The firing of the transition *dcc* assigns the occurrence time of CCF and the variable of failure detection at each token of the system that is shock sensitive. The transition *no_def_dcc* allows to remove the tokens representing boards that are not shock sensitive. The transition *new_dcc* allows to generate the next occurrence

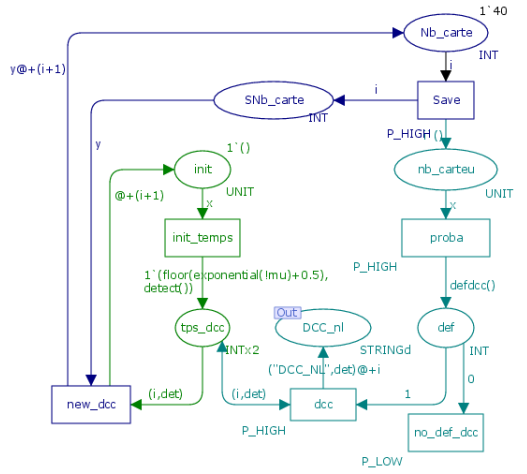

Figure 3: CPN sub-net modelling the *non-lethal CCF*

time of the non-lethal shock and to redefine the number of boards, which are shock sensitive.

Lethal CCF are modelled by the CPN sub-net shown in figure 4. It corresponds to the substitution transition *DCC_letale* of the figure 2. The firing of the transition *gene_dcc_l* allows to determine the occurrence time of the lethal shock using the function *floor(exponential(!omega)+0.5)*. A lethal CCF affects all the components (electronic boards) of the system and is always detected online. Thus, there are issued *N* temporized tokens with a color *('*DCC-NL',1) (*1* for detection). The next occurrence time for a new lethal CCF is calculated since the previous is realized.

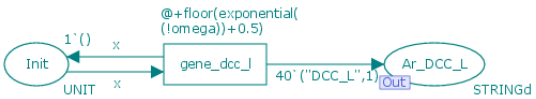

Figure 4: CPN sub-net modelling the *lethal CCF*

The Atwood model introduces three parameters to estimate: p, μ and ω. Two approaches, analytic or by simulation, can be used for doing their estimation.

Analytical approach for estimation of CCF model parameters. From the expressions of α, β_{letal} and λ_{TOT}, we obtain the following equations system:

$$(1-\alpha\sum_{k=1}^{N}p^k(1-p)^{N-k})\mu+\alpha\omega=\alpha\lambda_{IND} \quad (5)$$

$$(-\beta\sum_{k=1}^{N}p^k(1-p)^{N-k})\mu+(1-\beta)\omega=\beta\lambda_{IND} \quad (6)$$

The value of conditional probability p is considered known (*e.g.* at classical default values 0.2, 0.33 or 0.5). The independent failure rate for an electronic board is $\lambda_{IND} = 2.35\ 10^{-6}\ h^{-1}$. The equations (5) and (6) give the values of occurrence frequencies of non-lethal shocks μ and of lethal shocks ω. The obtained results are presented in Table 1.

Table 1: The values of occurrence frequencies μ and ω for non-lethal and lethal shocks as a function of p using analytical approach

p	$\mu\ in\ h^{-1}$	$\omega\ in\ h^{-1}$
0.2	$9.52\ 10^{-7}$	$1.18\ 10^{-8}$
0.33	$9.52\ 10^{-7}$	$1.18\ 10^{-8}$
0.5	$9.52\ 10^{-7}$	$1.18\ 10^{-8}$

Monte-Carlo simulation approach for estimation of CCF model parameters. We introduce the ratio between the occurrence rate of independent failures λ_{IND} and the total failure rate λ_{TOT} of a component (an electronic board):

$$\gamma=\frac{\lambda_{IND}}{\lambda_{TOT}}=1-\alpha.\sum_{k=1}^{N}C_{N-1}^{k-1}p^k.(1-p)^{N-k}-\beta_{letal} \quad (7)$$

$$\gamma=1-\alpha.p-\beta_{letal} \quad (8)$$

We introduce also E_i that represents the number of independent failure events realized in 10 years of simulations. This number is obtained by simulating only the independent failures in Petri net model and their occurrences are counted. It allows to obtain from the equation 9, the average independent failure rate λ_{IND} for a board in the system. The different rates can be estimated from the following equations:

$$\lambda_{IND} = \frac{E_i}{10\ ans\ *N} \quad (9)$$

$$\mu = \frac{\alpha.\lambda_{IND}}{\gamma} \quad (10)$$

$$\omega = \frac{\beta_{letal}.\lambda_{IND}}{\gamma} \quad (11)$$

The expected value of E_i is equal to 8.28 and the value obtained for independent failures rate is: $\lambda_{IND} = 2,36\ E^{-6}\ h^{-1}$. The results obtained by applying this approach are presented in Table 2.

The occurrence frequencies μ and ω for non-lethal and lethal shocks obtained by applying these approaches (analytical and simulation approaches) are almost identical. This result allows, firstly, to validate the proposed CPN modelling approach for the Atwood shock model. Secondly, the Monte-Carlo simulation approach could be used to revisit some assumptions supporting the Binomial Failure Rate model underlying the Atwood shock model, especially in the case of digital I&C systems including software.

Table 2: The values of occurrence frequencies μ and ω for non-lethal and lethal shocks as a function of p using Monte-Carlo simulation approach

p	γ	λ_{TOT}	μ	ω
0.2	0.995	$2.37\ 10^{-6}$	$9.62\ 10^{-7}$	$1.18\ 10^{-8}$
0.33	0.995	$2.37\ 10^{-6}$	$9.62\ 10^{-7}$	$1.18\ 10^{-8}$
0.5	0.995	$2.37\ 10^{-6}$	$9.62\ 10^{-7}$	$1.18\ 10^{-8}$

Introduction of asymmetry in CCF propagation. For a realistic modelling of common causes failures (CCF) and of their impact on the systems dependability, it is interesting to assume that some non-lethal shocks predominantly affect some *k* components among the all *N* components of the system, with $1 \leq k \leq N$ (*e.g.* only some types of electronic boards belonging to the I&C systems). We propose to modify the generation of non-lethal CCF for simulating the asymmetries in their propagation, in other words considering *"oriented" CCF*.

In a system with *N* components, a non-lethal shock affects the boards with a conditional probability *p*. The expected number of affected components is $N * p$. The set of *N* components can be divided in two sub-sets *A* (SSA) and *B* (SSB), containing respectively *a* et *b* components, such as $a + b = N$. Let be x (respectively y) the probability that a component of SSA (respectively SSB) is affected by a non-lethal shock. From reasoning on mathematical expectation, we have:

$$ax + by = Np \tag{12}$$

To determine x and y we choose how a CCF will affect the SSA (p_1) and SSB (p_2), such as $p_1 + p_2 = 1$. Thus, we obtain:

$$x = \frac{N.p.p_1}{a} \tag{13}$$

$$y = \frac{N.p.p_2}{b} \tag{14}$$

The solutions of these equations, *x* and *y*, are the probabilities of non-lethal shock for the CPN tokens that represent respectively the SSA and SSB components.

3.3.2 *System modelling by CPN*

The hierarchical and modular aspects of Coloured Petri nets are exploited to develop the CPN model of I&C system. Thus, each of its divisions is modelled by means of a substitution transition at the high level of the system, in the Figure 2. A division includes five APU, each of them includes the correct number of electronic boards *C1* and *C2*. The CCF are transmitted to the APU and to the boards by means of CPN places (socket places). The state of an APU is determined by the state of its boards (available or unavailable). Once the state of a board changes, the new state of APU is sent to the specification that determines the state of the whole I&C system.

An electronic board represented in the Figure 5 has three possible tangibles states: operational ("Marche" place), failed and non-detected ("detection" place) and in reparation ("reparation" place). When the board is operational, it can change its state if one of the following four events occurs:

- independent failure detected online by a self-test (modelled by the purple Petri sub-net on the right side of the model)
- independent failure detected offline in periodical-tests (modelled by the purple sub-Petri net on the left side of the model)
- non-lethal CCF detected online and lethal CCF (modelled by the tokens received by "AR_DCC" place from the CCF models of the Figures 3 and 4)
- non-lethal CCF detected offline in periodical-tests (modelled also by the tokens received by "AR_DCC" place from the CCF model of the Figure 3)

If the failures are detected during the periodic tests, the "rep" transition is fired and the board changes its state to the reparation state. If the failures are detected online, the board changes its state immediately from the operational to the repair state. The repair time is calculated using the function *floor(exponential(1/!MTTR)+1.0)*. As soon as the board is repaired, its state changes immediately to the operational state. The next occurrence times of the independent failures detected online and offline are also calculated.

This CPN model of electronic boards are generic. For all boards, only the numerical values of parameters (failure and repair rates) are different.

3.3.3 *System state modelling by CPN*

Using the information about the state (available/unavailable) of the APU i ($i \in [0, 4]$ of the division j ($j \in [1, 4]$)), it is possible to determine the state of the I&C system during the Monte-Carlo simulation using the CPN of Figure 6. The system state is represented by a token whose colour is composed of five booleans, each of them representing the state of one APU. The different configurations on the transitions' guards allow to define the conditions of availability/unavailability of the system.

The entire CPN model obtained for the I&C system has 685 transitions and 504 places. Even if the model size is large enough, the use of hierarchy and colours concepts have resulted in a modular and readable model obtained through the instantiation of generic templates. We can note, that an equivalent classical Petri net model for the same I&C system should have

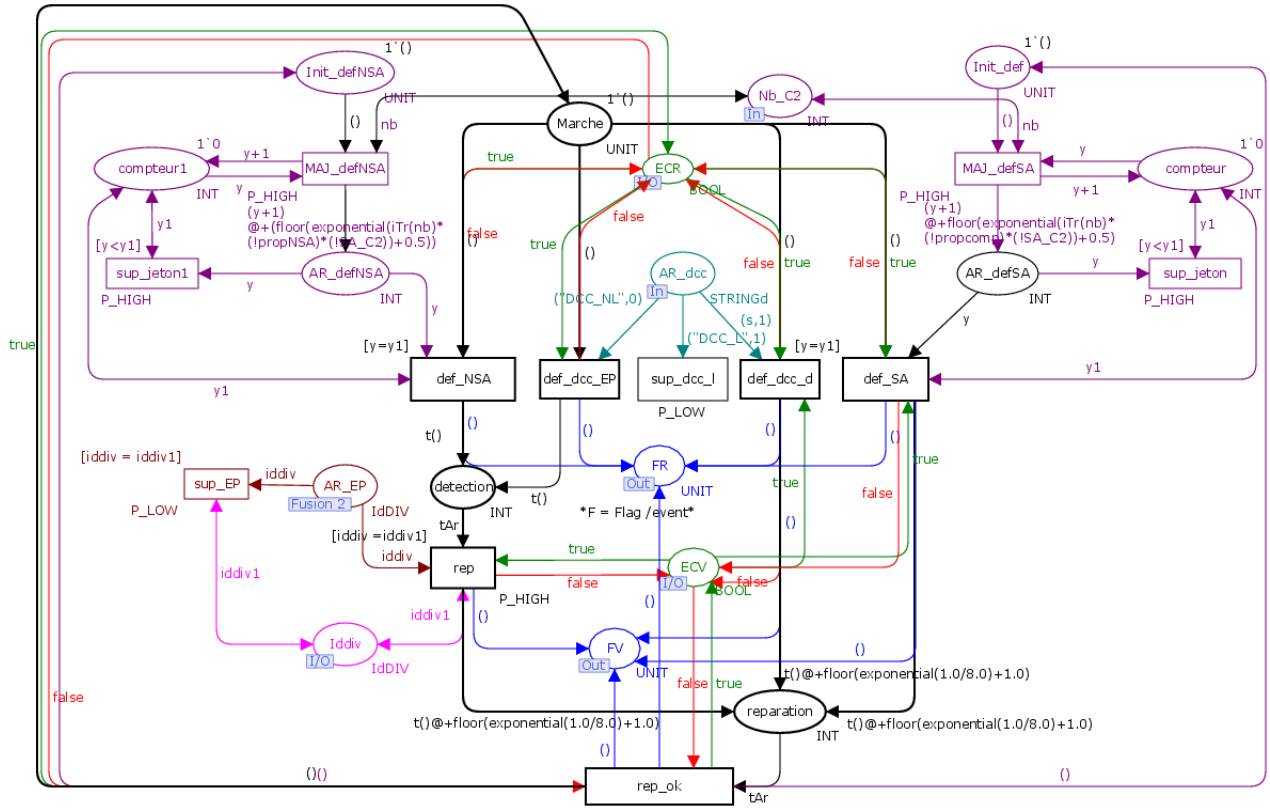

Figure 5: CPN sub-net of an *electronic board*

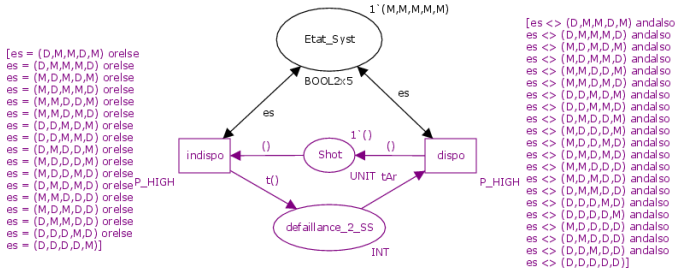

Figure 6: CPN sub-net to determine the state of the whole I&C system (available or unavailable)

several thousands places and transitions. The obtained CPN model allows the probabilistic dependability assessment of the system.

4 PROBABILISTIC DEPENDABILITY ASSESSMENT

4.1 *Probability of failure on demand*

Since the I&C system is a protection system (its mission is to protect the nuclear power plant), we are interested to asses only the *Probability of Failure on Demand* (PFD). This is in accordance with the IEC-61508 (2010) standard and its declination IEC-61513 (2011) that address the functional safety of digital systems. We define two kinds of PFD:

- the *real PFD* that represents the I&C system unavailability starting with the moment where the electronic boards are not anymore in their operational state;
- the *visible PFD* that represents the system unavailability only starting with the moment where the boards failure is detected. The time between the occurrence of non-detected failures and their detection by a periodical-test is not considered.

The definition of the two kinds of PFD allows to estimate the difference between the real state of the system and the state observed by plant operators during operation.

The PFD is estimate using Monte-Carlo simulation by the following equation:

$$PFD = \frac{System\ unavailability\ time}{Mission\ time} \tag{15}$$

The results presented in the Table 3 are obtained after 10,000 histories during 10 years. The 95% confidence interval for all of the results presented in Table 3 is also estimated and its value is $< 10^{-6}$.

According to IEC-61513 (2011) "there is not an equivalent scheme to the reliability/risk reduction SIL levels proposed in IEC 61508 in common use in the nuclear sector". Consequently, we do not associate a SIL level for the system under study.

If the conditional probability of failure of one component in a non-lethal shock p increases, there will be more components affected by a shock and the PFD also increases. The difference between the real PFD and the visible PFD is about 10 to 100.

Table 3: Real and visible PFD of the protection I&C system for different values of *p*

Indicators	p	Average
real PFD	0.2	$2.5\ 10^{-5}$
visible PFD	0.2	$< 10^{-6}$
real PFD	0.33	$2.73\ 10^{-4}$
visible PFD	0.33	$1.0\ 10^{-6}$
real PFD	0.5	$5.4\ 10^{-4}$
visible PFD	0.5	$4.0\ 10^{-6}$

4.2 *Influence of the oriented non-lethal CCF*

To asses the impact of asymmetric propagation of non-lethal CCF, we consider the orientation of CCF on the two sub-systems SSA and SSB, using the approach presented in section 3.3.1.

The conditional probability of failure of one component in a non-lethal shock is $p = 0.2$. The frequency of non-lethal shocks is arbitrary fixed at one shock per year, i.e. $\mu = 1.14\ 10^{-1}h^{-1}$. The lethal shocks are not represented. 10,000 trajectories during 10 years are also realized and the occurrence of system failure ends the trajectory simulation. Table 4 shows the results. The sum of failures' combinations (columns) is equal with the total number of histories (10,000) for a fixed CCF orientation.

Table 4: Combinations of failed boards leading to the system downtime depending on p_1 and p_2

CCF orientation	p_1 SSA	0.1	0.2	0.3
	p_2 SSB	0.9	0.8	0.7
only CCF		9404	9723	9787
indep. SA failures		3	0	1
indep. NA failures		21	9	9
indep. SA and NSA		77	46	42
CCF & indep. SA failures		8	6	1
CCF & indep. NSA failures		487	216	160
MTTFF (in h)		49586	28921	22056

We can observe that the more a sub-system is preferred (according to p_1 and p_2), the more the MTTFF increases. The logic vote explains this phenomenon. We observe also that independent failures combinations without CCF rarely leads to system failure, due to the high level of redundancy. Independent failures detected offline lead more easily to system failure than the ones detected online. This aspect can be improved by increasing the frequency of periodic tests or the coverage rate of self-tests.

5 CONCLUSIONS

The coloured Petri nets allow to represent the digital I&C systems and to assess the dependability indicators considering CCF. The shock Atwood model has been transposed in Petri net. It allows to take in account the independent failures, the lethal CCF, but also the non-lethal CCF. An extension of this model was proposed to represent the asymmetric propagation of non-lethal CCF on privileged axes. This allows to relax the assumption of the random repartition of non-lethal shocks on the all components and to represent the effects of diversity. The proposed approach has been applied to a representative case of I&C system of a nuclear power plant.

The extremely low volume of operating experience related to the protection I&C systems makes it difficult to estimate the α factors representing the conditional probability of failures on demand of the *k* components in a group of *N* components when a CCF occurs. This CPN model could be used to simulate operating experience for obtaining more data, which make a more accurate estimation of these factors.

Another interesting axis concerns the estimation of the three parameters of the Atwood model. The proposed Monte-Carlo simulation approach for the estimation of these parameters has been validated by an analytical approach. This Monte-Carlo simulation approach could be used to revisit the assumptions supporting the Binomial Failure Rate model underlying the Atwood model.

REFERENCES

Atwood, C. L. (1980). *Estimating common cause failure rates for pumps in nuclear reactors*. Ph. D. thesis, California.

Bricman-Rejc, Z., M. Cepin, & A. Sitdikova (2013). Estimating common-cause failures parameters within power system reliability analysis. In *Annual Conference of the European Safety and Reliability Association, ESREL 2013*, Amsterdam, pp. 2841–2846.

IEC-61508 (2010). *Functional safety of electrical/electronic/programmable electronic safety-related*, Volume 1-7.

IEC-61513 (2011). *Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems*.

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

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

Lilleheier, T. (2008). Analysis of common cause failures in complex safety instrumented systems.

Pinna, B., G. Babykina, N. Brînzei, & J.-F. Pétin (2013). Deterministic and stochastic dependability analysis of industrial systems using Coloured Petri Nets approach. In *Annual Conference of the European Safety and Reliability Association, ESREL 2013*, Amsterdam, pp. 2969–2977.

Signoret, J.-P., Y. Dutuit, P.-J. Cacheux, C. Folleau, S. Collas, & P. Thomas (2013). Make your petri nets understandable: Reliability block diagrams driven petri nets. *Reliability Engineering and System Safety 113*, 61–75.

US-NRC (1987). *NUREG/CR-4780. Procedures for treating common-cause failures in safety and reliability studies*, Volume 1 and 2. Washington, DC: US Nuclear Regulatory Commission.