Chapter 2

Models for the Reliability Analysis of Digital Instrumentation and Control Systems for Nuclear Power Plants

Jonathan M. O. Pinto, Ian B. Gomes,
Pedro L. C. Saldanha, Eustério B. Furieri and
Paulo F. F. e Melo

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/64649

Abstract

The objective of this chapter is to discuss two approaches for reliability analysis of digital instrumentation and control systems in nuclear power plants taking into account the regulatory side. Dynamic Flowgraph Methodology (DFM) and Markov/Cell-to-Cell Mapping Technique (CCMT) are discussed and case studies developed are presented. These case studies involve simplified control systems for a steam generator and a pressurizer of a Pressurized Water Reactor (PWR) plant for the purpose of evaluating each method. Advantages and limitations of each approach are addressed. For the DFM approach, three concerns in the literature are addressed: modeling of the system itself, incorporation of the methodology results into existing Probabilistic Safety Assessments (PSA), and identification of software failures. The Markov/CCMT, which has been used in dynamic probabilistic safety assessments, is approached by means of a simplified digitally controlled water volume control system. The Markov/CCMT methodology results in detailed data of the system reliability behavior in relation to time. However, it demands a higher computational effort than usual as the complexity (i.e., number of components and failure states) of the system increases. As a regulatory research conclusion, the methodologies presented can be used on PSA risk informed assessment, contributing to the regulatory side.

Keywords: DFM, MARKOV/CCMT, digital I&C systems, reliability

1. Introduction

Instrumentation and Control Systems (I&C) are an essential element in the normal, abnormal, and emergency operation of nuclear power plants [1]. These systems measure thousands of variables and activate several devices to control and protect the plant [2].

The I&C are designed to keep the process variables within plant design limits. I&C ensure plants' safety and efficient production by reacting appropriately to failures and abnormal events [2, 3].

Given the increasing incorporation of digital systems in nuclear power plants, due to their numerous advantages over analog systems, a specific approach to reliability and risk analysis has been required [4]. These systems reflect many interactions between their components (process variables, hardware, software, and human actions). Besides, physical system components have a well-defined reliability approach. The same is not true in terms of software component [5, 6].

On digital systems, software promotes flexibility, cost reduction, and reliability through its high capacity of modification without the need of replacements. If one can complete debugs software, it will continue working indefinitely, and therefore, there is no possibility of aging [5].

However, there is no perfect software. Its development process presumes human failures besides documentation and cognitive errors. Therefore, a reliability approach that models the behavior of these elements is necessary.

The construction of new reactors and the I&C modernization in the operating ones are demanding licensing and safety evaluation activities by the regulatory bodies, particularly, regulatory preparedness concerning computer-based I&C systems licensing.

The safety of nuclear power reactors is centered on deterministic concepts like defense-in-depth and diversity to minimize risks from internal or external events, which may lead to common cause failures of passive and active systems. Risk studies and lessons learned of operating reactors have contributed to improve the reliability of the new digital I&C design, but the benefits of digital technology could be impaired by the growing complexity of the components and I&C architecture due to difficulties during the regulatory review [7].

The combination of deterministic and probabilistic approaches, system architecture designed with Defense-in-Depth and diversity (D-in-D concept), the use of the best-estimate methodology for beyond design base events, like Software Common Cause Failure (SCCF), have been accepted to demonstrate the adequacy of digital I&C architectures and their functionality to meet the acceptance criteria.

In this context, the quantification of probabilistic risk analysis to demonstrate the quality and reliability attributes has been arisen many different interpretations from the industries and regulators, even considering the very low probability of the combination of some design-based accidents [like Large Break Loss of Coolant Accident (LBLOCA), in conjunction with Software Common Cause Failure].

http://dx.doi.org/10.5772/64649

To some extent, difficulties of regulatory decision making have been arisen because of different positions and interpretations from industry and regulators in explaining and applying some numbers of failure rate probabilities on digital instrumentation technologies.

The use of operational experience in case of safety qualification of digital instrumentation should be processed with relative care because of different approaches in processing operational experience data and the lack of sufficient statistical data related to safety instrumentation.

The application of traditional safety concepts and design philosophy of nuclear reactors, in the case of the new digital I&C systems, have been shown different interpretations and evaluations for the reliability and qualification of functions, and components of digital I&C systems and architectures.

Each country has its own legislation and a particular licensing process to implement the review and assessment of safety analyses. As the safety functions could be impaired by the failure of digital I&C systems redundancies (through potential software Common Cause Failure [CCF]), the currently approach know as Quantitative Software Reliability Analysis (QSRA) have been shown difficulties for regulatory decision making. The application of the D-in-D concept conservative approach (with diversity of both software and hardware) from the NRC (Nuclear Regulatory Commission) [7] has been strengthened by some regulators of countries involved with new reactor licensing (i.e., European Pressurizer Reactors, EPR design).

The industries claim that the reliability figures of new digital I&C systems have been shown equal or better failure rates than hardware and human failures. More information on recent regulatory positions and studies of quantitative software reliability analysis can be found in reference [7]. There are examples of international regulatory research to improve the bases and tools on using quantitative risk analysis for regulatory review of digital I&C technologies with more complex architecture, which include digital displays and human-factor analysis of highly integrated digital control rooms.

There are dynamic interactions present in the systems that are not treated by the traditional approaches (fault trees methodology). In addition, there are existing requirements in reliability and safety analysis (e.g., the availability of relevant information to users (as cut sets and failure probabilities) and the possibility of incorporating the results into Probabilistic Safety Assessment (PSA)) that must be met in conjunction with the dynamic interactions [4, 5, 8].

Appropriate methods for assessing safety and reliability are the key to establishing the acceptability of digital I&C systems in safety and control systems of nuclear power plants (hardware and software).

Reliability models suitable for digital I&C systems are in development process or in validation process.

Reference [8] presents the desirable characteristics a PSA methodology of a digital system must have to be applied satisfactorily. The methodologies that fulfilled the most the requirements were the Dynamic Flowgraph Methodology (DFM) and the Markov/CCMT (Cell-to-Cell Mapping Technique).

The objective of this chapter is to present two different approaches for reliability analysis of digital I&C systems applying the methodologies cited above in different case studies [5, 9–11]. Consequently, these approaches are analyzed in terms of acceptability in the regulatory context.

This chapter is organized as follows: the discussion of Dynamic Flowgraph Methodology and Markov/CCMT (Cell to Cell Mapping Technique) is presented in the following two sections. Conclusions are presented at the last section.

2. Dynamic flowgraph methodology

DFM discretizes the most relevant variables of the analyzed system in states that reflect their behavior, sets the logic that connects them through decision tables, and finally performs a system analysis, aiming, for example, the root causes (prime implicants) of a given failure top event of a fault tree.

The experience accumulated and reported in the literature indicates the DFM [4, 8] as the one that meets the most the requirements mentioned on the previous section regarding digital systems.

DFM describes interactions among the control system and other subsystems, as well as process variables. It models a system as a whole. There are examples of applications concerning failures of control systems in nuclear power plants and failures in spatial digital control systems (including dependences description) [11–14].

A network is constructed considering the causality and temporal relationship between the system elements. These elements are Process Nodes (PN), Condition Nodes (CN), Condition Edges (CO), Causality Edges (CE), Transfer Boxes (TB), and Transition Boxes (TT). More information is found in references [5, 8, 9, 11, 12, 15].

The physical system and control system main elements are the PN of the model. The discrete behavior of these elements is represented by CN [5]. TB and TT reflect the time and causality relationships between the variables [5].

Decision tables, each one associated with its respective TB/TT, are defined reflecting the possible states combination between the model variables [5].

The analysis consists in defining a top event of interest and finding out how the elements can possible combine their states, presented in the model [11].

DFM works with the concept of prime implicants [11, 13, 15, 16], which are the minimum combinations of variable states causing the top event of interest. The set of prime implicants can be used to represent the various states in which the system can be found [11].

Examples of DFM methodology and its details can be found in references [12–15]. There are applications on software failures on digital control systems, human errors, failures of control

http://dx.doi.org/10.5772/64649

systems in nuclear power plants, and failures in spatial digital control systems. This work presents a simplified example [5, 9, 11] based on a current PWR pressurizer [5].

The proposed system has the same functionality implemented by a digital system, but with some simplifications and assumptions in the controlled plant. This system and its modeling are presented on references [5, 9, 11]. It contains heaters, sprays, a relief valves, and a safety valve. Failure modes considered for each component. **Figure 1** illustrates the proposed digital system. **Table 1** summarizes the system control logic, where P is the pressure, HT is the heaters, SP is the sprays, RV is the relief valve, and SV is the safety valve.

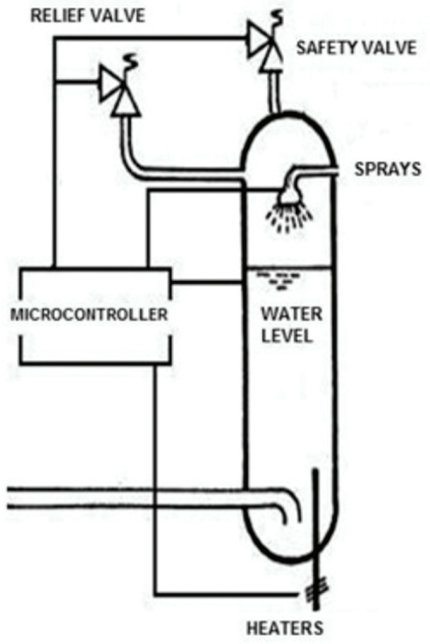

Figure 1. Proposed digital system.

P	HT	SP	RV	SV
Very low	On	Off	Closed	Closed
Low	On	Off	Closed	Closed
Lower	On	Off	Closed	Closed
Normal	Off	Off	Closed	Closed
Higher	Off	On	Closed	Closed
High	Off	On	Opened	Closed
Very high	Off	On	Opened	Opened

P: pressure; HT: heaters; SP: sprays; RV: relief valve; SV: safety valve.

Table 1. System control logic.

The system has four mechanisms of pressure control triggered by a microprocessor that runs a control logic through a software. These actuators, heating control, spraying control, and the two valve controls, are the key parameters of the control system, and therefore they will become PN in the DFM model as well as the pressure variable, which is the key parameter of the controlled process. These variable states are discretized as shown in **Table 2**, where SS is the sensor state; HTS is the heaters state; SPS is the sprays state; RVS is the relief valve state; and SVS is the safety valve state.

PN	State	CN	State
P	Very high (169–175 bar)	SS	Failed high
	High (166–169 bar)		Normal
	Higher (160–166 bar)		Failed low
	Normal (156–160 bar)	HTS	Failed on
	Lower (148–156 bar)		Normal
	Low (140–148 bar)		Failed off
	Very low (131–140 bar)	SPS	Failed on
RV	Opened		Normal
	Closed		Failed off
SV	Opened	RVS	Failed opened
	Closed		Normal
HT	On		Failed closed
	Off	SVS	Failed opened
SP	On		Normal
	Off		Failed closed

Table 2. Model process and conditions nodes.

SS	P	HT	RV
Normal	Very high	Off	Opened
	High	Off	Opened
	Higher	Off	Closed
	Normal	Off	Closed
	Lower	On	Closed
	Low	On	Closed
	Very low	On	Closed
Failed low	–	On	Closed
Failed high	–	Off	Opened

Table 3. Model TB 1.

http://dx.doi.org/10.5772/64649

The next step consists in interconnecting the model variables through transfer and transition boxes. Each of these elements has an associated decision table showing the causality relationship that exists between the variables.

The group of heaters and relief valve action logic is shown on the decision table linked to a TB (**Table 3**). The decision table related to a TT is shown in **Table 4**. This decision table shows the control mechanisms of the system [5].

P	HT	SP	RV	SV	P+
Very low	Off	Off	Closed	Closed	Very low
	Off	Off	Closed	Opened	Very low
Low	Off	On	Opened	Opened	Low
	On	Off	Closed	Closed	Lower
Normal	On	Off	Opened	Opened	Lower
	On	On	Closed	Closed	Lower
Very high	On	On	Closed	Opened	Lower
	On	On	Opened	Opened	Normal

Table 4. Model TT 1.

Var	State	Prob
SS	Failed high	0.033
	Failed low	
HTS	Failed on	0.018
	Failed off	
SPS	Failed on	0.046
	Failed off	
RVS	Failed opened	0.004
	Failed closed	
SVS	Failed opened	0.007
	Failed closed	
P	Very high	<10E-166
	High	<10E-96
	Higher	<10E-14
	Normal	9.0 10E-1
	Lower	9.2 10E-2
	Low	<10E-81
	Very low	<10E-295

Table 5. Model variable probabilities.

The DFM model provides a quantitative analysis of the results from the state probabilities of its variables. Using failure data from reference [17] and the probability distribution estimated for pressure, the probabilities were obtained and are shown in **Table 5**.

For control devices in continuous mode, 1 year of operation time in a nuclear power plant has been considered calculation. For control devices in demand mode, one demand operation has been considered. Generic failure modes for each device have been considered.

The pressure probabilities in each state were calculated from the probability density function in each interval.

Regarding the analysis, the top event "Pressure Very Low", representing one of the failures in the pressurizer control and later reactor trip is one of the top events of interest [5, 9, 11].

The toolset DYAMONDA® [15], from ASCA® Inc., was utilized.

The prime implicants or, in other words, the smallest number of combinations of variable states in the system that lead to the failure top event are searched. Setting the sentence "Pressure Very Low @ t = 0", where t = 0 is a notation indicating the end of the analysis time, the results are 32 prime implicants.

Assuming boundary conditions consisting of a proper work of the level sensor and heaters off and running, the result is the prime implicant shown in **Table 6** [5, 9, 11].

Prime Implicant Probability = 1.0609E-06
Pressure was Normal at time −1
Sensor State was Normal at time −1
Heaters State was Normal at time −1
Safety Valve State was Failed Opened at time −1
Relief Valve State was Failed Opened at time −1
Sprays State was Failed On at time −1
Sprays state was failed on at time −1

Table 6. Prime implicant for "pressure very low."

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

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

http://dx.doi.org/10.5772/64649

The results of the DFM meet this requirement. One can incorporate them by using a traditional tool in failure analysis, as the SAPHIRE code [18], for instance. This procedure is illustrated below.

The SAPHIRE code requires a text file to be imported in an extension. Ftl written in a specific format. Taking as an example, the results of the top event "Pressure Very Low", the. Ftl would be written as follows [9]:

pressure_very_low

= pressure_very_low or

pressure_very_low_subsystem_1

pressure_very_low_subsystem_2

pressure_very_low_pressurizer

etc

…

pressure_very_low _pressurizer or

prime_implicant_1

prime_implicant _1 and

pressure_normal_t-1

heaters_normal_t-1

sensor_normal_t-1

sprays_failed_on_t-1

reliefvalve_failed_opened_t-1

safetyvalve_failed_opened_t-1

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

More details regarding incorporation on PSA can be found on references [4, 8], where guidelines are made available.

DFM can be used to identify system software failures reflected in the model on the definition of some decision tables through its two modes (inductive and deductive), as shown in references [8, 19]. Once the deductive mode is utilized, one can utilize the inductive mode, step by step, to verify the correctness of the software logic.

DFM can also incorporate Human Reliability (HRA) on the system failure analysis, as shown in reference [20].

3. MARKOV/CCMT approach

Markov/CCMT [4, 21–23] is an approach that combines Markov stochastic processes with the CCMT to represent the dependencies between failure events that can originate from the dynamic interactions between the digital I&C system and the controlled process and also among the different components of the digital I&C system itself.

Markov processes can treat dependencies among events, like common-cause failures, shared-load components, and also repair.

CCMT [22–24] is a systematic procedure to describe the dynamics of both linear and nonlinear systems in discrete time and discretized system state space (like Markov processes do).

CCMT provides a very effective means to account for epistemic uncertainties, nonlinear aspects of the system dynamics, and stochastic fluctuations in dynamic system operation. CCMT produces a model that is compatible with the Markov process approach for representing failures [20, 22, 23].

The conventional Markov chain represents the stochastic evolution of a system through the transition probabilities among possible system states. Transitions between states can be represented graphically by directed links (edges) through Markov transition diagrams. Even if failure data are not available, a Markov/CCMT model can be used in both the inductive and deductive steps (that is, identification of accident sequences and safety system failure analysis, respectively) of a PSA. The results from the former can be used to obtain the relations between initiating and top events or operational state (cause-consequence relations) and the results from the latter to investigate the primary causes that lead to a specific top event or system state [4].

Importance analyses (frequency ordering of sequence events or components) can be carried out using standard PSA tools [4, 18]. If failure data are available, then the scenario frequency and top event probability can be quantified. The Markov/CCMT model can be integrated into standard PSAs using standard PSA tools [4, 8, 18, 24].

A full Markov/CCMT discretizes the whole system in states defined by the user and shows all the possible transitions between these states. The analysis is carried out by defining top events or initialing events of interest and system behavior observation. It may not be computational feasible to construct large models with Markov/CCMT (generally models with several thousands of system states) [4, 23, 24].

The steps in applying Markov/CCMT are (a) construct the Markov/CCMT model to represent the system of interest; (b) analyze the Markov/CCMT model; and (c) quantify the deductive and the inductive analytical results. These steps are described below [4].

The input to the Markov/CCMT model construction is the set of discretized system states. These states are identified from a Failure Mode and Effect Analysis (FMEA), as well as the system control logic. One must define mutually exclusive intervals (just like the process carried out in finite difference methods) for continuous process variables. These intervals are called

http://dx.doi.org/10.5772/64649

cells. Then, throughout simulations (defining final and initial conditions as well as a time-step interval), the transition probabilities between cells are found. The state transition probabilities of the system must also be simulated and combined with the former continuous variables' transition probabilities. Although some of the steps in model construction have been mechanized, general purpose software for model construction is not yet available [4].

Reference [8] shows some limitations of the methodology. These limitations comprise computational difficulties arising from the volume of model states defined (model complexity) as well as time step and mission time definition on the analysis. Also, Markov/CCMT requires a substantially larger amount of technical knowledge compared to that needed for a traditional event tree/fault tree analysis [4]. The methodology produces a large amount of data; therefore, some postprocessing of the results is required. Here, it is presented a simplified example of application of the methodology to an adapted digital control system of the water level of a typical PWR steam generator [10].

In the adapted digital system, the water level is measured by two-level sensors and their average signal is fed to the controller, which compares it to the set point. The difference is fed to a PI "Proportional-Integral" control routine that generates a correction signal, which controls a motorized feedwater valve and the water that enters the steam generator. From this adaptation, a simulation of the system was built and the Markov/CCMT methodology was applied to the system.

Failure mode		Effects	Failure rate (/h)
MC1	Signal loss of one sensor	Computer operates solely with the signal of the remaining sensor.	λ_1^{MC} 16.4×10^{-7}
MC2	Signal loss of both sensors	Computer maintains the control valve completely open.	λ_2^{MC} 8.2×10^{-7}
MC3	Processing failure of the data received by the computer	Control is transferred to the Backup Computer.	λ_3^{MC} 1.2×10^{-6}
MC4	Failure to communicate with the valve	Signal fed to the valve is 0.0 V, keeping it completely closed.	λ_4^{MC} 1.8×10^{-6}

Table 7. FMEA of the main CPU.

The next step is to perform an FMEA of this system. In this case, only its main components were considered. Failures induced by external phenomena, such as fires and radiation were not considered. Also, component repair or replacement was not considered. These restraints are not taken into account in a complete PSA. The failure rates were taken from reference [25].

Two computers work together to ensure proper system operation. In case a failure occurs in the Main CPU, the Backup CPU assumes control of the system. Failure modes of the sensors as well as failure modes of the CPUs may be considered, since the consequences of these

failures are the same [4]. **Table 7** presents the FMEA of the Main CPU and **Table 8** presents the FMEA for the Backup CPU.

It is now possible to build the Markovian transition diagrams for each of the system components, based on the Failure Modes and Effect Analyses. Since the two CPUs work together, their transition diagrams are also built together.

Failure mode		Effects	Failure rate (/h)
BC1	Signal loss of one sensor	The computer operates solely with the signal of the remaining sensor.	λ_1^{BC} 16.4×10^{-7}
BC2	Signal loss of both sensors	The computer maintains the control valve completely open.	λ_2^{BC} 8.2×10^{-7}
BC3	Processing failure of the data received by the computer	Automatic control of the process is lost and the valve is maintained closed.	λ_3^{BC} 1.2×10^{-6}
BC4	Failure to communicate with the valve	The signal fed to the valve is 0.0 V, keeping it completely closed.	λ_4^{BC} 1.8×10^{-6}

Table 8. FMEA of the backup CPU.

Other failure modes are possible for the CPUs but, in order to simplify the analysis, they were ignored. They must be considered in a full PSA.

Table 9 presents the Failure Mode and Effects Analysis of the Feedwater Valve. As was said with respect to the CPUs, other failure modes for the Feedwater Valve are possible but were ignored in order to simplify the analysis.

Failure mode		Effects	Failure rate (/h)
V1	The valve gets stuck completely closed.	The feedwater flowrate is 0, 0 and the water level decreases continuously.	λ_1^{VPC} 1.7×10^{-5}
V2	The valve gets stuck completely open.	The feedwater flowrate is max and the water level increases continuously.	λ_2^{VPC} 1.7×10^{-5}

Table 9. FMEA for the feedwater valve.

For example, the following assumptions were made for the states transitions of the CPUs: (1) the transfer of control between the two CPUs is made instantly once the Main CPU reaches state MC3; (2) the only other failure mode that is possible after the failure of one of the sensors is the failure of the other sensor; (3) the Backup CPU can only fail after it begins operating.

Figure 2 presents the Markov transition diagram for the Feedwater Valve, and **Figure 3** presents the Markov transition diagram for both the Main CPU and the Backup CPU.

http://dx.doi.org/10.5772/64649

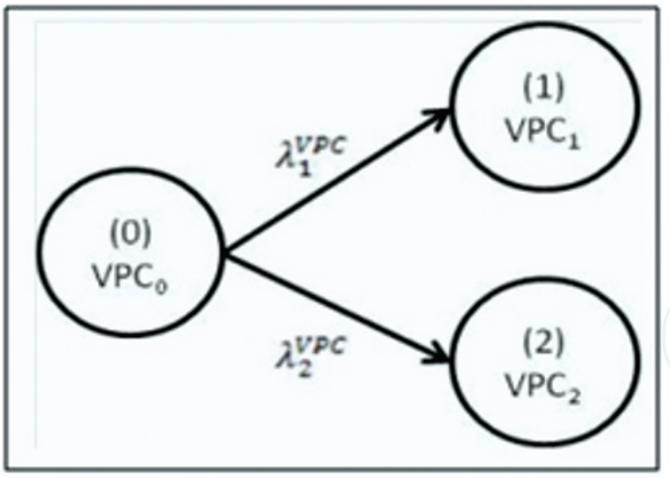

Figure 2. Markov transition diagram for the Feedwater Valve.

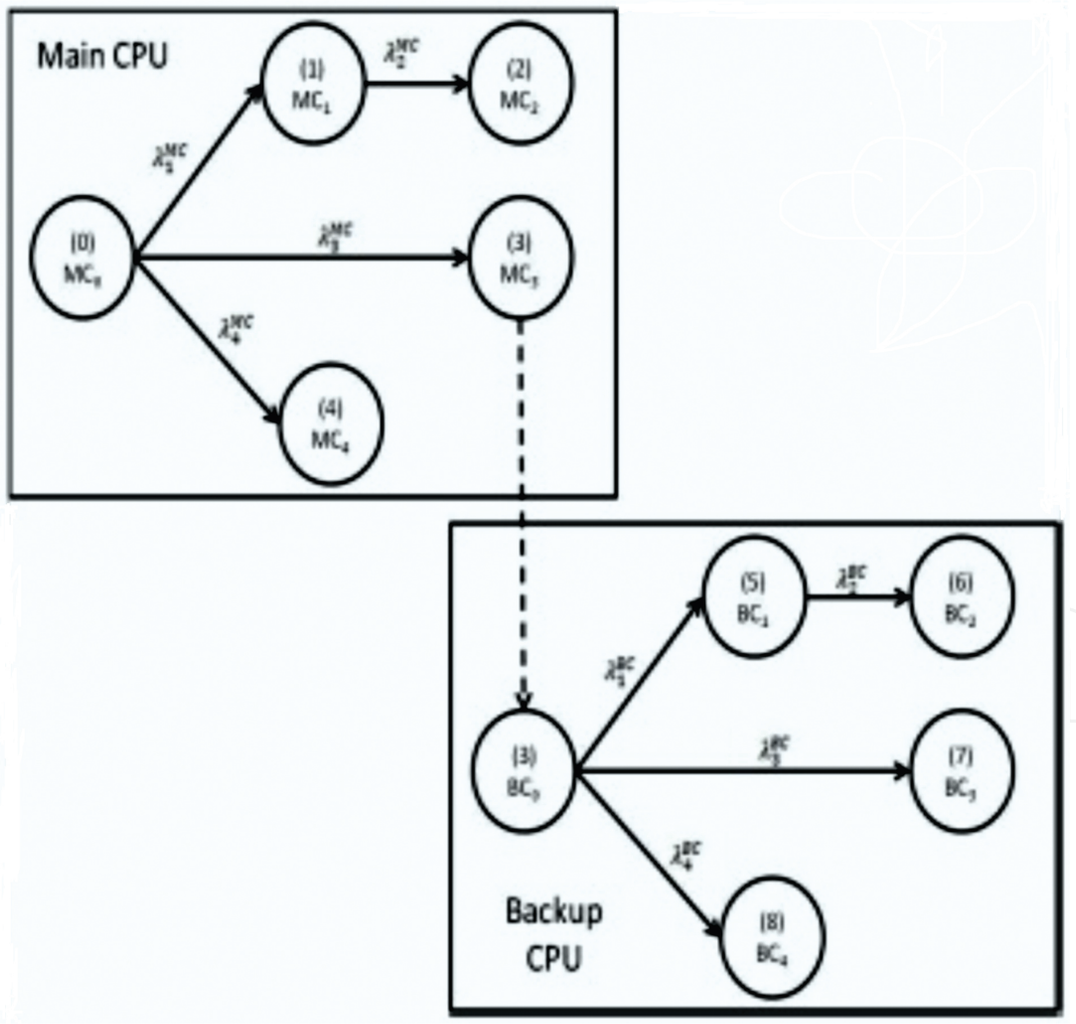

Figure 3. Markov transition diagram for the Main CPU and the Backup CPU.

From the transition diagrams, sets of differential equations are obtained. These sets of differential equations were solved using the finite difference method.

It is necessary to define a time step that must be the same for both transition diagrams. The time step must respect the following condition Eq. (1):

$$\Delta t \leq \frac{1}{\lambda} \tag{1}$$

Therefore, since the largest transition rate of the whole system is $\lambda_1^{VPC} + \lambda_2^{VPC} = 3,\ .4 \times 10^{-5}$ failures/h, the time step must respect

$$\Delta t \leq 29411.76 \text{ h} \tag{2}$$

Respecting this condition, the time step was chosen to be 10 h. It was chosen this value because it was long enough so that changes in the behavior of the system could be observed and small enough so that it could account for the changes in the operation scenario.

The next stage is applying CCMT to the system. Its first step is the Controlled Variables States Space (CVSS) partitioning, where the sole Controlled Variable for this example is the Steam Generator water level. **Table 10** shows the cells of the CVSS that were chosen for this study. These cells are subsequently divided into four subcells ($P = 4$).

$j = 1$	$x \leq 11.2$ m	Failed low
$j = 2$	11.2 m < x ≤ 11.7 m	Low
$j = 3$	11.7 m < $x \leq 12.2$ m	Normal-low
$j = 4$	12.2 m < $x \leq 12.7$ m	Normal-high
$j = 5$	12.7 cm < $x \leq 13.2$ cm	High
$j = 6$	$x > 13.2$ cm	Failed high

Table 10. Cells of the CVSS.

Once the subcells are defined, the probability $g(j|j', nc', nv', k)$ (i.e., the probability that the water level goes from cell Vj′ to cello Vj given that it was at cell Vj′, the CPUs were at state nc′ and the valve was at state nv′ at instant $t = k.\Delta t$) may be obtained. The simulation of the system is used for this purpose.

The simulation is adjusted so that the CPUs are at state nc′, the valve at state nv′, and the initial water level is at the midpoint of each of the subcells of Vj′. The number A of arrivals at cell Vj is observed and $g(j|j', nc', nv', k)$ is obtained through Eq. (3):

http://dx.doi.org/10.5772/64649

$$g(\mathrm{j}|\mathrm{j}',\mathrm{n}',k)=\frac{A}{P} \tag{3}$$

The probability of occurrence of Top Events and the reliability of the system are obtained from equations as follows:

The probability that the system is in cell Vj at $t = (k+1).\Delta t$, given that it was in cell Vj' at time $t = k.\Delta t$ is [4]

$$q_{\mathrm{j}}(k+1\,|\,\mathrm{j}',k)=\sum_{n'=1}^{\mathrm{N}} g(j|\mathrm{j}',\mathrm{n}',k)\,h_{\mathrm{n}'}(k) \tag{4}$$

where $h_{\mathrm{n}'}(k)$ is the probability that the component was at state n' at $t = k$, obtained from the Markov model. Therefore,

$$p_{\mathrm{j}}(k+1)=\sum_{j'=1}^{\mathrm{J}} q(j,k+1|\mathrm{j}',k).p_{\mathrm{j}'}(k) \tag{5}$$

Since the cells cover the whole CVSS and are mutually exclusive and exhaustive, it is possible to state that

$$\sum_{j=1}^{\mathrm{J}} p_{\mathrm{j}}(k)=1 \tag{6}$$

Having defined the Top Events, i.e., the cells where the system is considered failed (Vi), it is possible to obtain the probability that the system is failed in an instant:

$$p_{\mathrm{ET}}(k)=\sum_{i=1}^{\mathrm{I}} p_{\mathrm{i}}(k) \tag{7}$$

Therefore, the reliability of the system can be obtained from

$$R(k)=1-\sum_{i=1}^{\mathrm{I}} p_{\mathrm{i}}(k)=1-p_{\mathrm{ET}}(k) \tag{8}$$

K	*t*	**P1(k)**	**P5(*k*)**	**PET(*k*)**
0	0	0.0	0.0	0
1	10	0.0	0.0	0
2	20	0.0	0.0	0
3	30	3.5E-08	1.78955E-08	5.3E-08
4	40	2.7E-06	1.1427E-07	2.8E-06

Table 11. Probability of occurrence of a top event.

Table 11 and **Figure 4** present the resulting Top Events occurrence probability, and **Table 12** and **Figure 5** present the resulting reliability of the system.

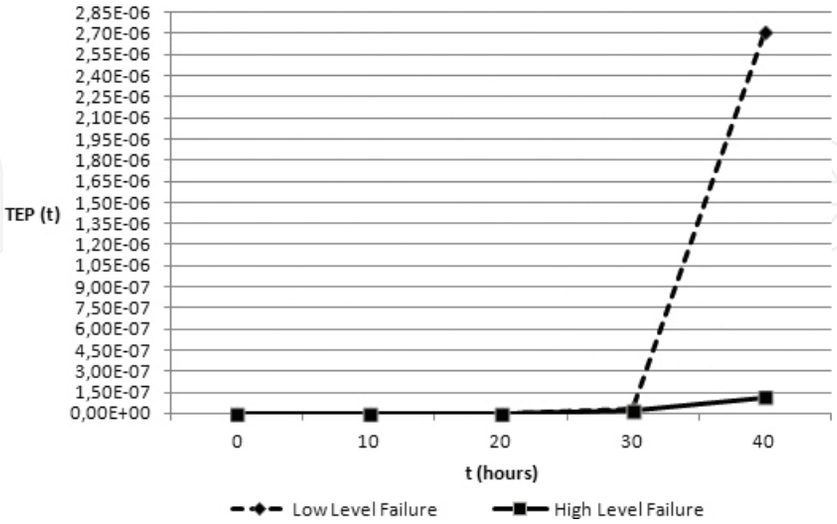

Figure 4. Probability of occurrence of a Top Event.

k	*t*	PET(*t*)	*R*(*t*)
0	0	0	1.00
1	10	0	1.00
2	20	0	1.00
3	30	5.3E-08	9.9999995E-01
4	40	2.8E-06	9.9999718E-01

Table 12. Reliability of the digital water level control system.

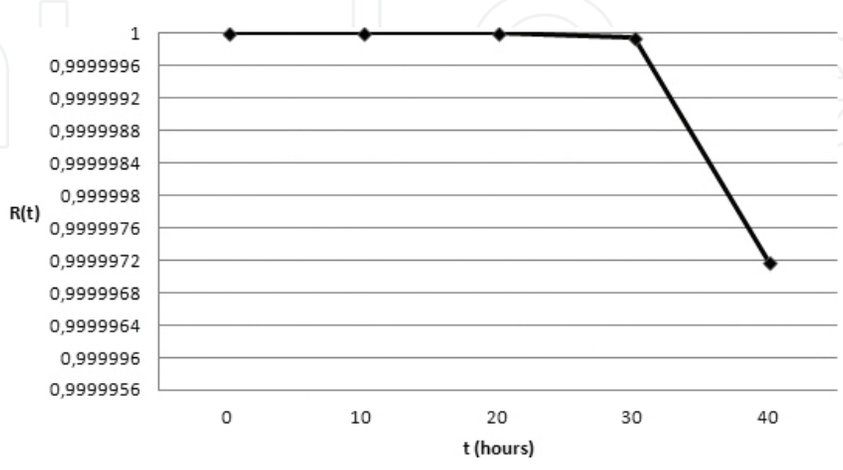

Figure 5. Reliability of the digital water level control system.

http://dx.doi.org/10.5772/64649

From the results it is possible to obtain information regarding the development of the reliability of the digital water level control system created for this study. Observing **Figure 4**, it is possible to verify that the failure with the largest probability of occurrence is low water level. In spite of the failure rates for both failure modes of the valve being the same, the failure modes of the CPUs increase the probability that the system fails low.

It is important to observe that the data in reference [25], used to obtain the failure rates of the system components, were published in 1988. Since its publication, I&C system components have been constantly improved, consequently increasing their reliability.

4. Conclusions

Appropriate methods for assessing safety and reliability are the key to establishing the acceptability of digital I&C systems in safety and control systems of nuclear power plants by the regulatory side.

Reliability models suitable for digital I&C systems are in development process or in validation process.

The traditional approach of using fault trees does not consider the dynamic interactions present in those systems; therefore, it is necessary to find a reliability methodology that takes into account these issues without violating the existing requirements concerning safety analysis.

This work discusses the application of DFM and MARKOV/CCMT to model the reliability of digital systems. As stated previously, these methodologies fulfilled the most the requirements concerning these type of systems.DFM is effective in modeling the interactions of the various components of a digital system (physical devices and software, the latter being implicit in the logic driving one or more decision tables). Through prime implicants, it allows the visualization of possible system states, failed, or not. Its deductive analysis allows an efficient study of failures tracing the causes of a given top event. Its inductive analysis can be used in the mitigation of failures found in deductive analyses and for the verification of system specifications. It can also be used for FMEA preparation, investigating the consequences of given initial conditions.

A limitation of the methodology is that the knowledge of the whole system both for modeling and for mitigations is necessary. But once built, the system can be analyzed for various failure modes and top events of interest.

As many digital systems still coexist with analog loops, it is important that the results reported by any methodology can be incorporated into existing PSAs. Only then, uncertainty and importance studies, for example, can be developed for digital systems such as those performed for other systems in failure analysis.

As the main element of a digital system is the software (and the fact that it does not have a defined reliability approach), it is quite convenient the existence of tools that enable the verification of faults and subsequent corrections in these elements.

In what concerns the Markov/CCMT approach, we intend to apply it to a PWR steam generator control system in order to assess its capabilities. The Markov/CCMT model can be used in both the inductive and deductive steps (that is, identification of accident sequences and safety system failure analysis, respectively) of a PSA to produce respectively the cause–consequence relations (event sequences and scenarios) between initiating events and top events, or operational states and the prime implicants leading to a specified top events or operational states. The ability of DFM to find the most probable causes for a specific Top Event can be used to determine the initial conditions for Markov/CCMT, which results in more detailed probabilistic data of the system's reliability behavior in relation to time. However, this methodology demands a higher computational effort than usual as the complexity (i.e., the number of components and failure states) of the system increases.

The models presented are relevant for Risk Informed decisions taken by the regulatory side where PSA models and results complement the primary deterministic requirements (regarding structures, systems, and components) to be met by the utility in the licensing process.

Author details

Jonathan M. O. Pinto[1*], Ian B. Gomes[2], Pedro L. C. Saldanha[1], Eustério B. Furieri[1] and Paulo F. F. e Melo[2]

*Address all correspondence to: jonathan.pinto.ufrj@gmail.com

1 National Commission of Nuclear Energy, Rio de Janeiro, RJ, Brazil

2 Graduate Program of Nuclear Engineering, COPPE, Federal University of Rio de Janeiro, Rio de Janeiro, RJ, Brazil

References

[1] IAEA. Modern Instrumentation and Control for Nuclear Power Plants: Guidebook. Vienna: International Atomic Energy Agency; 1999.

[2] Hashemian H. M. Nuclear Power Plant Instrumentation and Control. In: P. Tsvetkov, editor. Nuclear Power—Control, Reliability and Human Factors. Texas: Intechopen; 2011. DOI: 10.5772/18768.

[3] NRC. Digital Instrument and Controls. Washington, DC: Nuclear Regulatory Commission; 2011.

[4] Aldemir T., Stovsky M. P., Krischenbaum J., Mandelli D., Bucci P., Mangan L. A., Miller D. W., Sun X., Ekici E., Guarro S., Yau M., Johnson B., Elks C., Arndt S. A. S. Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments, NUREG/CR-6942. Washington, DC: Nuclear Regulatory Commission; 2007.

[5] Pinto J. M. O., Frutuoso e Melo P. F., Saldanha P. L. C. A DFM/ATHEANA Human Failure Analysis of a Digital Control System for a Pressurizer. In: Proceedings of the European Safety and Reliability Conference, Taylor & Francis, Netherlands; 2013.

[6] Stamatelatos M. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. Washington, DC: NASA; 2002.

[7] Furieri E. B. Internal Guideline on Review and Assessment of Digital I&C System. Brazil: National Commission of Nuclear Energy, CNEN; 2016.

[8] Aldemir T., Miller D. W., Stovsky M. P., Kirschenbaum J., Bucci P., Fentman A. W., Mangan L. T. Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessment, NUREG/CR-6901. Washington, DC: Nuclear Regulatory Commission; 2006.

[9] Pinto J. M. O., Frutuoso e Melo P. F., Saldanha P. L. C. A Dynamic Failures Evaluation of a Simplified Digital Control System for a Nuclear Power Plant Pressurizer. In: Proceedings of the European Safety and Reliability Conference, Taylor & Francis, Greece; 2010.

[10] Gomes I. G., Frutuoso e Melo P. F., Saldanha P. L. C. A Cell-to-Cell Markovian Model for the Reliability of a Digital Control System of a Steam Generators. In: International Nuclear Atlantic Conference, ABEN, Brazil; 2013.

[11] Pinto J. M. O., Frutuoso e Melo P. F., Saldanha P. L. C. A DFM/Fuzzy/ATHEANA Human Failure Analysis of a Digital Control System for a Pressurizer. Nuclear Technology. 2014;188:20–33. DOI: 10.13182/NT13-48.

[12] Aldemir T., Stovsky M. P., Krischenbaum J., Mandelli D., Bucci P., Mangan L. A., Miller D. W., Sun X., Guarro S., Yau M., Johnson B., Elks C., Arndt S. A., Dion J., Nguyen Q., Ekici, E. A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems, NUREG/CR-6985. Washington, DC: Nuclear Regulatory Commission; 2009.

[13] Yau M., Apostolakis G., Guarro S. The Use of Prime Implicants in Dependability Analysis of Software Controlled Systems. Reliability Engineering and System Safety. 1998;62:23–32.

[14] Guarro S., Yau M., Apostolakis G. Demonstration of the Dynamic Flowgraph Methodology using the Titan II Space Launch Vehicle Digital Flight Control Software. Reliability Engineering and System Safety. 1995;49:335–353.

[15] Guarro S., Yau M., Motamed M. Development of Tools for Safety Analysis of Control Software in Advanced Reactors. Washington, DC: Nuclear Regulatory Commission; 1996.

[16] Garret C. J., Apostolakis G. Automated Hazard Analysis of Digital Control Systems. Reliability Engineering and System Safety. 2002;77:1–17.

[17] IEEE. Equipment Reliability Data for Nuclear-Power Generating Stations. New York: IEEE and John Wiley & Sons; 1984.

[18] Smith C. L., Wood S. T., Galyean W. J., Schroeder J. A., Beck S. T., Sattison M. B. Systems analysis Programs for Hands-On 17 Integrated Reliability Evaluations (SAPHIRE) Summary Manual, NUREG/CR-6116. 18 Washington, DC: Nuclear Regulatory Commission; 2008.

[19] Guarro S., Yau M., Motamed M. Development of Tools for Safety Analysis of Control Software in Advanced Reactors, NUREG/CR-6465. Washington, DC: Nuclear Regulatory Commission; 1996.

[20] Aldemir T., Kirschenbaum J., Mandelli D., Bucci P., Mangan L. A., Miller D. W., Sun X., Guarro S., Yau M., Arndt S. A., Ekici, E. Probabilistic Risk Assessment Modeling of Digital Instrumentation and Control Systems Using Two Dynamic Methodologies. Reliability Engineering and System Safety. 2010;95:1011–1039.

[21] Aldemir T. Computer-Assisted Markov Failure Modeling of Process Control Systems. IEEE Transactions on Reliability. 1987;R-36:133–144.

[22] Hsu C. S. Cell-to-Cell Mapping: A Method of Global Analysis for Nonlinear Systems. New York: Springer-Verlag; 1987.

[23] Aldemir T. Utilization of the Cell-to-Cell Mapping Technique to Construct Markov Failure Models for Process Control Systems. In: Probabilistic Safety and Assessment and Management, PSAM-1, Elsevier, Greece; 1991.

[24] Aldemir T., Bucci P., Mangan L. A., Kirschenbaum J., Mandelli D., Arndt S. A. Incorporation of Markov Reliability Models for Digital Instrumentation and Control Systems into Existing PRAs. In: Proceedings of NPIC&HMIT 2006, American Nuclear Society, La Grange Park, IL; 2006.

[25] IAEA. Component Reliability Data for Use in Probabilistic Safety Assessment. Vienna: International Atomic Energy Agency; 1988.