COMMON CAUSE FAILURE PARAMETERS ESTIMATION 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

Laurent Gérard
ENSEM, Université de Lorraine
2 Avenue de la Forêt de Haye, 54518 Vandoeuvre-lès-Nancy, France.

The object of the article is the estimation of Common Cause Failures (CCF) in digital systems, e.g. protection system of nuclear plants. The system under study is composed of four divisions, 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 the CCF impact on the system dependability. Assumptions related to hardware reliability and system logic, maintenance and repairs are taken into account in the model that is thus dynamic. The simulation, based on a CPN model and the assumptions of the Atwood model, permits to compare estimators of CCF parameters. An example of comparison is presented in this article, based on the Impact Vectors approach. Finally, some conclusions are presented.

I. COMMON CAUSE FAILURES IN LARGE DIGITAL SYSTEMS

I.A. Specific Issues

Digital Instrumentation and Control systems (I&C) have a key role for regulation and safety of nuclear power plants. Their characteristics are a large size, a high level of redundancy and a complex logic of vote. Although digital systems have failure detection capabilities, and although their components are more reliable than the analog systems they replace, some characteristics raise specific issues on the modeling 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 so-called Alpha Factor and Beta Factor models are the most widely used for taking into account CCF within various types of nuclear plants systems [1] and, more generally, in power systems [2]. The Beta Factor model implies the failure of the 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 the 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.

I.B. Atwood model

In this section, we introduce the Atwood model [3] of CCF that takes into account independent failures of components and CCF failures due to shocks that affect all or only some components. It 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 $1 \leq k < N$. Each component has then a conditional probability of failure ρ. 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. 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. 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:

$$\lambda_1^{(N)} = \lambda_{IND} + \mu\rho(1-\rho)^{N-1} \qquad (1)$$

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

$\lambda_k^{(N)} = \mu\rho^k(1-\rho)^{N-k}$ (2)

The failure rate of N components due to a nonlethal and lethal shock is:

$\lambda_N^{(N)} = \mu\rho^N + \omega$ (3)

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

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

The capability to represent CCF affecting only a part of the all components of the system implies the use of three parameters (μ, ρ, ω), whatever the size of the CCF group is. The default values are:

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

$\rho = 0.2$ or 0.33 or 0.5 (conditional probability of component failure in a non-lethal shock),

$\beta_{letal} = \frac{\omega}{\lambda_{TOT}} = 5x10^{-3}$ (rate of lethal shocks).

II. SYSTEM UNDER STUDY – DESCRIPTION AND ASSUMPTIONS

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

II.A. System architecture

This protection I&C system contains four divisions, which are identical, see figure 1.

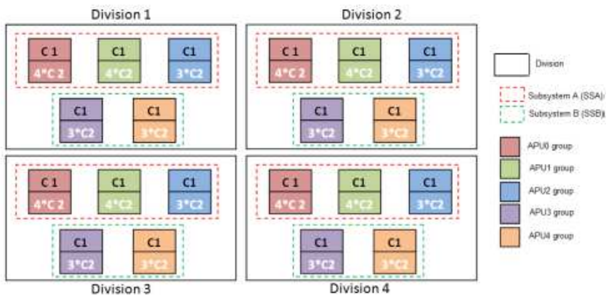

Figure 1: Architecture of the case study I&C system

These divisions are physically separated. Each division is composed of five processing units (APU). The APU 0, 1 and 2 compose the subsystem A (SSA). The APU 3 and 4 compose the subsystem B (SSB). A control function, 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 I&C signals of interest for PSA, two kinds of electronic modules, C1 and C2, are used by each APU. Each APU contains one C1 module. The APU 0 and 1 contain four C2 modules, and the APU 2,3 and 4 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 ϵ[0,4]) of the four divisions.

II.B. Assumptions for the electronic modules

A constant failure rate is considered for 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, periodic tests take place every period of 18 months. So every 6 weeks, 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-self-detected failures (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 specified conditions. 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:

$\lambda_{SA} = a.\lambda_{IND}$ and $\lambda_{NSA} = (1-a).\lambda_{IND}$ (5)

II.C. Assumptions for system states and logic

The hazardous event is the unavailability of a given 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 one of its GAPU fails.
- I&C 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.

III. SYSTEM MODELING USING COLORED PETRI NETS

III.A. Benefits of Petri Nets for this modeling

The model should be able to represent the dynamic sequences of states of large digital systems and estimate dependability measures. Markov chains or Petri Nets have this capability. The Beta-factor model has already been integrated in Markov chains [4] and in the basic Petri Nets [5]. The main drawback of these models is the combinatorial explosion of their size when the modeled system is large and complex.

To remediate this drawback, we used Colored Petri Nets (CPN) [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).

III.B. Definition of a hierarchical timed Colored Petri Net

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

P is a finite set of **places**

T is a finite set of **transitions**, $P \cap T = \emptyset$

$A \subseteq (P \times T) \cup (T \times P)$ is a set of **directed arcs**

Σ is a finite set of **non-empty colour sets**

V is a finite set of **typed variables:** $\forall v \in V,\ Type[v] \in \Sigma$

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

$G: T \rightarrow EXPR_v$ is a **guard function**. It assigns a condition to each transition:

Type[G(t)] = Bool (Boolean data type)

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

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

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

Also, the probabilistic dependability assessment requires to take account of the time dependence of the system. In a timed CPN [6], [7], 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 a time given by the global clock. 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.

III.C. Drawbacks

Low readability of Petri Nets. It is highly reduced by using the concepts of colors and hierarchy of the CPN.

Difficulty of verification.

A first verification of CPN can be realized by the step-by-step simulation. This step-by-step simulation allows verifying the behavior of each CPN sub-module or of the entire model for some functional or dysfunctional scenarios of behavior. But this type of verification cannot guarantee the exhaustiveness of all possible system behaviors. To overcome this, more complete verification methods are proposed: a quantitative one and a qualitative one.

A Monte-Carlo simulation (quantitative method) can be done for a partial verification of the model. To do that, we compare two approaches for parameters estimation of Atwood model: an analytical and a Monte-Carlo simulation from the CPN [8].

A more exhaustive verification can be done by a state space method (qualitative 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 reach a given state. This formal verification of a CPN has been done for some specific safety properties of I&C systems [9].

III.D. CPN modeling of the system under study

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)

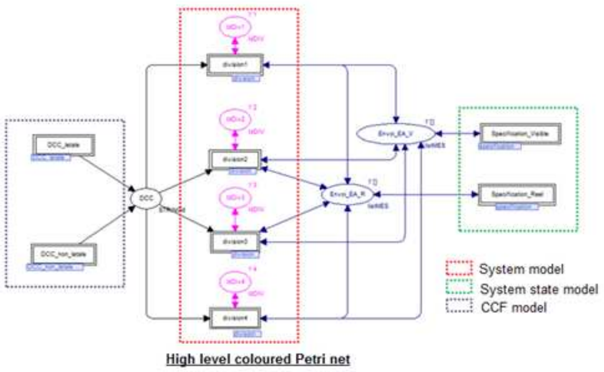

Figure 2: High level colored Petri net of the I&C system

In this article, we focus on the modeling of CCF with CPN.

III.E Lethal CCF modeling

Lethal CCF are modeled by the CPN sub-net shown in figure 3. It corresponds to the substitution transition *DCC_letale* of the figure 2 (left box). The firing of the transition *gene_dcc l* determines the occurrence time of the lethal shock using an exponential function *floor(exponential(!omega)+0.5)*. A lethal CCF affects all the N components of the system and is always detected online. Thus, N temporized tokens are issued with a color (*DCC-L,1*) (1 for detection). The next occurrence time of a lethal CCF is also calculated.

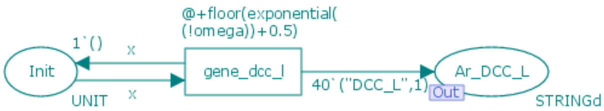

Figure 3: CPN sub-net modeling the lethal CCF

III.F. Non-lethal CCF modeling

Non-lethal CCF are modeled by the CPN sub-net shown in figure 4. It corresponds to the substitution transition *DCC_non_letale* of the figure 2. The place *Nb-carte* contains the number of electronic modules N in the system. The firing of transition *Save* set the number of electronic modules 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 in the interval [0,1]. If the value is lower than conditional probability ρ, the considered module is shock sensitive. The returned value is 1, otherwise 0.

The firing of *init_temps* 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. This is done using the function *detect()*. This function draws a random value using an uniform distribution in the interval [0,1]. If the value is lower than the coverage rate of self-tests, the failure is detected. In this case the function returns the value 1, otherwise 0.

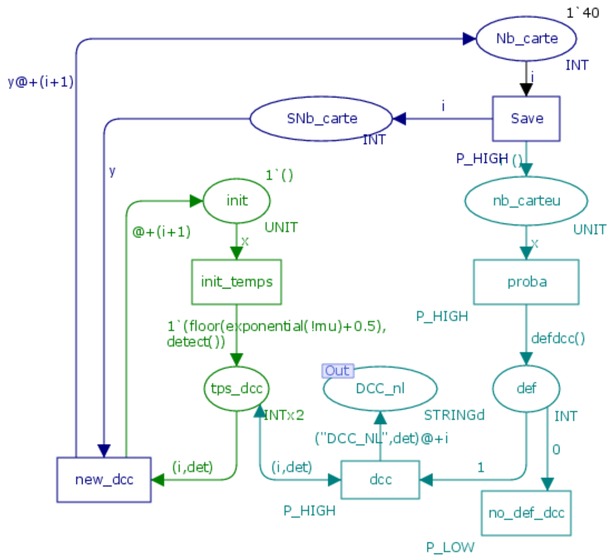

Figure 4: CPN sub-net modeling the non-lethal CCF

The firing of the transition *dcc* assigns the occurrence time of CCF and the variable characteristic of failure detection to each token of the system that is shock sensitive. The transition *no_def_dcc* removes the tokens representing modules that are not shock sensitive. The transition *new_dcc* generates the next occurrence time of a non-lethal shock and redefines the number of modules, which are shock sensitive.

III.G Applications of the CPN model

The timed hierarchical CPN based on Atwood model may compute safety measures of interest for PSA, like the probability of failure on demand (Pfd), the spurious failure rate and the probabilistic parameters representing CCF (Beta Factors , Alpha Factors…), MTFF (Mean Time To First Failure). We do not consider here the Probability of Failure per hour (Pfh), defined in IEC 61508 [10]. It is not relevant for the type of protective actions modeled in PSA. Also, we do not associate a SIL level for the system under study. According to IEC 61513 [11]: " there is not an equivalent scheme to the reliability/risk reduction SIL levels proposed in IEC 61508 in common use in the nuclear sector".

This simulator may be used for various purposes. In [8], 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.
Also, the Atwood model can be modified to "direct" non-lethal CCF on certain parts of the system and take into account 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 the effect of diversity and separation between divisions [8]. We present here another possible application. We compare the CCF parameters Alpha factors obtained by the empiric method of Impact Vectors and the Alpha Factors that could be obtained if we had a perfect knowledge of the failures conditions.

IV. CCF PARAMATERS ESTIMATIONS WITH SIMULATIONS

IV.A The Impact Vectors approach for Alpha Factors estimation

The very low number of failures observed in digital I&C Operating Experience (OE) and the presence of failures discovered lately makes difficult to estimate the measures of interest.
Various approaches have been developed to cope with this general difficulty of OE. One of them is the Impact Vectors. It is used in NRC studies to analyze and aggregate OE related to various systems from NPRDS (Nuclear Plant Reliability Data System), LER (Licensee Event Report), for the 1980-1993 time interval, on the basis of studies like [12], [13], [14]. Impact Vector approach is still today used to assess CCF parameters on various systems, like diesel generators, pumps, control rods....
The Impact Vector assesses the impact an event (observation of one failure or more at a given time) would have on a common cause group. The impact is usually measured as the number of failed components out of a set of similar components in the common cause group [15]. The Alpha Factor can be directly obtained from this approach with the following estimator, where:

$$\widehat{\alpha_k^N} = \frac{n_k}{\sum_{j=1}^{N} n_j} \quad (6)$$

N: size of the CCF group
n_k: number of events where k elements of the CCF group failed.
If k>1, it is a CCF event.
If k = 1, it may be an independent failure or a partial CCF event.
The expression of n_k in function of averaged Impact Vectors $F_{k,ave}^i$ is:

$$n_k = \sum_{i=1}^{r} F_{k,ave}^i \quad (7)$$

where r is the total number of events.

IV.B Application to OE of digital I&C

Although Impact Vector method was not originally experienced on digital I&C, it may be used to analyze operating experience of such systems. However we do not have an accurate assessment of the uncertainty due to this application.
The purpose of the application is to compare Alpha Factors estimates and validate the Impact Vectors approach. *Observed Alpha Factors* are obtained on a simulated set of data using Impact Vectors with limited information. *Real Alpha Factors* are obtained on a simulated set of data using Impact Vectors with full information. A simulation with colored Petri nets generating a large number of chronicles, including a significant quantity of CCF, is fruitful to do this comparison.
The description of the Impact Vectors approach may be found in [15], [16]. We present here only the assumptions done specifically for this application. Three factors are used to "blur" the data, and in some way, to explicit uncertainty in the observation.

Definition of failure sets.
First, failure events have to be merged in sets. In the case of *Real Alpha Factors*, the information is exhaustive; there is no difficulty to merge CCF in such sets. In the case of *Observed Alpha Factors*, some CCF may cause failures spread within a time interval. Thus, many different sets of CCF can be built. A rule for merging has to be defined: the set that corresponds to the CCF of the largest size is chosen.

Degradation Factor (Fd).
For each element of a CCF group involved in a CCF event, a degradation factor is associated. For the hardware part of a digital system, at the level of electronic modules, we consider that there is no wearout. Preventive maintenance policies permit to identify and avoid the presence of electronic parts sensitive to wearout. Thus, we consider only two levels of degradation:
Fd = 1, if the module is in functional failure state.
Fd = 0, in other cases.

Simultaneity Factor (Fs).
It is a subjective probability, which estimates the belief in the simultaneity of failures affecting the CCF group. This factor is associated to events.

With full information, the values used to estimate the *Real Alpha Factors* are:
Fs= 1 in the case of a CCF,
Fs = 0 in other case

With limited, realistic information, the values used to estimate the *Observed Alpha Factors* depend on the periodic testing. Indeed, in the case of digital I&C systems, there are two modes of failure detection: self-test or periodic testing. The idea is to compare the time spread of a set of failures, to the time required to detect all latent failures (T). When two failures are separated by a time lapse higher than T, there is a negligible risk of simultaneity; in other cases, there is a possibility of simultaneity (see table 1)

Time spread of a set of failures	Simultaneity factor (Fs) value
$Spread \leq \frac{T}{4}$	1
$\frac{T}{4} < Spread \leq \frac{T}{2}$	0.5
$\frac{T}{2} < Spread \leq T$	0.1
$T < Spread$	0

Table 1. Simultaneity factor (Fs) values

Also, to take account of the different detection and repair times between the various failures, two rules are defined and will have to be compared:
Rule A: T is the off-line test periodicity, whatever the failure detection type is (SA/NSA)
Rule B: T is the off-line test periodicity interval for NSA detection type, 8 days for SA.

Shared Cause Factor (Fc).
It reflects the degree of belief of the analyst in the existence of common cause failures in a set of simultaneous failures. It is a conditional probability, associated to set of failure events.
With full information, the values used to estimate the *Real Alpha Factors* are:
Fc= 1 in the case of a CCF,
Fc = 0 in other case

With limited, realistic information, in the case of digital systems, the following values are used for *Observed Alpha Factors*:
Fc= 0 if there is evidence of no coupling (proven independent failures)
Fc = 1 in other situations. This is a rather conservative assumption.

IV.C Results
Three series of simulations are presented. Each one has a specific scope. The CCF group is a group of four APU of the same kind, distributed in four divisions. Analytical expressions from [15], [16], have been implemented in a dedicated Excel add-on (*ParamDCC*).

Influence of the rules for simultaneity factor.
5 chronicles lasting 10 years have been simulated. They are equivalent to 50 reactor.years, under assumption of constant failure and event rates. Values of Atwood model parameters are default values (see I.B.)
Tables 2 and 3 compare the influence of rule A and B on the difference between real and observed Alpha Factors.
For CCF of order 2, 3 and 4, Rule B generally overestimates the real value (95% of figures), but with slightly less conservatism than Rule A. The preliminary conclusion is to use Rule B for simultaneity factor.

Comparison between Real and Observed Alpha factors on a realistic sampling

20 chronicles of 10 years have been simulated. They are equivalent to 200 reactor×years, under assumption of constant failure and event rates. This is representative of the size of the samples present in real OE. Values of Atwood model parameters are ρ=0.2 or 0.33 or 0.5; α=0.405; β=0.005. Rule B for simultaneity factor is used.
Tables 4, 5 and 6 compare maximum and average deviation between Real Alpha Factors and Observed Alpha Factors estimated with the Impact Vector approach. The deviation is defined by:

$$\delta = \frac{\alpha^N_{k,observed} - \alpha^N_{k,real}}{\alpha^N_{k,real}}$$

Average deviation values at high CCF orders (3 and 4) are relatively low. It means that the assumptions done in IV.B, using Rule B, permit acceptable Alpha Factor estimate with the Impact Factors approach. Tables 4 to 6 show that for ρ=0.2 or 0.33, at high CCF orders (3 and 4), estimates are generally more conservative than optimistic (Tables 4 and 5). Deviation increases with lethality: for ρ=0.5, observed Alpha Factors may be significantly underestimated (Table 6). This may be due to the limited number of reactor×years. In these situations, the use of Rule A may be an artifact to limit the risk of underestimation of Observed Alpha Factors.

Chronicle	(k,N)	Real Alpha(k,N)	Observed Alpha(k,N)
1	(1,4)	$9.21x10^{-1}$	$8.99x10^{-1}$
	(2,4)	$4.8x10^{-2}$	$6.9x10^{-2}$
	(3,4)	$1.6x10^{-2}$	$1.7x10^{-2}$
	(4,4)	$1.6x10^{-2}$	$1.5x10^{-2}$
2	(1,4)	$8.80x10^{-1}$	$8.68x10^{-1}$
	(2,4)	$7.2x10^{-2}$	$8.8x10^{-2}$
	(3,4)	$3.6x10^{-2}$	$3.1x10^{-2}$
	(4,4)	$1.2x10^{-2}$	$1.2x10^{-2}$
3	(1,4)	$9.01x\ 10^{-1}$	$8.71x\ 10^{-1}$
	(2,4)	$2.8x\ 10^{-2}$	$4.0x10^{-2}$
	(3,4)	$4.2x\ 10^{-2}$	$4.5x10^{-2}$
	(4,4)	$2.8x\ 10^{-2}$	$4.5x10^{-2}$
4	(1,4)	$8.91x\ 10^{-1}$	$8{,}40x\ 10^{-1}$
	(2,4)	$7.8x10^{-2}$	$1.19x\ 10^{-1}$
	(3,4)	$3.1x10^{-2}$	$4.2x10^{-2}$
	(4,4)	0	0
5	(1,4)	$9.75x\ 10^{-1}$	$9.24x\ 10^{-1}$
	(2,4)	$1.2x10^{-2}$	$6.3x10^{-2}$
	(3,4)	0	0
	(4,4)	$1.2x\ 10^{-2}$	$1.3x\ 10^{-2}$

Table 2. Real and observed Alpha Factors (Rule A) - Example of 5 chronicles ($\rho = 0.2$)

Chronicle	(k,N)	Real Alpha(k,N)	Observed Alpha(k,N)
1	(1,4)	$9.21x\ 10^{-1}$	$9.09x\ 10^{-1}$
	(2,4)	$4.8x\ 10^{-2}$	$6.1x\ 10^{-2}$
	(3,4)	$1.6x\ 10^{-2}$	$1.5x\ 10^{-2}$
	(4,4)	$1.6x\ 10^{-2}$	$1.5x\ 10^{-2}$
2	(1,4)	$8.80x\ 10^{-1}$	$8.72x\ 10^{-1}$
	(2,4)	$7.2x\ 10^{-2}$	$8.6x\ 10^{-2}$
	(3,4)	$3.6x\ 10^{-2}$	$3.0x\ 10^{-2}$
	(4,4)	$1.2x\ 10^{-2}$	$1.2x\ 10^{-2}$
3	(1,4)	$9.01x\ 10^{-1}$	$8.97x\ 10^{-1}$
	(2,4)	$2.8x\ 10^{-2}$	$1.60x\ 10^{-2}$
	(3,4)	$4.2x\ 10^{-2}$	$4.35x\ 10^{-2}$
	(4,4)	$2.8x\ 10^{-2}$	$4.35x\ 10^{-2}$
4	(1,4)	$8.91x\ 10^{-1}$	$8.52x\ 10^{-1}$
	(2,4)	$7.8x\ 10^{-2}$	$1.15x\ 10^{-1}$
	(3,4)	$3.1x\ 10^{-2}$	$3.3x\ 10^{-2}$
	(4,4)	0	0
5	(1,4)	$9.75x\ 10^{-1}$	$9.49x\ 10^{-1}$
	(2,4)	$1.2x\ 10^{-2}$	$3.8x\ 10^{-2}$
	(3,4)	0	0
	(4,4)	$1.2x\ 10^{-2}$	$1.3x\ 10^{-2}$

Table 3. Real and observed Alpha Factors (Rule B) - Example of 5 chronicles ($\rho = 0.2$)

	Maximum deviation		Average deviation (Estimate is conservative when >0)
(k,N)	Observed < Real (Estimate is optimistic)	Observed > Real (Estimate is conservative)	
(1,4)	-2.2%	1.4%	0.45%
(2,4)	-90%	102%	30%
(3,4)	N.S.	1.5%	0.22%
(4,4)	N.S.	N.S.	N.S.

Table 4: Comparison of $\boldsymbol{\alpha_k^N}$ estimates, $\boldsymbol{\rho = 0.20}$

	Maximum deviation		Average deviation (Estimate is conservative when >0)
(k,N)	Observed < Real (Estimate is optimistic)	Observed > Real (Estimate is conservative)	
(1,4)	-1.2%	2.3%	0.5%
(2,4)	-47%	58%	18%
(3,4)	-26.4%	2.0%	2.4%
(4,4)	N.S.	1.2%	0.12%

Table 5. Comparison of $\boldsymbol{\alpha_k^N}$ estimates, $\boldsymbol{\rho = 0.33}$

(k,N)	Maximum deviation: Observed < Real (Estimate is optimistic)	Observed > Real (Estimate is conservative)	Average deviation (Estimate is conservative when >0)
(1,4)	-1.3%	2.3%	1.0%
(2,4)	-48%	58%	20%
(3,4)	-75%	16%	13%
(4,4)	-2.5%	2.2%	0.9%

Table 6. Comparison of $\boldsymbol{\alpha_k^N}$ estimates, $\boldsymbol{\rho = 0.5}$

Comparison between Real and Observed Alpha factors on a larger sampling

To assess the uncertainty due to the limited size of real samples, $Observed\,Alpha\,Factors$ values have been estimated from 100 chronicles of 5 years. They are equivalent to 500 reactor.years, under assumption of constant failure and event rates. Minimal and maximal values of Alpha Factors are presented in Table 7.

	ρ=0.2		ρ=0.33		ρ=0.5	
(k,N)	Min	Max	Min	Max	Min	Max
(1,4)	9.35×10^{-1}	1	8.83×10^{-1}	1	8.35×10^{-1}	9.79×10^{-1}
(2,4)	0	5.6×10^{-2}	0	8.51×10^{-2}	9×10^{-3}	1.0×10^{-1}
(3,4)	0	3.5×10^{-2}	0	3.61×10^{-2}	0	7.3×10^{-2}
(4,4)	0	1.3×10^{-2}	0	1.3×10^{-2}	0	4×10^{-2}

Table 7: Minimal and maximal values of Observed Alpha Factors

A complementary analysis can be done by comparing Real Alpha Factors and theoretical Alpha Factors (see table 8). The theoretical Alpha Factors are estimated from analytical expressions of Beta Factors obtained from the Atwood model parameter, with a conversion of Beta Factors in Alpha Factors. The deviation is defined by:

$$\delta = \frac{\alpha_{real} - \alpha_{theoretical}}{\alpha_{theoretical}}$$

	ρ=0.2		ρ=0.33		ρ=0.5	
(k,N)	Min	Max	Min	Max	Min	Max
(1,4)	-5%	2%	-8%	5%	-9%	6%
(2,4)	-100%	251%	-100%	171%	-80%	144%
(3,4)	-100%	1212%	-100%	250%	-100%	158%
(4,4)	-100%	774%	-100%	387%	-100%	364%

Table 8: Comparison between Real Alpha Factors and theoretical Alpha Factors

The deviation may be in the order of 100%, and up to 1000%, depending of the chronicle simulated. The simplifications used for analytical expressions may lead to higher deviation than the difference in available information between Real and Observed Alpha Factors.

Note: The so-called « Real Alpha Factor » is obtained with a complete information, but on a limited duration. The comparison between « real » and « theoretical » could be more relevant on durations higher than 5 ans, more representative of the real age of nuclear plants. Also, the standard deviation of the so-called « deviation » could also be used to assess the spread between chronicles, in addition to average, min and max.

V. CONCLUSIONS

In this article, we have presented how to use efficiently Colored Petri Nets (CPN) to model digital I&C system. This approach has been applied to a representative case of protection system of a nuclear power plant. The simulation permits to compare estimators of CCF parameters. An example has been presented in this article. Various estimation approaches like the Impact Vectors can be evaluated. The purpose is to assess the effect of uncertainties due to the use of simplified analytic expressions and limited knowledge from real operating experience. However the number of simulations is a key factor if the comparison has to be done with theoretical values obtained from analytical expressions.

Also, as the Atwood model may not be a fully satisfactory representation of CCF in digital I&C, further have to be done. The main ideas are to represent the various modes of CCF as described in [17], [18], by orientation and combination of CCF in the CPN model [8].

ACKNOWLEDGMENTS

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

REFERENCES

[1] *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*. NUREG/CR-5485. A. Mosleh, D. M. Rasmusson, F. M. Marshall, 1998.
[2] 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.
[3] *Estimators for the Binomial Failure Rate Common Cause Model*. C. L. Atwood, Report No.EGG-EA-5112. March 1980.
[4]. *Analysis of common cause failures in complex safety instrumented systems*. Technical note. Lilleheier, T. (2008).
[5] *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.
[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] *Common cause failures modelling by means of coloured Petri nets for dependability assessment of a control system of nuclear power plant.* N. Brınzei, G. Deleuze, N. Villaume, J.F. Petin. ESREL 2014 European Safety and Reliability Conference. Wroclaw, September 2014
[9] B. Pinna, G.Babykina, N.Brınzei, 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.
[10] IEC-61508 (2010). Functional safety of electrical/electronic/programmable electronic safety-related, Volume 1-7.
[11] IEC-61513 (2011). Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems.
[12]. *Incompletness in Data Bases: Impact on parameter estimation uncertainty*. SRA 1984 Annual Meeting, 1984.
[13]. *Technical Note: Modelling Uncertainty in Parameter Estimation*. Nuclear Safety, vol. 27, p 212, 1986.
[14]. *Hidden Sources of Uncertainty: judgement in collection and analysis of data*. Nuclear Engineering and Design, vol 93, 1986.
[15] *Procedures for Treating Common Cause Failure in Safety and Reliability Studies: Procedural Framework and Examples,* Volume 1, NUREG/CR-4780, EPRI NP-*5613*. *Pickard, Lowe, Garrick,* January 1988.
[16] *Procedures for Treating Common Cause Failure in Safety and Reliability Studies: Procedural Framework and Examples,* Volume 1, NUREG/CR-4780, EPRI NP-*5613*. Pickard, Lowe, Garrick, January 1989.
[17] *Failure modes taxonomy for reliability assessment of digital I&C systems for PRA.* OECD/AEN WGRisk Task DIGREL. 12 january 2014.
[18] *A taxonomy for the FMEA of digital I&C protection systems.* H. Bruneliere, G.Deleuze, N Thuy, C.Smidts, PSA 2013, Columbia.