Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN)

Philippe Weber, Lionel Jouffe

Reliability Engineering and System Safety 91/2, (2006) 149-162

Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN)

Weber Philippe[+], Jouffe Lionel*

[+] *Centre de Recherche en Automatique de Nancy (CRAN),*
UMR 7039 CNRS - UHP - INPL
2, rue Jean Lamour
54519 VANDOEUVRE-LES-NANCY Cedex – FRANCE
Email: [Philippe.Weber@cran.uhp-nancy.fr]

** Bayesia,*
6, rue Léornard de Vinci, BP 0119
53001 LAVAL – FRANCE
Email: [jouffe@bayesia.com]

Abstract Nowadays, the complex manufacturing processes have to be dynamically modelled and controlled to optimise the diagnosis and the maintenance policies. This article presents a methodology that will help developing Dynamic Object Oriented Bayesian Networks (DOOBNs) to formalise such complex dynamic models. The goal is to have a general reliability evaluation of a manufacturing process, from its implementation to its operating phase. The added value of this formalisation methodology consists in using the a priori knowledge of both the system's functioning and malfunctioning. Networks are built on principles of adaptability and integrate uncertainties on the relationships between causes and effects. Thus, the purpose is to evaluate, in terms of reliability, the impact of several decisions on the maintenance of the system. This methodology has been tested, in an industrial context, to model the reliability of a water (immersion) heater system.

Keywords: Dynamic Object Oriented Bayesian Networks (DOOBNs), Markov Chain, Reliability estimation.

1. Introduction

One of the main challenges of the Extended Enterprise is to maintain and to optimise the quality of the services delivered by industrial objects in a dynamic way along their life cycle. The purpose is to conceive decision aiding systems to maintain the system in operation. Nevertheless, most of the automated systems do not provide the means of intelligent interpretation of the information when great process disturbances have to be considered. Moreover, decisions can be taken without a perfect perception of state of the system. This partial perception argues in favour of using a probabilistic estimation of the system state. As described in [9], tools issued from the Artificial Intelligence can be used to bring help in decision aiding systems of manufacturing processes.

Works on system safety and Bayesian Networks (BNs) were recently developed in [16] and the current works presented by Boudali and Dugan [5]. Bobbio, *et al.*, [6] explain how the Fault Tree can be implemented by using BNs. In the paper [7] the authors describe the stochastic modeling techniques as FT, BN and Petri Net. They present some application cases and highlight the advantages of each technique with respect to the others. Nevertheless, large and complex BNs are difficult to design and to maintain. This is the reason why the method proposed within the SERENE project [8] is interesting. This method is based both on BNs and on a hierarchical decomposition of the decision-making model for system safety analysis. Recent publications focus on Object Oriented Bayesian Networks (OOBNs) [18], [3], [4]. Indeed, they allow to implement the SERENE methodology based on Bayesian networks.

The top down BNs construction that uses several levels of abstraction, and the powerful model elaboration mechanism for the models that have repetitive structures, make OOBNs very useful to model processes. Elementary models are then used and both the structure and the parameters can be improved through an analysis of past experiences.

Weber, *et al.* [24], proposed a model-based decision system based on a static probabilistic model that allows to diagnose faults by using an analysis of the system's functioning and malfunctioning. In order to improve diagnosis and maintenance strategies, our purpose is to define a dynamic model of the process behaviour. This model allows computing state probability distributions by taking into account both the age of the components and the latest maintenance operations.

The purpose of this paper is to introduce an Object Oriented Approach to model the system's reliability with Dynamic Bayesian Networks (DBNs) model. In [20] the authors demonstrate that DBNs are equivalent to Markov Chains (MCs). The problems that are considered here are those involving systems whose dynamics can be modelled as stochastic processes, in which the decision maker's actions influence the system's behaviour. The current state of the system and the action that is applied on that state determine the probability distribution over the next states. In the work [26] a study is dedicated to the comparison between MCs and DBNs for system reliability estimation and the paper [27] describes the reliability modelling effectiveness of the DBNs to simulate a stochastic process with exogenous constraints.

This paper is divided into 6 sections. Section 2 presents the problem statement and highlights the main drawback of a model based on a MC model, i.e. the fast growing of the state space with respect to the system complexity. Section 3 describes the Bayesian Networks theory and defines the dynamic and the object oriented representation of BN used in the following. The proposed methodology is an original formalisation that can be useful to model system reliability (section 4) by means of DOOBNs (section 5). Finally, the simulation of a water heater system is developed in section 6 and some conclusions and perspectives are discussed in Section 7.

2. Problem statement

In order to take the uncertainty into account, the process state is considered as a random variable that takes its values in a finite state space corresponding to the set of all the possible process states. A MC allows to model the system dynamics over these states [9].

2.1. The Markov Chain notations in reliability

We will first of all define the notations used to describe the MC model. Let X be a discrete random variable used to model a process with a finite number of mutually exclusive states $\{s_1,...,s_M\}$. The vector π, then, denotes a probability distribution over these states:

$$\pi = [\pi(s_1) \quad ... \quad \pi(s_m) \quad ... \quad \pi(s_M)],\ \pi(s_m) \geq 0$$
$$\text{with } \pi(s_m) = p(X = s_m) \text{ and } \sum_{m=1}^{M} \pi(s_m) = 1 \qquad (1)$$

Assuming that the occurrence of events imply system state transitions, from a state at time step (k-1) to a state at time step (k), the process produces a sequence $(\pi_0, \pi_1, ...\pi_{k-1}, \pi_k)$ that can be modelled as a discrete MC if: $\pi_k(s_m) = p(X_k = s_m | \pi_{k-1})$. The Markov property makes it possible to specify the statistical relationship among states as a transition probability matrix $\mathbf{P}_{MC}$. The MC is qualified as homogeneous if the state transition probabilities $p_{ij} = p(X_k = s_j | X_{k-1} = s_i)$ are time independent.

The reliability of a system can be modelled by using a MC. This method leads to a graphical representation ([1], pp. 124). Let's consider the modelling of a component (entity). We will use a discrete random variable X with two states {*up*, *down*} to represent respectively the operational and failure state of the component. The matrix PMC described below defines the probabilistic state transitions between (*up*) and (*down*):

$$\mathbf{P}_{MC} = \begin{bmatrix} 1 - p_{12} & p_{12} \\ 0 & 1 \end{bmatrix} \qquad (2)$$

Where p_{12} represents the failure probability of the component between time steps (k-1) and (k) $p_{12} = p(X_k = down | X_{k-1} = up)$. Let T the time to failure of the component be a positive random variable with an exponential distribution $f(T) = \lambda \cdot e^{-\lambda \cdot t}$. In reliability studies, λ is the parameter known as the component failure rate. Then, we have: $p_{12} \approx \lambda \cdot \Delta t$ (see page 37 in [2]) where Δt represents the time interval between time steps (k-1) and (k), λ being a probability per time unit (Fig. 1). In the following Δt is assumed to be equal to 1 hour. For constant failure rates, the Mean Time to Failure (MTTF) is defined (see page 87 in [10]): $MTTF = 1/\lambda$.

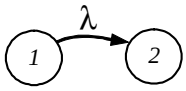


Fig. 1. Markov Chain.

2.2. Problem to model complex process

The MC method is suitable for computing the reliability of entity or system of low complexity. However, when we deal with complex systems with several components, we assist to a combinatorial explosion of the number of states that are necessary to model the system reliability, making MC unmanageable. To decrease the model's complexity, the hypothesis (a) according to which there is no simultaneous occurrence of failure is assumed. Even if this hypothesis simplifies the transition probability matrix, the number of states is still prohibitive for the modelling of complex real systems with MC.

In practice, to deal with this modelling problem, methods based on Fault Tree (FT) or Success Tree (ST) (p. 146 in [10]) can be used. These methods assume the statistical independence between events (hypothesis (b)), and they also assume that a static model of the situations is given. However, hypothesis (b) is no longer valid when components have common causes or when components have several failure modes.

Stochastic Petri Net ([19] and [11]) is also a method traditionally used to model the system reliability. Stochastic Petri Nets provide a powerful modelling formalism. Unfortunately, the reliability analysis relies on a Monte Carlo

simulation procedure that requires a great number of simulations when very low probabilities are targeted.

The following part deals with a method that will allow to exploit the advantages of both the MC and the FT approaches within a single representation that does not assume the hypotheses (a, b) and that does not rely on a Monte Carlo simulation to calculate the systems reliability. This method is based on Dynamic Bayesian Networks.

3. Bayesian Network theory

BNs are probabilistic networks based on graph theory. Each node represents a variable and the arcs indicate direct probabilistic relations between the connected nodes. Variables are defined over several states. The DBNs allow to take into account time by defining different nodes to represent the variables at different time slices.

3.1. The Bayesian Network notations

BNs are directed acyclic graphs used to represent uncertain knowledge in Artificial Intelligence [15]. A BN is defined as a couple: $\mathsf{G}=((N, A),\mathsf{P})$, where (N,A) represents the graph; "N" is a set of nodes; "A" is a set of arcs; P represents the set of probability distributions that are associated to each node . When a node is not a root node, i.e. when it has some parent nodes, the distribution is a conditional probability distribution that quantifies the probabilistic dependency between that node and its parents.

A discrete random variable X is represented by a node $n \in N$ with a finite number of mutually exclusive states. States are defined on $\mathsf{S}_n : \{s_1^n, ... s_M^n\}$. The vector π^n denotes a probability distribution over these states as eq. (1), where $\pi^n(s_m^n)$ is the marginal probability of n being in state s_m^n. In the graph depicted in Fig. 2, nodes n_i and n_j are linked by an arc. If $(n_i, n_j) \in A$ and $(n_j, n_i) \notin A$ then n_i is considered as a parent of n_j. The set of the parents of node n_j is defined as $pa(n_j) = n_i$.

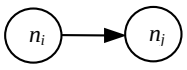


Fig. 2. Basic BN.

In this work, the set P is represented with Conditional Probability Tables (CPT). Then, each node has an associated CPT. For instance, in Fig. 2, the nodes n_i and n_j are defined over the sets $\mathsf{S}_{n_i} : \{s_1^{n_i}, ... s_M^{n_i}\}$ and $\mathsf{S}_{n_j} : \{s_1^{n_j}, ... s_L^{n_j}\}$.The CPT of n_j is then defined by the conditional probabilities $p(n_j | n_i)$ over each n_j state knowing its parents states (n_i). This CPT is defined as a matrix:

$$\mathbf{P}\left(n_j \middle| pa(n_j)\right) = \begin{bmatrix} p\left(n_j = s_1^{n_j} \middle| n_i = s_1^{n_i}\right) & \cdots & p\left(n_j = s_L^{n_j} \middle| n_i = s_1^{n_i}\right) \\ \vdots & & \vdots \\ p\left(n_j = s_1^{n_j} \middle| n_i = s_M^{n_i}\right) & \cdots & p\left(n_j = s_L^{n_j} \middle| n_i = s_M^{n_i}\right) \end{bmatrix} \quad (3)$$

Concerning the root nodes, *i.e.* those without parent, the CPT contains only a row describing the *a priori* probability of each state.

Various inference algorithms can be used to compute marginal probabilities for each unobserved node given information on the states of a set of observed nodes. The most classical one relies on the use of a junction tree (see [15], pp. 76). Inference in BN [13] then allows to take into account any state variable observation (an event) so as to update the probabilities of the other variables. Without any event observation, the computation is based on *a priori* probabilities. When observations are given, this knowledge is integrated into the network and all the probabilities are updated accordingly.

Knowledge is formalised as evidence. A *hard evidence* of the random variable X indicates that the state of the node $n \in N$ is one of the states $\mathsf{S}_n : \{s_1^n, ... s_M^n\}$. For instance X is in state $s_1^n : p(n = s_1^n) = 1$ and $p(n = s_{m \neq 1}^n) = 0$. Nevertheless, when this knowledge is uncertain, *soft evidences* can be used (see [22]). A soft evidence for a node n is defined as one that enables the updating of the prior probability values for the states of n. For example, X is in state s_1^n and s_M^n with the same probability and not in the other states: $p(n = s_1^n) = 0.5$, $p(n = s_M^n) = 0.5$ and $p(n = s_{m \neq (1,M)}^n) = 0$.

3.2. Dynamic Bayesian Network

A DBN is a BN that includes a temporal dimension. This new dimension is managed by time-indexed random variables. X_i is represented at time step k by a node $n_{(i,k)} \in N$ with a finite number of states $\mathsf{S}_{n_i} : \{s_1^{n_i}, ... s_M^{n_i}\}$. $\pi_k^{n_i}$ denotes the probability distribution over these states at time step k. Several time stages are represented by several sets of nodes $N_0, \ldots N_k$. N_k includes all the random variables relative to time slice k ([14] and [9] pp. 38-45).

An arc that links two variables belonging to different time slices represents a temporal probabilistic dependence between these variables. Then DBNs allow to model random variables and their impacts on the future distribution of other variables. Defining these impacts as *transition-probabilities* between the states of the variable at time step k-1 and those at time step k leads to the definition of CPTs, that are relative to inter-time slices, equivalent to the one defined in the previous section (eq. (3)). With this model, the future slice (k) is conditionally

independent of the past given the present (k-1), which means that the CPT $\mathbf{P}(n_{i,k}|pa(n_{i,k}))$ respects the Markov properties [17]. Moreover, this CPT is equivalent to the Markovian model of the variable X_i described in section ***2.1*** if $pa(n_{i,k}) = n_{i,k-1}$ and $\mathsf{S}_{n_{i,k-1}} = \mathsf{S}_{n_{i,k}}$ *i.e.*:

$$\mathbf{P}(n_{i,k}|n_{i,k-1}) = \mathbf{P}_{MC} \quad (4)$$

Starting from an observed situation at time step k=0, the probability distribution $\pi_k^{n_i}$ over n_i states is computed by the DBN inference. To compute $\pi_{k+T}^{n_i}$, several solutions are proposed in the literature. One of them consists in developing T time slices, resulting to a network size growing proportionally to T [17]. In this work, we have chosen another solution that allows keeping a compact network form, and that uses iterative inferences [28]. The notion of time is introduced through inference. Indeed, it is possible to compute the probability distribution of any variable X_i at time step k based only on the probabilities corresponding to time step k-1. The probability distributions at time step k+1… are computed using successive inferences. Then, a network with only two time slices is defined Fig 3. The first slice contains the nodes corresponding to the current time step (k-1), the second one those of the following time step (k). Observations, introduced as hard evidence or probability distributions, are only realised in the current time slice. The time increment is carried out by setting the computed marginal probabilities of the node at time step k as observations for its corresponding node in the previous time slice.

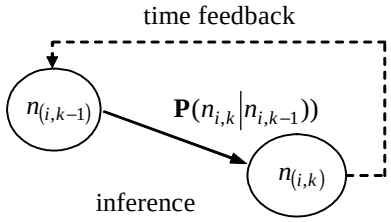


Fig. 3. DBN for the random variable X_i.

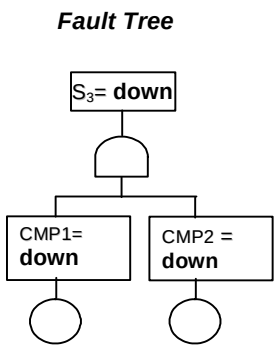


Fig. 4. Classical FT models of parallel components.

3.3. Object Oriented Bayesian Networks

Modelling systems containing an important number of variables with BNs generally leads to complex models. To avoid this phenomenon, Koller has defined a particular class of BNs, the Object Oriented Bayesian Networks (OOBN) [18]. Their modelling is based on the decomposition of the global network into hierarchical levels [3],[4]. This representation method allows to decentralize and to structure the knowledge within BNs of reduced size. Thanks to their structure, the OOBNs are then well suited for the modelling of industrial systems.

4. Reliability models with BN

Bayesian networks provide a powerful mathematical formalism to model complex stochastic processes. The equivalence between Bayesian Networks and the classical Fault Trees method is described in the following section in the same way as it is in [6] and [5]. The comparison between Fault Trees and Bayesian Networks is done under the hypothesis of Fault Trees validity: in other words, events related to components or to functions can only be modelled with binary states. Then, the power of BN will be presented in the next section. We will argue that BNs are well suitable methods for the modelling of the complex propagation of failures through a probabilistic network of multimodal variables. This section will present the BN model of the dependent failure modes and the propagation of uncertainty. The last section will describe the dynamic BN and their equivalence to the Markov Chains.

4.1. Fault Trees and Bayesian Networks to model reliability

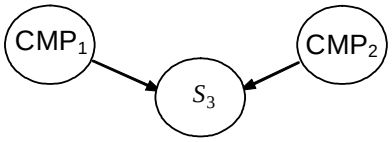
A Fault Tree allows to describe the propagation logics of the failure across the system. System reliability or availability are modelled according to the assumption of independence between the events affecting the entities (hypothesis (a), see chapter 7 in [10]).

When components cannot be repaired, the basic fault events represent component failures. Under such conditions, the probability evaluation of fault trees based on the failure rates corresponds to the system reliability. The hypothesis (a) is then naturally respected. When components are repairable, the basic fault events depend on the failure and repair rate. Thus, the components' unavailability are computed using a Markov model and used as basic events in the FT. Under assumption (a), the probability evaluation of such fault trees corresponds to the system unavailability. Nevertheless, from a practical view point, hypothesis (a) is hardly verified. Indeed, in the case of a repairable system, the failure of a component generally has an effect on the behaviour of the other components. Therefore, in this paper the purpose is only to model the systems' reliability.

The following notation is adopted: (CMP = *up*) indicates that the component CMP is functioning, and (CMP = *down*) indicates that a failure has occurred (the component is then unable to perform its function). Fig. 4 compares elementary models of parallel components CMP1 and CMP2 that make up the system function S_3. Whereas a classical model of this parallel structure is based on a Fault Tree, the modelling with

Bayesian Network is realized with a single structure as depicted in Fig. 5 (the structure is identical for serial configurations). The CPT contains the conditional probabilities that translate the failure propagation logics across the functional architecture of the system. Therefore, the CPT is defined automatically by an OR/AND gate. These CPTs are *a priori* given, and probabilities are equal to 0 or 1 since the logic of the failure propagation is deterministic. To compute the reliability of the function S_3, events on component are considered as statistically independent ([12] and [23]):

$$\begin{aligned} &\Pr(S_3 = up)_{ET} = \Pr(CMP_1 = up \cap CMP_2 = up) \\ &\Pr(S_3 = down)_{FT} = \\ &\qquad \Pr(CMP_1 = down \cup CMP_2 = down) \\ &\Rightarrow \Pr(S_3 = up)_{ET} = \prod_{i=1}^{n} \mathbf{Pr}(CMP_i = up) \\ &= 1 - \prod_{i=1}^{2} \Pr(CMP_i = down) = \Pr(S_3 = up)_{BN} \end{aligned} \quad (5)$$



$\mathbf{P}(S_3 | CMP_1, CMP_2)$

	CMP_1	up		down	
	CMP_2	up	down	up	down
S_3	up	1	1	1	0
	down	0	0	0	1

Fig. 5. Equivalent BN of the parallel structure.

4.2. BN to model dependent failure modes and uncertain propagations

Thanks to the CPTs, BNs provide a model of the propagation of several failure modes in the system. Then, it is possible to synthetically represent in a factorised form system made up of entities with several failure modes. The hypothesis of independence between events (failures) made for FT is not necessary. Indeed, BNs allow computing exact repercussions of dependent variables to the system reliability. Moreover, it is possible to introduce uncertainty by setting probabilities in the interval of value [0, 1].

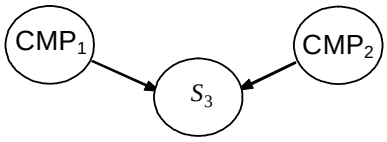
Failure Mode, Effects Analysis (FMEA) [23] allows to determine the failure modes associated with a component (Table 1). Therefore, the states (considered as exhaustive) of a CMP node are, for instance:

- *up*: the component is available,
- *down1*: the component is unavailable due to the failure 1,
- *down2*: the component is unavailable due to the failure 2…

Table 1. FMEA.

Failure Modes	*Causes*	*Effect*
function in mode 1	CMP failure1	Effect 1
	CMP failure2	Effect 2

The states of function S3 are defined by failure modes. For instance, node S3 in the BN (Fig. 6) takes the following states: *up* or *down.* No prior probability is associated with these states because they are computed according to the states of their parents, i.e. the causes described by CMP_i nodes.



$\mathbf{P}(S_3 | CMP_1, CMP_2)$

	CMP_1	up		down1		down2	
	CMP_2	up	down	up	down	up	down
S_3	up	1	1	1	0	0.2	0
	down	0	0	0	1	0.8	1

Fig. 6. BN to model complex structure.

The CPT of the function S_3 is defined by using the columns of the causes and the failure modes of the FMEA analysis. Nevertheless, a BN representation can turn out to be useful insofar as a combination of causes (for instance CMP_1=*down2* and CMP_2=*up*) can lead to several failure modes of the function with different probabilities. In Fig. 6, the uncertainty is represented by the probability distribution (0.2; 0.8).

As it is known in the FMEA analysis, a failure mode can happen to cause other failure modes according to the logics of the failure propagation through the system. The BN representation is able to model this propagation; nevertheless the construction of this model has to be structured. Section 5 of this paper presents a method to model the reliability of complex systems.

4.3. Dynamic Bayesian Networks to model entities

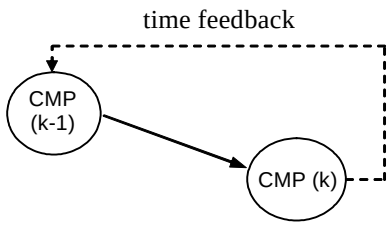


Fig. 7. Generic Component DBN.

The reliability of low complexity components can be modelled as a DBN made up of two nodes as presented in Fig. 7. An MC model of component X_i reliability is easily translated into a DBN model [26]. Thus, independent components (entities) of the process are modelled using DBN equivalent to an independent MC. For instance, as it is defined in section ***2.1***, a component is modelled by a discrete random variable X with states {*up*, *down*}. Then two nodes are defined to model the random variable at time slices (*k*) and (*k*-1): CMP(*k*) and CMP(*k*-1). These nodes, linked by an arc that represents the dependency between the component states at time step *k* and its states at time step (*k*-1), are both described by the states {*up*, *down*}.

Equations (2) and (4) define the CPT $\mathbf{P}(CMP(k)|CMP(k-1))$ linking the two time slices. The parameters are those defined to build the MC model of the component. To compute the probability $p(CMP(k)=up)$ according to which the variable X_i is in the state *up* at (*k*), the following equation may be used:

$$p(CMP(k)=up)=(1-\lambda\Delta t)\,p(CMP(k-1)=up) \quad (6)$$

Equation (6) corresponds to the classical formula of the discrete model of the MC.

5. Modelling approach

The main interest of such a method enabling a reliability modelling thanks to BNs lies in the propagation of the component failure states through the functionality of the system. Nevertheless, modelling complex systems requires a methodology that will help specify the BN's structure and the states of its variables. Methods like Structured Analysis and Design Technique (SADT) and FMEA are traditionally used in practice; therefore we will endeavour to formalise the BN from this knowledge representation [25].

5.1. Unification of system functioning and malfunctioning knowledge

The model is elaborated before the implementation of the system. By that time, the main technological choices are made. But it is still necessary to define the logistics of maintenance which contribute to reach goals in terms of performance. We propose here to design the BN model by using both the functional analysis (SADT) and the malfunctioning analysis of the system (FMEA). The definition of the environment, external resources, and failure modes are formalised at the level of the main function and Elementary Function (EF). The description of the components failures and reliability are made at the level of component (CMP).

The modelling approach consists, from the analysis of the systemic functioning based on SADT graphical representation [21], in representing the abnormal operation (malfunctioning) based on FMEA and then in formalising and unifying these two results in a unique model by means of OOBNs.

The functioning and malfunctioning of the system are dual and must be studied together to control each system variable. It leads, first, to focus on the system functioning in relation to its environment and its internal and external resources. This action can be made by using SADT graphical representation. This modelling is based on a principle of functional decomposition of the components, from functions and sub-functions to elementary functions.

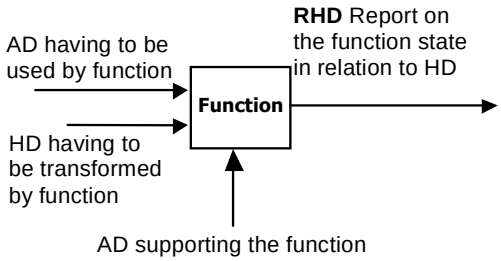


Fig. 8. Flows and Function Representation.

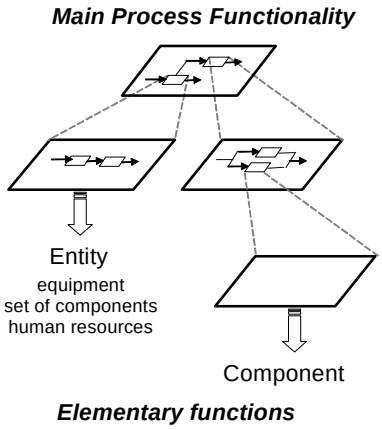


Fig. 9. Functional decomposition.

Each function (Fig. 8) represents a modification of a "product" carried out by the system. It produces or consumes flows such as "Having to Do" (HD) materialising the Input/Output (I/O) finality and "being Able to Do" (AD) representing I/O energies, resources, activity support. From this step, simplifying assumptions are made for estimating the reliability. Therefore, the output flow is a report (RHD) that represents the function's finality. This flow is assumed to be the added value on the product flow represented in Fig. 8 by the Input HD flow that is transformed by the function. This output flow represents the functioning or failure modes of the function (as reliability of the function). Only the RHD flow is taken considered as output. It is thus transferred as informational view of physical result through the input flow of another function.

From this functioning, the malfunctioning is induced by considering that the relationship between these two modes is directly linked to the relationship between the normal and

abnormal states of the variables. An FMEA analysis enables to create a malfunctioning model that helps identify the failure or degradation modes of each function, the elements that are responsible for the failure (causes) and the possible consequences of these failures (effects).

For example, the RHD flow can take the value "*up*" corresponding to the nominal state of the activity or the values "*down1*", "*down2*" to identify the causes and the effects associated with these two abnormal states. The failure causes are either external (linked to the Input flows) or internal when they are linked to the AD function support flow (components). A set of states can thus be associated with each component. These states correspond to: nominal operation, failure 1, failure 2…

In the same way, the consequences are observable either on function output flows or on the influence of the component degradation development on itself (to go towards a breakdown state). To sum up, a failure cause leads to a failure mode (e.g. the modification of the function state reported in RHD), which leads the function to be unable to produce the HD nominal flow any more.

5.2. Reliability modelling with OOBN

The Bayesian Network representation is based on the functional decomposition of the system. The flows are represented by discrete random variables that are represented by the nodes of the BN. This representation is structured as a tree (Fig. 9). Its root is an OOBN representing the highest abstraction level. The elementary functions represent the lowest functional levels modelled by BNs. The connections between the sub-functions are modelled by logical functions. OOBNs are consist of generic sub-functions in the high functional levels of the model.

Then, a unified representation can be obtained by directly building OOBNs from the dual functioning/malfunctioning analysis presented above. To keep the concept of the generic function, inputs are modelled by input nodes defining the random variables associated with the flows AD, HD. The generic function represented in BN formalism is given in Fig. 10.

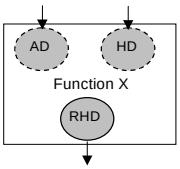


Fig. 10. Generic BN input and output nodes structure.

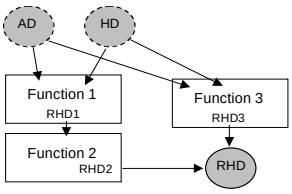


Fig. 11. High level of the functional decomposition.

To model high functional levels, OOBNs are composed of generic sub-functions that are structured as in Fig. 10. When the function carries out several missions, it is possible to duplicate several inputs or outputs nodes (AD, HD…). Moreover, it is also possible to model sub-functions in parallel or in series (Fig. 11).

In Fig. 11, as the generic sub-functions F1 and F2 are in line, the report RHD1 is transferred to F2 through the input flow HD. As the functions F2 and F3 form a V structure, the node RHD is linked to RHD2 and RHD3 in order to compute the RHD of the overall function. The connections between functions are defined as CPT that represents the propagation logics of the failure modes, as it is presented Fig. 6.

OOBNs allow to describe systems thanks to serial or parallel component architectures. However, the CPTs—rather than the OOBN structures—constitute the relations of serial or parallel architectures.

Thus, the same relation between functions can be represented by the two different structures depicted in Fig. 12 and Fig. 13. This structural difference has no impact on the calculations of reliability if the CPT is defined as follows, where * is a logical operator representing the relation between functions F_1 and F_2:

- Fig. 12: the CPT of the node F3 defined $P(F_3|F_1, F_2) = P(F_1) * P(F_2)$.
- Fig. 13: the CPT models the transformation $P(X|F_1, F_2) = P(F_1) * P(F_2)$ and the CPT associated to F_3 ($P(X|F_3)$) corresponds to the identity operator (i.e. the CPT's diagonal is equal to 1, all the others probabilities being equal to 0).

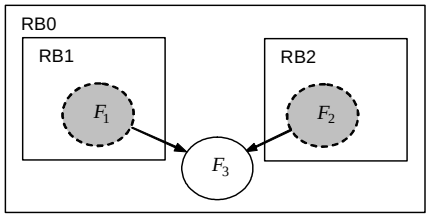


Fig. 12. RB: V structure.

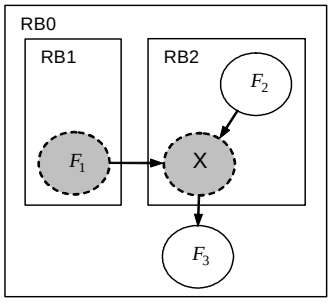


Fig. 13. RB: in line structure.

These two structures are then equivalent. The choice of one structure rather than another depends on the specificity of the problem

The OOBN model offers the possibility to compute the system reliability. However, equivalence between FTs and BNs is verified only if the system variables are described as binary.

This restrictive hypothesis does not apply to BNs as they allow to consider random discrete variables defined on an unrestricted set of states. In short, a BN can always be defined as equivalent to a FT, but the reverse is false. Therefore, the modelling of failure modes by OOBN represents an increase of precision with respect to the reliability model.

5.3. To model Elementary Function states related to components

If a component is used to perform several sub-functions, the output node CMP of the Component BN appears at the highest level containing the component. If a component performs only one sub-function (Elementary Function EF), the output node CMP appears as an AD flow supporting the function (Fig. 8) in a generic sub-function BN (Fig. 14).

The CMP output nodes are directly linked to the EF nodes representing their functionality. The CMP states are defined by the causes analysed by means of FMEA. The causes are either internal to the low BN level i.e. linked to CMP, or external, i.e. linked to the input nodes AD or HD. The common causes are defined in higher hierarchical levels and the information is forwarded by heritage between the levels through the input and output nodes.

The EF nodes are linked to the CMP nodes and to the input nodes leading to compute the RHD states probabilities (Fig. 14). If all the EFs are up then the RHD is up.

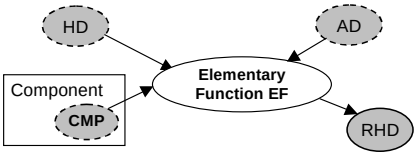


Fig. 14. Low level of the functional decomposition.

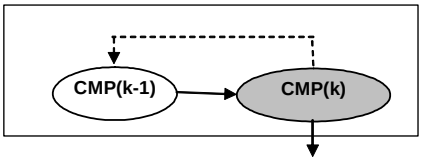


Fig. 15. Generic Component BN.

5.4. Model of components DOOBN

As for functions, a generic model is proposed for components (or for a set of components). Fig. 15 describes a Dynamic Object Oriented Bayesian Network DOOBN representing the model of a generic component: a component node CMP(k-1) and its evolution defined as a Markov Chain modelled by the CPT of the node CMP(k).

It is now necessary to determine the probabilities associated with the states of the component. These probabilities depend on the reliability of the component.

Then, the probabilities associated with CMP(k) node states in the BN are estimated for a given operating time (Table 2).

The CMP(k) node is defined as an output node. Then, probabilities associated with the CMP(k) states are used to compute probabilities of the Elementary Function states related to this component.

Table 2. Component states and probabilities.

CMP(k=0)	up (correct operation)	1
	down1 (cause of failure 1)	0
	down 2 (cause of failure 2)	0

5.5. Use of the model in operation: reliability estimator

The objective of the decision-making problems is to compare several alternative solutions (combination of decisions). The proposed model allows the simulation of several scenarios.

Once decisions have been taken, the BN model defined above can be used as an estimator of the system's reliability with respect to the chosen policy. The BN model allows to analyse the influences implied by the degradations on the functions' states. This analysis is based on the simulation of a component failure, a common cause or an unconformity of a sub-function. The objective is to forecast the impact of failures on the functions. It is then possible to analyse the upstream and downstream consequences on the whole system. For example, if we consider a component failure, an evidence can be set as P (CMP=down1) = 1. The sub-functions probabilities are then updated by the BN inference. The RHD of each function relates the failure impact on each functional level.

6. Application

The proposed method is applied to a classical example of a water heater process. The objective of the thermal process (show in Fig. 16) is to ensure a constant water flow rate with a given temperature. The process is composed of a tank equipped with two heating resistors R1 and R2.

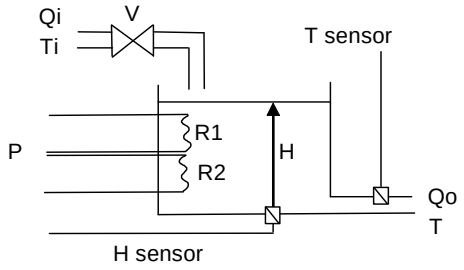


Fig. 16. Thermal process.

The system inputs are the water flow rate Qi, the water temperature Ti and the heater electric power P that is controlled by a computer. The outputs are the water flow rate Qo and the temperature T that are regulated around an operating point (Qi=Qo= 20 $l.min^{-1}$ and T = 50°C). The input temperature of the water Ti = 20°C is assumed to be constant.

The components of this system are indexed in the FMEA analysis (Table 3). The failure modes of each component are defined as well as their effects. The causes are linked with the component states or the unavailability of the electric energy required to supply the component. Therefore, the loss of energy is a common cause of the 6 failure modes.

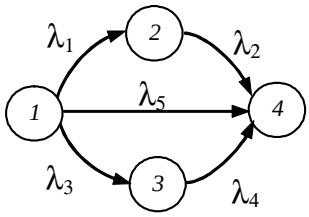
The figures (Fig. 17 to Fig. 23) present the Mean Time To Failure (MTTF) parameter allowing to determine the failure rates quantifying the transition between component states. These figures depict the Markov Chains of the components, which are considered, in this study, as independent. State 1 represents a component without failure.

The process is made of seven components that have 2, 3 or 4 states. Modelling the system with a Markov Chain leads to define 1728 states (4x2x3x4x3x3x2=1728). The system's reliability is then computed according to the transition matrix $\mathbf{P}_{MC}$ that defines the probabilities linking all the states. This matrix requires approximately 3 million parameters.

Therefore, the reliability estimation of this process from the MC model is very difficult to obtain. In the following, the DOOBN modelling proves to be a more efficient and convenient tool. This model is a unified representation of the knowledge formalised from FMEA, SADT analysis, and independent MC of components.

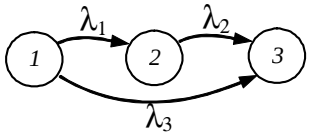
Table 3. FMEA - Component states.

Function	***Element***	***Failure Mode***	***Effects***	***Causes***
to transform pressure to Qi	VALVE V	Remains closed	*Qi=0*	*No energy from (AD)* *Valve is down (state 4)*
		Remains open	*Qi>0*	*No energy from (AD)* *Valve is down (state 3)*
		The water flow rate is biased	*Qi different from the desired Qi*	*Valve is down (state 2)*
to stock water Qi to H	TANK	Leak of water	*Water loss in the environment*	*Tank is down (state 2)* *Fissure*
to transform H to Qo	WATER PIPE	Clogged	*Qo =0*	*Pipe is down (state 3)*
		Restricted	*Qo< desired Qo*	*Pipe is down (state 2)*
to heat water from Ti to T	HEATING RESISTOR	Maximum level of heat	*T> desired T*	*Heating resistor is down (state 2)*
		No heating	*T=Ti = 20°C*	*No energy from (AD)* *Heating resistor is down (state 4)*
		Heating power loss	*T< desired T*	*Heating resistor is down (state 3)*
to measure H	H SENSOR	Biased measure	*Qo is different from the real Qo*	*H sensor is down (state 2)*
		No measure	*Impossibility to control Qo*	*No energy from (AD)* *H sensor is down (state 3)*
to measure T	T SENSOR	Biased measure	*T is different from the real T*	*T sensor is down (state 2)*
		No measure	*Impossibility to control P*	*No energy from (AD)* *T sensor is down (state 3)*
to control V and P	COMPUTER	Control loss	*Deviation of T and H*	*No energy from (AD)* *Computer is down (state 2)*



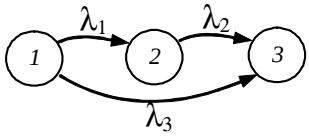
$MTTF_1$=10 000 h	λ_1=1 10^{-4} h^{-1}
$MTTF_2$=500 h	λ_2=20 10^{-4} h^{-1}
$MTTF_3$=7 000 h	λ_3=1.43 10^{-4} h^{-1}
$MTTF_4$=2 000 h	λ_4=5 10^{-4} h^{-1}
$MTTF_5$=15 000 h	λ_5=0.66 10^{-4} h^{-1}

Fig. 17. HEATING RESISTOR reliability MC model.



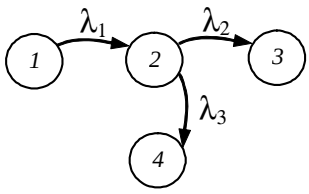
$MTTF_1$=5 000 h	λ_1=2 10^{-4} h^{-1}
$MTTF_2$=3 000 h	λ_2=3.3 10^{-4} h^{-1}
$MTTF_3$=45 000 h	λ_3=0.22 10^{-4} h^{-1}

Fig. 18. H SENSOR reliability MC model.



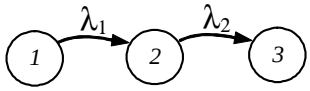
$MTTF_1$=5 000 h	λ_1=2 10^{-4} h^{-1}
$MTTF_2$=3 000 h	λ_2=3.3 10^{-4} h^{-1}
$MTTF_3$=45 000 h	λ_3=0.22 10^{-4} h^{-1}

Fig. 19. T SENSOR reliability MC model.



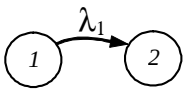
$MTTF_1$=5 000 h	λ_1=2 10^{-4} h^{-1}
$MTTF_2$=3 000 h	λ_2=3.3 10^{-4} h^{-1}
$MTTF_3$=6 000 h	λ_3=1.66 10^{-4} h^{-1}

Fig. 20. VALVE V reliability MC model.



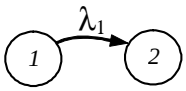
$MTTF_1$=5 000 h	λ_1=2 10^{-4} h^{-1}
$MTTF_2$=10 000 h	λ_2=1 10^{-4} h^{-1}

Fig. 21. WATER PIPE reliability MC model.



$MTTF_1$=40 000 h	λ_1=0.25 10^{-4} h^{-1}

Fig. 22. TANK reliability MC model.



MTTF1=8 000 h	λ_1=1.25 10^{-4} h^{-1}

Fig. 23. COMPUTER reliability MC model.

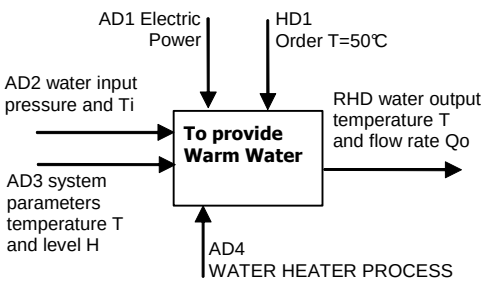


Fig. 24. SADT level A-0.

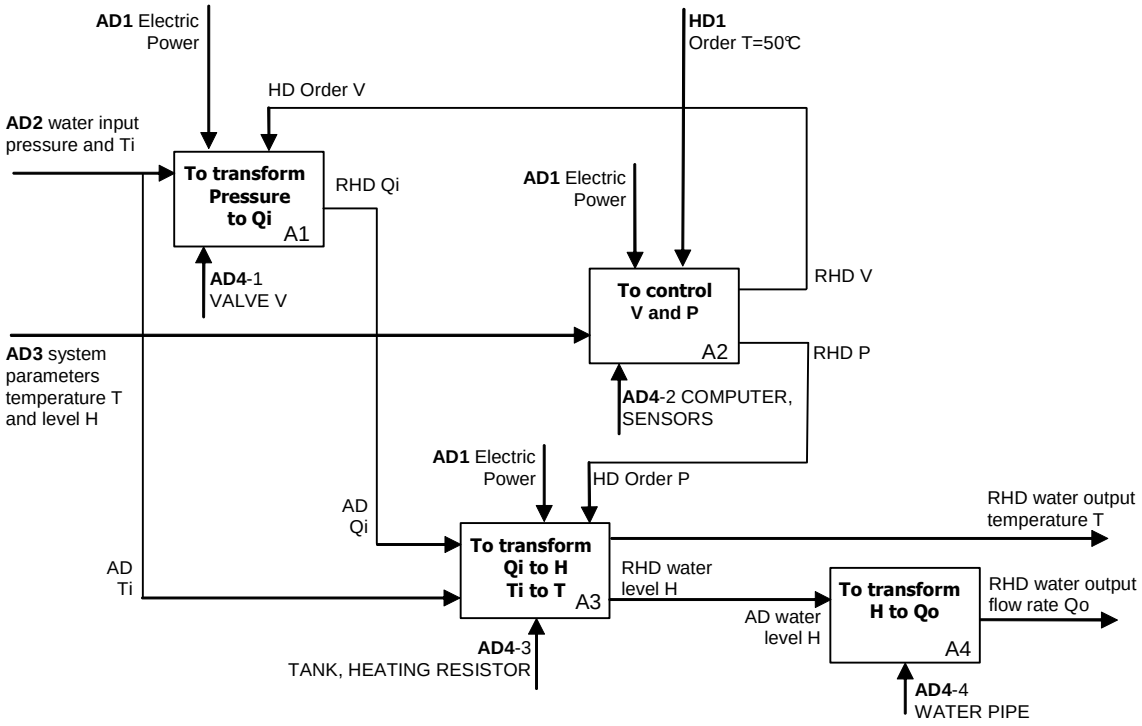


Fig. 25. SADT level A0.

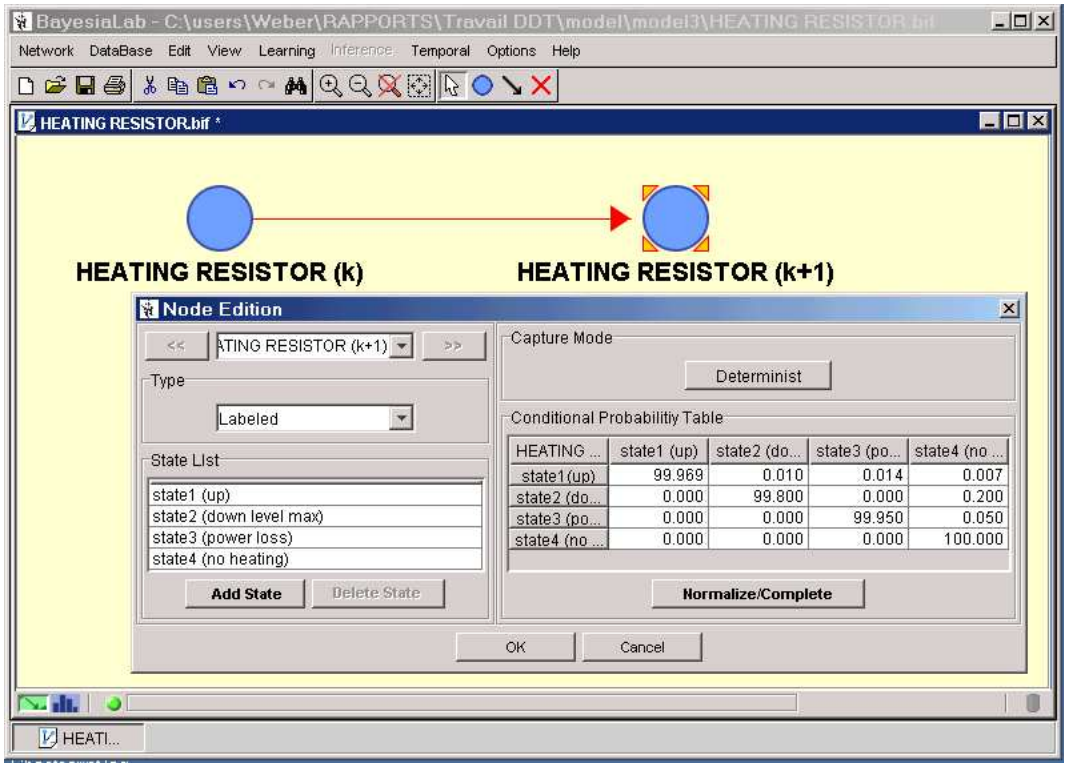


Fig. 26. Dynamic Bayesian Network model of the HEATING RESISTOR.

6.1. *SADT Analysis*

Fig. 24 presents the level A-0 of the system SADT analysis. This figure depicts the interaction between the system and the external environment through the AD, HD and RHD flows. The main functionality of the process is:

- to provide Warm Water.

The next figure presents the level A0 describing the four functions that are necessary to perform the main task of the system (Fig. 25):

- to transform Pressure into Qi (A1),
- to control V and P (A2),
- to transform Qi into H and Ti into T (A3),
- to transform H into Qo.

Fig. 27 formalises the function "to transform Qi into H and Ti into T" from the elementary functions:

- to stock water supported by the component TANK,
- to heat water supported by the component HEATING RESISTOR.

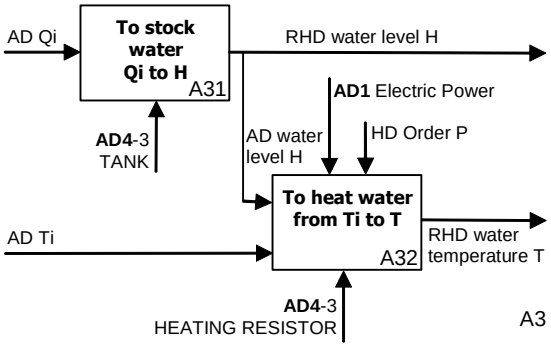


Fig. 27. SADT level A3 "to transform Qi to H and Ti to T".

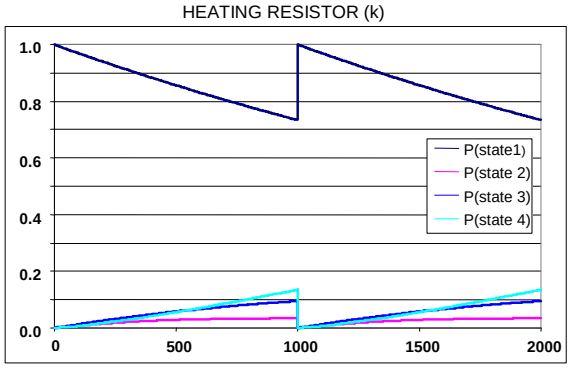


Fig. 28. States probabilities of the HEATING RESISTOR.

6.2. *DOOBN Model*

The DOOBN model is depicted in figures: 26, 29, 30, and 31.

The Dynamic Bayesian Network that models the component HEATING RESISTOR, is presented in Fig. 26. The conditional Probability Table describes the independent Markov Chain that models the reliability of this component. Inferences are realised by using the **BayesiaLab (*β version*)** software (http://www.bayesia.com) that uses an iterative procedure to compute probabilities. The states probabilities are presented in the Fig. 28 according to the current time step (k). A maintenance action is simulated when k=1000h. This maintenance action is assumed to be perfect, i.e., the component is reset in state 1 (no failure, no degradation). This event is simulated in order to illustrate its propagation through the model.

The propagation through the Object Oriented Bayesian Network model allows to take into account the dependency between the failure modes and the common cause to compute the system's reliability R(k). The Fig. 29 to 31 present OOBN models corresponding respectively to the SADT levels A3, A31 and A32 (see Fig. 27).

The elementary function "EF to heat water" is supported by the component HEATING RESISTOR (Fig. 31), and depends on the states of the flows:

- AD Electric Power,
- AD Ti,
- AD Water level H,
- HD Order P.

This elementary function is described by four states according to the FMEA (Table 3). These states correspond to the following failure modes:

- State 1: Function to heat water is correct.
- State 2: Function to heat water is incorrect, the heating level is maximum.
- State 3: Function to heat water is incorrect, the heating level is lower than the required level.
- State 4: Function to heat water is incorrect, the heating level is equal to zero.

Probabilities related to these states are depicted in Fig. 32. The maintenance action with the component HEATING RESISTOR has an impact on the "EF to heat water" states. P(state1) increases and the other probabilities decrease. Nevertheless, in spite of the assumptions of a perfect maintenance action, P(state1) is less than 1. This is due to the failure and the degradation of the other components. The ageing of the system results in a degradation of the input flows (for example: AD level H or HD Order P) of the function "to heat water". Then, the "EF to heat water" cannot be perfectly performed.

The objective of the system is to provide warm water at temperature T with flow rate Qo. The reliability of the system depends on the states of the functions: to transform Qi into H and Ti into T; to transform H into Qo.

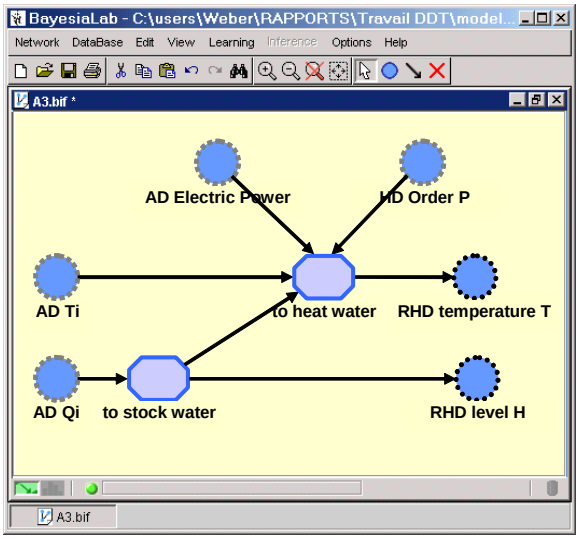


Fig. 29. OOBN model of A3 SADT level.

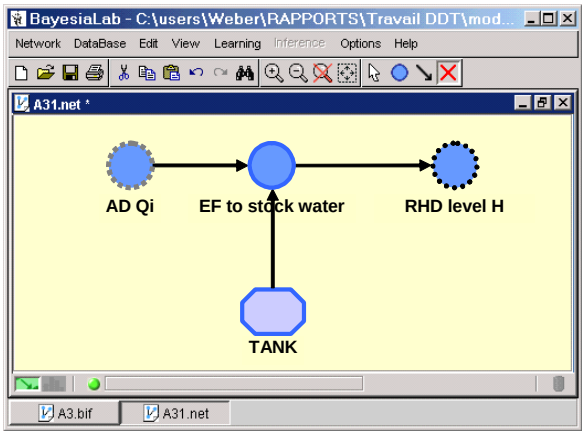


Fig. 30. OOBN model of A31 SADT level.

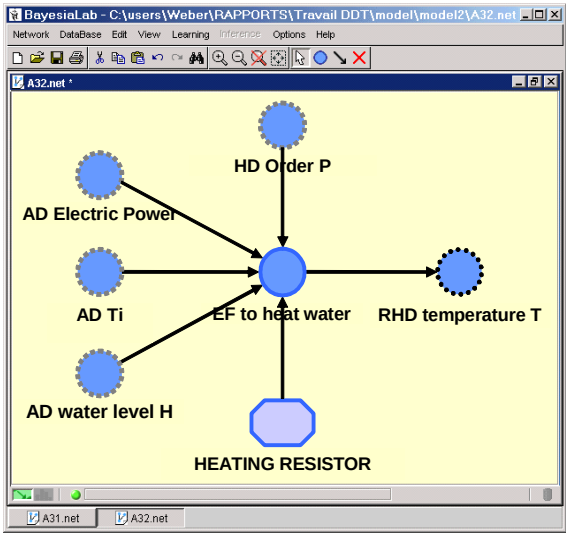


Fig. 31. OOBN model of A32 SADT level.

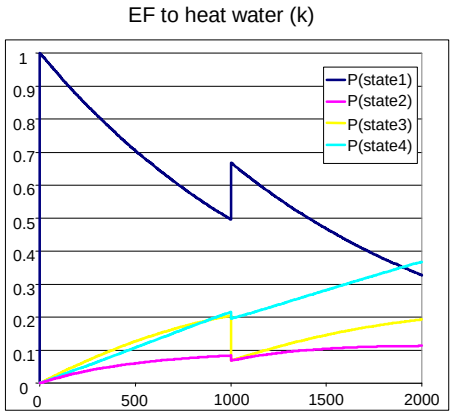


Fig. 32. States probabilities of the elementary function: to heat water.

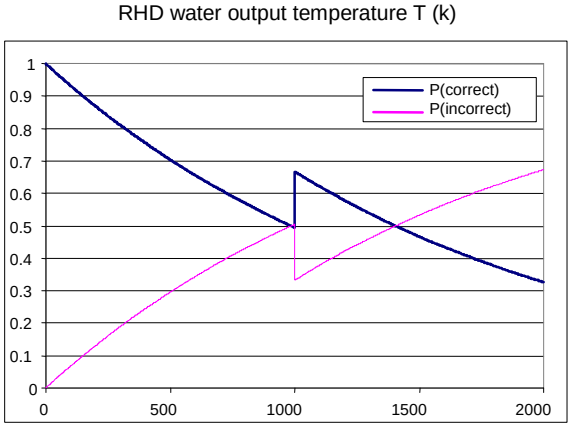


Fig. 33. States probabilities states of the flow “RHD water output temperature T”.

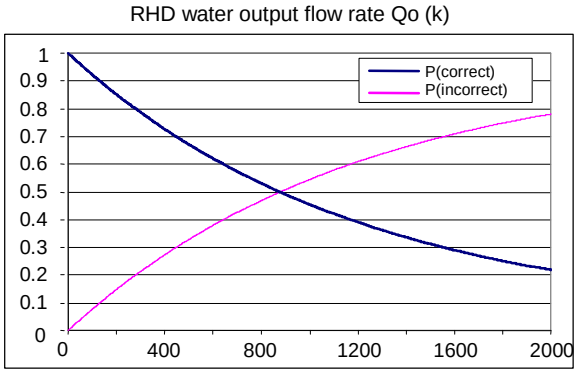


Fig. 34. States probabilities of states of the flow “RHD water output flow rate Qo”.

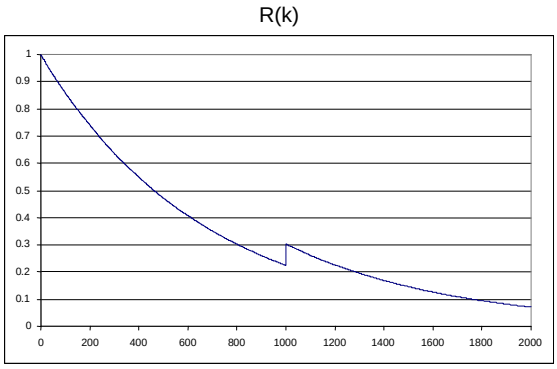


Fig. 35. Reliability of the system.

Fig. 33 presents the states of the flow "RHD output water temperature T" and Fig. 34 presents the states of the flow "RHD output water flow rate Qo". The "RHD output water temperature T" is sensitive to the maintenance event. This is not the case for the flow "RHD output water flow rate Qo" since the water level is assumed to be controlled independently from the water temperature.

Fig. 35 presents the reliability of the system and allows to observe the impact of the event corresponding to the maintenance of the HEATING RESISTOR.

7. Conclusion

The proposed method, based on the Dynamic Bayesian Networks and Object Oriented Bayesian Networks theory, easily allows designing DOOBN structures to model the temporal behaviour of the probabilities of complex system states. The correspondence between Markov Chain, Fault Tree Event Tree and DBN is presented and applied to the system reliability estimation.

Our method turns out to be a satisfying solution as far as the modelling of complex systems is concerned. Indeed, the number of states needed to model a complex system with MC increases exponentially (one state for each combination of elementary states). As the DBNs representation is based on the modelling of process entities, the obtained model is more compact and readable than the MC model. Furthermore, the dependency between several failure modes of a component and common modes is easily modelled by BN. This paper shows that DOOBNs represent a very powerful tool for decision-making in maintenance.

In future works, in order to achieve this modelling technique, we have to define to what extent the learning algorithms of BN can contribute to model the dynamics of the system's reliability, and how the parameters' behaviour can then be modelled.

References

[1] Ansell J.I. and M.J. Phillips (1994). Practical methods for reliability data analysis. Oxford University Press Inc., ISBN 0 19 853664 X, New York.

[2] Aven T., U. Jensen (1999). Stochastic Models in Reliability. Springer-Verlag, (applications of mathematics: 41, Edited by I. Karatzas and M. Yor), ISBN 0-387-98633-2, SPIN 10695247, New York.

[3] Bangso O. and P.-H. Wuillemin (2000a). Top-down construction and repetitive structures representation in Bayesian Networks. Thirteenth International Florida Artificial Intelligence Research Symposium Conference, Florida, USA.

[4] Bangso O. and P.-H. Wuillemin (2000b). Object Oriented Bayesian Networks A framework for topdown specification of Large Bayesian Networks and repetitive structures. AALBORG University Technical report, September.

[5] Boudali H. and J.B. Dugan (2005). A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering and System Safety, **87**, 337-349.

[6] Bobbio A., L. Portinale, M. Minichino and E. Ciancamerla (2001). Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety, **71**, Issue 3, March, 249-260.

[7] Bobbio A., E. Ciancamerla, G. Franceschinis, R. Gaeta, M. Minichino and L. Portinale (2003). Sequential application of heterogeneous models for the safetyanalysis of a control system: a case study. Reliability Engineering & System Safety, **81**, Issue 3, September, 269-280.

[8] Bouissou M., F. Martin and A. Ourghanlian (1999). Assessment of a Safety-Critical System Including Software: A Bayesian Belief Network for Evidence Sources. RAMS'99 Reliability and Maintainability Symposium, Washington, USA.

[9] Boutillier C., T. Dean, S. Hanks (1999). Decision-theoretic planning: structural assumptions and computational leverage. Journal of Artificial Intelligence Research, **11**, 1-94.

[10] Dhillon B.S., (1999). Design reliability: Fundamentals and applications. CRC Press LLC, ISBN 0-8493-1465-8, New York.

[11] Dutuit Y., E. Châtelet, J.-P. Signoret, P. Tomas (1997). Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases. Reliability Engineering and System Safety, **55**, 117-124.

[12] Hoyland A., M. Rausand (1994). System reliability theory: models and statistical methods. New York; Wiley.

[13] Huang C. et A. Dawiche (1996). Inference in Belief Networks : A Procedural Guide. International Journal of Approximate Reasoning, **15**, p225-263.

[14] Hung K. B., S. Venkatesk, G. West (1999). Layered dynamic probabilistic networks for spatio-temporal modelling. Intelligent Data Analysis, **3**, 339-361.

[15] Jensen F.V. (1996). An Introduction to Bayesian Networks. (UCL Press (Ed)). London.

[16] Kang C.W. and M.W. Golay (1999). A Bayesian belief network-based advisory system for operational availability focused diagnosis of complex nuclear power systems. Expert Systems with Applications, **17**, 21-32.

[17] Kjaerulff U. (1995). dHugin: a computational system for dynamic time-sliced Bayesian networks. Internationnal journal of forecasting, **11**, 89-111.

[18] Koller D et A. Pfeffer (1997). Object Oriented Bayesian Networks. In Proceeding of the Thirteenth Annual Conference on Uncertainty in Artificial Intelligence (AI-97). Rhode Island, USA, July.

[19] Nourelfath M., Dutuit Y., (2004). A combined approach to solve the redundancy optimization problem for multi-state systems under repair policies. Reliability Engineering and System Safety, **86**, 205-213.

[20] Padhraic S. (1997). Belief networks, hidden Markov models, and Markov random fields : A unifying view. Pattern Recognition Letters, **18**, 1261-1268.

[21] Santarek K. et I. Buseif (1998). Modeling and design of flexible manufacturing systems using SADT and Petri nets tools. Journal of materials Processing Technology, **76**, 212-217.

[22] Valtorta M., Y.G. Kim, J. Vomlel (2002). Soft evidential update for probabilistic multiagent systems. International journal of Approximate Reasoning, **29**, 71-106.

[23] Villemeur A (1992). Reliability, availability, maintainability and safety assessment: methods and techniques. New York: Wiley. Translatied from French Edition, 1991 by Cartier A. and Lartisien M.C.

[24] Weber P., M.C. Suhner and B. Iung (2001). System approach-based Bayesian Network to aid maintenance of manufacturing process. 6th IFAC Symposium on Cost Oriented Automation, Low Cost Automation, Berlin, Germany, October 8-9, 33-39.

[25] Weber P., M.C. Suhner (2002). An application of bayesian networks to the performance analysis of a process. In Proceedings of λμ 13, ESREL 2002 European Conference. Lyon, France.

[26] Weber P., L. Jouffe (2003). Reliability modelling with Dynamic Bayesian Networks. 5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS'03), Washington, D.C., USA, June 9-11.

[27] Weber P., P. Munteanu, L. Jouffe (2004). Dynamic Bayesian Networks modelling the dependability of systems with degradations and exogenous constraints. 11th IFAC Symposium on Information Control Problems in Manufacturing (INCOM'04), Salvador-Bahia, Brazil, April 5-7.

[28] Welch R. and T. Thelen (2000). Dynamic reliability analysis in an operational context: the Bayesian network perspective. In Dynamic reliability: future directions. Edited by: C. Smidts, J. Devooght and P.E. Labeau, ISBN 0 9652669 3 1, Maryland, USA.