Communications reliability analysis in networked embedded systems

Damien Aza-Vallina, Bruno Denis, Jean-Marc Faure

Communications reliability analysis in networked embedded systems

Damien Aza-Vallina & Bruno Denis & Jean-Marc Faure
LURPA, ENS de Cachan, Cachan, France

ABSTRACT: This paper presents a novel method to obtain an analytical expression of the reliability of a data transmission between two terminals of a networked system where components may fail in different manners, e.g. silent or babbling, and some failures may propagate to the adjacent components. This method is exemplified on a typical architecture for critical networked systems; comparison to a common approach which does not consider multiple failure modes and propagating failures shows the benefits of this contribution.

1 INTRODUCTION

Communications between the components of control systems (controllers, sensors, actuators) have been only implemented in the past by point-to-point connections. These solutions are gradually replaced, even in critical systems, by communication networks, like CAN (Controller Area Network), FlexRay, but also Ethernet-based technologies, such as Ethernet/IP, Ethernet Powerlink, AFDX (Avionics Full DupleX) in aeronautics, for cost reduction reasons.

Parallel to these industrial changes, numerous research works have been performed to facilitate the development and operation of networked embedded systems. The results of these works are methods to assess time performances (Marsal 2007)(Georges, Krommenacker, Divoux, & Rondeau 2006)(Bauer, Scharbarg, & Fraboul 2010) or reliability (Ghasemzadeh, Meinel, & Khanji 2008) of these systems. This paper focuses only on this latter feature, which is a fundamental dependability attribute when the network is embedded in a critical system.

Reliability analysis of a networked system is based on a topological model of interconnected components which are terminals, data senders and/or receivers like controllers or smart sensors/actuators, or data transmission devices, such as hubs and switches. A common assumption is that there is only one failure mode for each component (Ball 1976)(Rosenthal 1977); hence, the behavior of a component can be described by a continuous, often homogeneous, Markov chain that comprises only two states: faultless and faulty. The reliability of a data transmission between two terminals is defined as the probability that there exists at least one path between these two terminals which includes only faultless components; it can be computed from the analysis of the topological model of the network and the knowledge of the behavioral models of the components.

The common two-states behavioral model (binary model) suits only hardware components, however. More complex behavioral models, with several faulty states, must be introduced for the components which contain hardware and software (including software implementation) because they may fail in different manners, e.g. fail-silent or -babbling. A good classification of failure modes of these components can be found in (Papadopoulos, Tran, Faure, & Grante 2006); according to this reference, six failure modes may occur, which can be ordered in three groups:

- data transmission failures: transmission omission or commission,
- data values failures: the value of the transmitted data is higher or lower than the real value,
- transmission time failures: the transmission happens too early or too late.

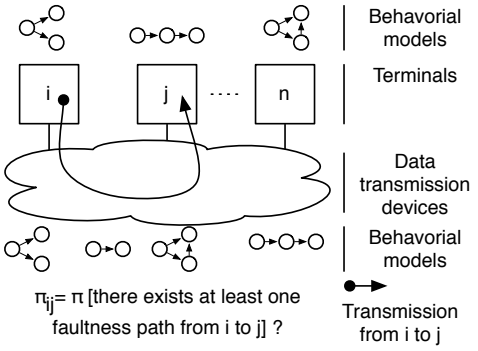


Figure 1: Aim of this work

Only failures of the first group are considered in this study. Moreover, some transmissions commissions, e.g. fail-babbling, may propagate, i.e. their

occurrence prevents other components from communicating, even if they are faultless. Consequently, a path is faultless not only if all components which belong to this path are non-faulty but, furthermore, if no propagating failure that impacts one of these components has occurred.

On the basis of these two observations, this paper proposes a novel method to obtain the reliability of a data transmission between two terminals of a networked system (Fig. 1). This method is appropriate to systems which include components whose behavioral models may comprise several faulty states and failure modes may propagate. The models on which this contribution relies are presented in the next section, while section 3 details the proposed method. Application to a typical critical networked system, in section 4, permits to show the interest of this proposal.

2 PROBLEM MODELING

The model of the network topology which was selected is first presented in this section. Then, a generic model of the behavior of a network component is proposed.

2.1 *Network topology modeling*

A communication network can be modeled as a non-directed graph $G = (\mathcal{N}, E)$ where:

- $\mathcal{N}$ is a set of nodes, a node representing a network component,
- E is a set of non-directed edges between couples of elements of $\mathcal{N}$. An edge represents a physical link between two nodes.

In this graph, the set of paths which permit to ensure data transmission between two nodes i and j will be noted P_{ij}; it may contain one or several paths. An element of P_{ij} will be noted P_{ij}^k. Two nodes are adjacent if there exists at least one edge between these nodes.

2.2 *Component behavior modeling*

As mentioned in the introduction, the aim of the paper is to propose a reliability assessment method that is appropriate to networks where components may fail in different manners, some failure modes being able to propagate to the adjacent components. Hence, the common two-states (faultless or faulty) behavioral component model is no more suitable.

The behavior of a network component will be then described by a continuous Markov chain MC_i ((Cassandras & Lafortune 2006)) :

$$MC_i =< X_i, p_i, \pi_i(0) > \quad (1)$$

where:

- X_i is the set of states of the Markov chain,
- p_i is the transition matrix,
- $\pi_i(0)$ is a vector which contains the probabilities that the different states be active at the initial date.

This chain may include more than two states according to the number of failure modes that are selected. These states can be however gathered in three sub-sets which define a partition on X_i:

- X_i^0 sub-set of correct operation states,
- X_i^P sub-set of propagating failure states. A component failure is termed "propagating" when its occurrence entails that every adjacent component becomes unable to ensure any communication, even if it is itself failure-free.
- X_i^F sub-set of non-propagating failure states. A component failure is termed "non-propagating" when its occurrence does not impact the behavior of adjacent components.

with $X_i^0 \cap X_i^F = X_i^0 \cap X_i^P = X_i^F \cap X_i^P = \emptyset$ and $X_i^0 \cup X_i^F \cup X_i^P = X_i$

The probability that the active state at date t is the state α will be noted $\pi_i^\alpha(t)$; the probability that the active state at date t belongs to one of the three sub-sets X_i^0, X_i^F , X_i^P will be noted respectively $\pi_i^{X_i^0}(t)$, $\pi_i^{X_i^F}(t)$,$\pi_i^{X_i^P}(t)$.

In the sequel of this paper, some limitations are introduced in this modeling:

- Fault occurrences are independent events.
- The number of states of correct operation is equal to one ($card(X_i^0) = 1$).
- The components are not repairable; there is no transition starting from a failure state to the correct operation state.
- The failures are persistent; there is no transition between two failure states.

The third assumption has been introduced because no reparation is allowed during a mission of embedded system. The fourth assumption comes from industrial design rules that specify that a component becomes faulty as soon as a fault occurs, whatever the duration of this fault.

With these assumptions, the behavior of a component can be described by the model of Figure 2(a), if all failure states are explicitly depicted on Figure 2(b) if only a description by the three states sub-sets which have been previously defined is selected. It matters to

note that these models do not contain degraded operation states; a component is either in a correct operation state or in a failure state. In the latter case, the failure may impact the ability of every adjacent component to transmit data (propagating failure) or not (non-propagating failure).

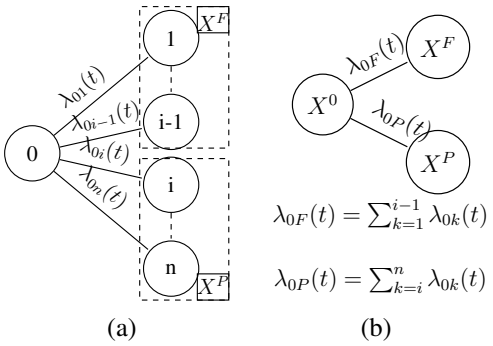


Figure 2: Component behavior modeling (λ_{XY} : failure rate)

3 TRANSMISSION RELIABILITY EVALUATION

From the models given in the previous section, a method to evaluate the reliability of a transmission between two terminal nodes i and j, probability that there exists at least one path which permits to ensure data transmission between these two nodes, has been developed. The aim of this method is to provide an analytic expression of this reliability. It is also aimed at avoiding components models composition so as to prevent from the classical state space explosion issue which occurs easily when composing discrete state space models.

This method comprises three steps which are performed sequentially:

A Research, for each minimum-length path between i to j, of the components states combinations such as the transmission through this path is possible.

B Determination, for the whole set of minimum-length paths between i to j, of the components states combinations such as the transmission is possible.

C Determination of the analytical expression of the transmission reliability.

These three steps will be detailed in the following sub-sections and illustrated on an example issued from (Barranco, Almeida, & Proenza 2005) (Fig. 3(a)). This communication network is composed of three CAN terminals which are interconnected by two stars (redundant medium); each star is implemented by a hub. The topological model of this network is given Figure 3(b); this graph comprises 5 nodes ($\mathcal{N} = \{a, b, c, d, e\}$), a, b, c for the terminals and d, e for the hubs. In what follows, focus is put on the data transmission between the terminals a and b for illustration purposes.

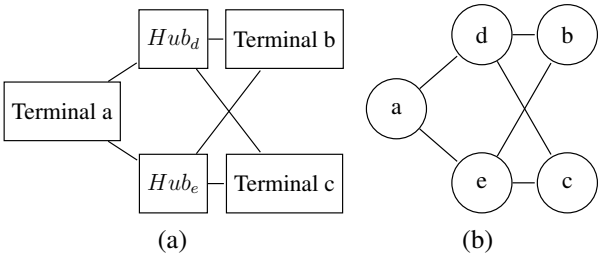


Figure 3: A five components network (a) and its topological model (b)

3.1 *Research of the components states combinations for one minimum-length path*

A transmission by the path[1] P_{ij}^k between the nodes i and j is possible if:

- every component which is represented in the topological model by a node which belongs to the path P_{ij}^k is in the correct operation state;
- every component which is represented in the topological model by a node which is adjacent to a node which belongs to the path P_{ij}^k is in the correct operation state or in a non-propagating failure state;
- all other components are in any state.

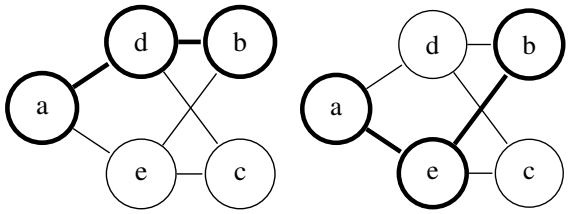
If N_{ij}^k denotes the set of nodes which belong to the path P_{ij}^k and PN_{ij}^k the set of nodes which are adjacent to a node of the path P_{ij}^k , the set of allowed states, states that allow data be transmitted through the path P_{ij}^k , for a component represented by a node l ($l \in \mathcal{N}$), is $X_l^{P_{ij}^k}$, with:

$$X_l^{P_{ij}^k} = \begin{cases} X_l^0 & if\ l \in N_{ij}^k \\ X_l^0 \cup X_l^F & if\ l \in PN_{ij}^k \\ X_l & else \end{cases} \quad (2)$$

For the example, there are two minimum-length paths to transmit data between the nodes a et b, noted P_{ab}^1 and P_{ab}^2 (Fig. 4). Then, the allowed states of the components, defined by (2), are given in Table 1.

The components a and b must be in their correct operation state (X_a^0 and X_b^0), whatever the path. On the opposite, the component c does not belong to any path but is always adjacent to a node belonging to a path (adjacent to d for the P_{ab}^1 and to e for P_{ab}^2); it must

[1]For brevity reasons, the term "path" will mean "minimum-length path" in the rest of this paper.



(a) P_{ab}^1 (b) P_{ab}^2

Figure 4: The two paths to transmit data between a and b

Component	Path	
	P_{ab}^1	P_{ab}^2
a	X_a^0	X_a^0
b	X_b^0	X_b^0
c	$X_c^0 \cup X_c^F$	$X_c^0 \cup X_c^F$
d	X_d^0	$X_d^0 \cup X_d^F$
e	$X_e^0 \cup X_e^F$	X_e^0

Table 1: Set of allowed states for each component and each path

not be in a propagating failure state. $X_c^{P_{ab}^1} \notin X_c^P$ i.e. $X_c^{P_{ab}^1} \in X_c - X_c^P = X_c^0 \cup X_c^F$.

The active state of the network at a given date is the combination of the active states of the components at this date; this combination comprises n terms, with $n = card(\mathcal{N})$. The set of the allowed combinations for a transmission through a path is then obtained from the sets of the allowed states of the components in the following way:

$$C_{ij}^{P_{ij}^k} = \prod_{l \in \mathcal{N}} X_l^{P_{ij}^k} \tag{3}$$

For the two transmission paths between a and b, these sets are:

$$C_{ab}^{P_{ab}^1} = X_a^0 \times X_b^0 \times (X_c^0 \cup X_c^F) \times X_d^0 \times (X_e^0 \cup X_e^F) \tag{4}$$

$$C_{ab}^{P_{ab}^2} = X_a^0 \times X_b^0 \times (X_c^0 \cup X_c^F) \times (X_d^0 \cup X_d^F) \times X_e^0 \tag{5}$$

It can be noted that each set contains only four combinations.

3.2 *Determination of the components states combinations for all paths*

The set of allowed states of a component depends on the studied path; a component may for instance belong to a given path P_{ij}^m and be adjacent to a component of path P_{ij}^n, where P_{ij}^m and P_{ij}^n are two different paths by which data can be transmitted from/to i to/from j. The set of the allowed components states combinations for all paths, noted C_{ij}, is then obtained by union of the sets of allowed combinations for each path:

$$C_{ij} = \bigcup_{P_{ij}^k \in P_{ij}} C_{ij}^{P_{ij}^k} \tag{6}$$

For the example, this set is obtained from (4) and (5). Then it comes:

$$C_{ab} = X_a^0 \times X_b^0 \times (X_c^0 \cup X_c^F) \times \left[(X_d^0 \times X_e^0) \cup (X_d^F \times X_e^0) \cup (X_d^0 \times X_e^F)\right] \tag{7}$$

It must be underlined that this set includes only 6 states combinations among the 243 (3^5) of the Markov chain which describes the whole behavior of the network. The steps A and B, which are based on analysis of the network topology and operations on sets, have avoided the construction of this model which is non-trivial-sized even for a simple example.

3.3 *Analytical expression of the reliability of the transmission*

Let c be a components states combination and α_l^c the state of component l in this combination. The probability that the network be in this combination at date t is noted $\pi^c(t)$. If the probability that the component be in a state α_l^c at date t is noted $\pi_l^{\alpha_l^c}(t)$, then $\pi^c(t)$ is computed as follows:

$$\pi^c(t) = \prod_{l \in \mathcal{N}} \pi_l^{\alpha_l^c}(t) \tag{8}$$

because faults occurrences are independent events.

Therefore, the reliability of the transmission is the sum of the probabilities of the allowed components states combinations:

$$\pi_{ij}(t) = \sum_{c \in C_{ij}} \pi^c(t) = \sum_{c \in C_{ij}} \prod_{l \in \mathcal{N}} \pi_l^{\alpha_l^c}(t) \tag{9}$$

For the example of Figure 3, the reliability of the transmission between the nodes a and b is:

$$\begin{aligned}\pi_{ab} = &\pi_a^{X_a^0}.\pi_b^{X_b^0}.\pi_c^{X_c^0}.\pi_d^{X_d^0}.\pi_e^{X_e^0} + \pi_a^{X_a^0}.\pi_b^{X_b^0}.\pi_c^{X_c^0}.\pi_d^{X_d^F}.\pi_e^{X_e^0} \\ &+\pi_a^{X_a^0}.\pi_b^{X_b^0}.\pi_c^{X_c^0}.\pi_d^{X_d^0}.\pi_e^{X_e^F} + \pi_a^{X_a^0}.\pi_b^{X_b^0}.\pi_c^{X_c^F}.\pi_d^{X_d^0}.\pi_e^{X_e^0} \\ &+\pi_a^{X_a^0}.\pi_b^{X_b^0}.\pi_c^{X_c^F}.\pi_d^{X_d^F}.\pi_e^{X_e^0} + \pi_a^{X_a^0}.\pi_b^{X_b^0}.\pi_c^{X_c^F}.\pi_d^{X_d^0}.\pi_e^{X_e^F}\end{aligned} \tag{10}$$

It is then possible to factorize this expression:

$$\pi_{ab} = \pi_a^{X_a^0}.\pi_b^{X_b^0}.(\pi_c^{X_c^0} + \pi_c^{X_c^F}).$$

$$\left[(\pi_d^{X_d^0}.\pi_e^{X_e^0}) + (\pi_d^{X_d^F}.\pi_e^{X_e^0}) + (\pi_d^{X_d^0}.\pi_e^{X_e^F})\right] \quad (11)$$

This new form of the reliability is structured in a similar fashion to expression (7).

This method will be applied in the next section to a network where terminal components communicate by using a redundant bus. This case study will permit to show the interest of the proposed modeling of the components behavior compared to a common modeling where every component owns only one non-propagating failure mode.

4 APPLICATION

A bus architecture can be used in a critical system only if medium redundancy is ensured. The method detailed in section 3 will be then illustrated on the generic example of Figure 5 where n terminals are connected by two buses B1 and B2 which will be assumed identical. Moreover, it will be admitted that there is only one failure mode, non-propagating failure, for a bus and two modes, propagating failure and non-propagating failure, for a terminal. Once the behavioral models of components given, the three steps of the method are developed. Last, the results obtained are discussed and compared to those which would have been yielded by a common modeling approach.

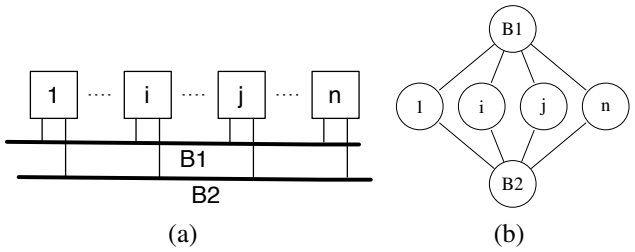


Figure 5: Redundant bus (a) and model of its topology (b)

4.1 *Components behavior modeling*

With the above assumptions on the number of failure modes, two kinds of behavioral models are to be used.

4.1.1 *Component with one failure mode*

In this case, the component behavior is described by a Markov chain which comprises two states (Fig. 6(a)): a state to model the correct operation, noted x^{OK}, and a state to model the failure, noted x^F . Then it comes: $X_l = \{x_l^{OK}, x_l^F\}, X_l^0 = \{x_l^{OK}\}, X_l^F = \{x_l^F\}$ and $X_l^P = \emptyset$. It will be assumed that this Markov chain is homogeneous; the failure rate λ_l is constant and the probabilities that a given state is the active state at date t are:

$$\begin{cases} \pi_l^{X_l^0}(t) = e^{-\lambda_l.t} \\ \pi_l^{X_l^F}(t) = 1 - e^{-\lambda_l.t} \end{cases} \quad (12)$$

4.1.2 *Component with more than one failure mode*

The following two failure modes are selected for this study:

- transmission omission, what means that a component does not communicate though it should. This failure mode does not propagate to the adjacent components and will be represented by a state x_l^F.
- transmission commission, what means, on the opposite, that a component communicates though it should not communicate; as failures are assumed persistent, this unexpected communication is continuously maintained and monopolizes the medium. This failure mode propagates to the adjacent components and will be represented by a state x_l^P.

The behavior of the component is then described by a Markov chain which comprises three states (Fig. 6(b)) such as:
$X_l = \{x_l^{OK}, x_k^F, x_l^P\}$, $X_l^0 = \{x_l^{OK}\}$, $X_l^F = \{x_l^F\}$ and $X_l^P = \{x_l^P\}$

If this Markov chain is homogeneous, the failure rates λ_l^f and λ_l^p are constant and the probabilities that the different states be active at date t are:

$$\begin{cases} \pi_l^{X_l^0}(t) = e^{-(\lambda_l^a + \lambda_l^p).t} \\ \pi_l^{X_l^F}(t) = \frac{\lambda_l^f}{\lambda_l^p + \lambda_l^f}.(1 - e^{-(\lambda_l^f + \lambda_l^p).t}) \\ \pi_l^{X_l^P}(t) = \frac{\lambda_l^p}{\lambda_l^p + \lambda_l^f}.(1 - e^{-(\lambda_l^f + \lambda_l^p).t}) \end{cases} \quad (13)$$

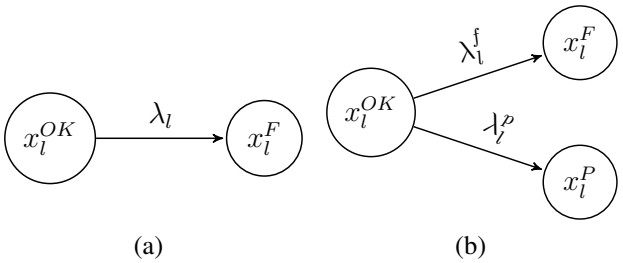


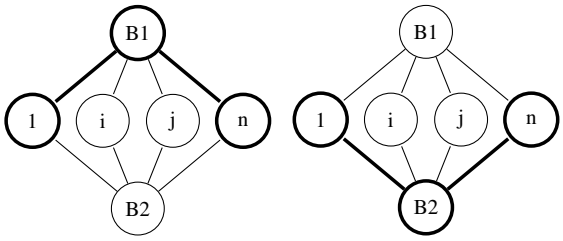
Figure 6: Model of the behavior of a component with one (a) and two (b) failure mode(s)

4.2 *Transmission reliability evaluation*

This analysis will be carried out on the example of the transmission between the terminals 1 and n; it can be easily transposed to any other couple of terminals.

4.2.1 *Research of the components states combinations for one path*

Two paths, noted P^1_{1n} et P^2_{1n}, permit data be transmitted between the nodes 1 and n (Fig. 7).



(a) P^1_{1n} (b) P^2_{1n}

Figure 7: The two paths to transmit data between 1 and n

For each path and for each component, it is possible to determine the sets of allowed states from (2); the result of this analysis is given in Table 2.

Component	Path	
	P^1_{1n}	P^2_{1n}
1	X^0_1	X^0_1
$l \in \{2...n-1\}$	$X^0_l \cup X^F_l$	$X^0_l \cup X^F_l$
n	X^0_n	X^0_n
B1	X^0_{B1}	$X^0_{B1} \cup X^F_{B1}$
B2	$X^0_{B2} \cup X^F_{B2}$	X^0_{B2}

Table 2: Set of the allowed states for a component according to the selected path

Both nodes 1 and n belong to the path, whatever it could be; hence, they must be in the correct operation state. At the opposite, the nodes 2 to $n-1$ do not belong to any path but are always adjacent to the bus and therefore must not be in a propagating failure mode; the corresponding unexpected communication would prevent the nodes 1 and n from accessing the bus in this case. Then, the expressions of the sets C^1_{1n} and C^2_{1n} are:

$$C^{P^1_{1n}}_{1n} = X^0_1 \times \left[\prod_{l=2}^{n-1}(X^0_l \cup X^F_l)\right] \times X^0_n \times X^0_{B1} \times (X^0_{B2} \cup X^F_{B2}) \quad (14)$$

$$C^{P^2_{1n}}_{1n} = X^0_1 \times \left[\prod_{l=2}^{n-1}(X^0_l \cup X^F_l)\right] \times X^0_n \times (X^0_{B1} \cup X^F_{B1}) \times X^0_{B2} \quad (15)$$

For each set, there is only one allowed state, the correct operation state, for three components (1, n and the bus which belongs to the studied path) and two allowed states for $n-1$ components ($n-2$ terminals and the other bus). The cardinality of these sets is then: $card(C^{P^1_{1n}}_{1n}) = card(C^{P^2_{1n}}_{1n}) = 1^3.2^{n-1} = 2^{n-1}$.

4.2.2 *Determination of the components states combinations for all paths*

The set C_{1n} of the allowed states combinations for the transmission is the union of the two sets $C^{P^1_{1n}}_{1n}$ and $C^{P^2_{1n}}_{1n}$, i.e.

$$C_{1n} = X^0_1 \times \left[\prod_{l=2}^{n-1}(X^0_l \cup X^F_l)\right] \times X^0_n \times \left[(X^0_{B1} \times X^0_{B2}) \cup (X^0_{B1} \times X^F_{B2}) \cup (X^F_{B1} \times X^0_{B2})\right] \quad (16)$$

This set contains 3.2^{n-2} combinations while $2^2.3^n$ combinations are possible with the previously defined behavioral models. For a network with 10 terminals for instance, there are 768 allowed combinations while the Markov chain which models the whole behavior of the network comprises 236,196 states, i.e. around three hundred times more.

4.2.3 *Analytical expression of the reliability of the transmission*

Once all allowed combinations determined, the reliability of the considered transmission in function of the probabilities of the states can be defined as follows:

$$\pi_{1n}(t) = \pi_1^{X^0_1}(t).\left[\prod_{l=2}^{n-1}(\pi_l^{X^0_l}(t) + \pi_l^{X^F_l}(t))\right].\pi_n^{X^0_n}(t) . \left[(\pi_{B1}^{X^0_{B1}}(t).\pi_{B2}^{X^0_{B2}}(t)) + (\pi_{B1}^{X^0_{B1}}(t).\pi_{B2}^{X^F_{B2}}(t)) + (\pi_{B2}^{X^F_{B1}}(t).\pi_{B2}^{X^0_{B2}}(t))\right] \quad (17)$$

With the behavioral models presented in 4.1 and in particular the expressions (12) and (13), the analytical expression of the considered reliability is:

$$\pi_{1n}(t) = e^{-(\lambda^f_1+\lambda^p_1).t}.\left[\prod_{l=2}^{n-1}\left(\frac{\lambda^f_l + \lambda^p_l.e^{-(\lambda^f_l+\lambda^p_l).t}}{\lambda^f_l + \lambda^p_l}\right)\right] .e^{-(\lambda^f_n+\lambda^p_n).t}.\left[(e^{-\lambda_{B1}.t}.e^{-\lambda_{B2}.t}) + (e^{-\lambda_{B1}.t}.(1-e^{-\lambda_{B2}.t})) + ((1-e^{-\lambda_{B1}.t}).e^{-\lambda_{B2}.t})\right] \quad (18)$$

It matters to clearly underline that this expression depends on the number of terminals which are connected to the bus. This novel result would not have

been obtained by using a binary model for every component.

4.2.4 *Numerical application*

Assuming the following failure rates:

- $\lambda_{B1,B2} = 10^{-7}h^{-1}$
- $\lambda_l^f = 8.10^{-8}h^{-1}$ et $\lambda_l^p = 2.10^{-8}h^{-1}$

the numerical application of (18), for three values of n: 2, 5 et 10, permits to represent the evolution of the reliability in function of time (Fig. 8).

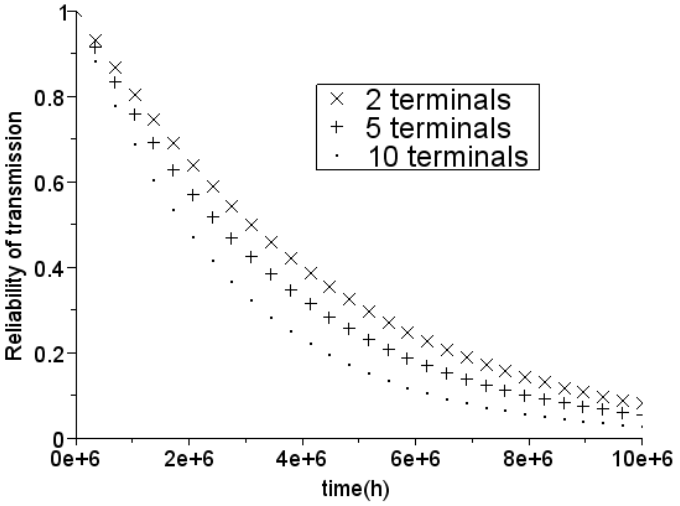


Figure 8: Reliability of the transmission between two terminals in function of time and the number of terminals connected to the bus(2,5,10).

This figure shows clearly that the reliability of the transmission depends on the number of terminals, as pointed out by equation (18). Increasing the number of terminals leads to lessen reliability because new propagating failures are thus introduced.

4.2.5 *Discussion*

Expression (17) must be now compared to those that yield the analyses:

- of an architecture without bus redundancy but based on the same behavioral models of components;
- of an architecture with bus redundancy but using for every component a two-states (correct operation, transmission omission) behavioral model.

Comparison with the reliability of an architecture without bus redundancy For an architecture with only one bus, there is only one path between 1 and n. From equation (13), it is then possible to define the set of the allowed states for the transmission (here the path):

$$C_{1n}^{1bus} = X_1^0 \times \left[\prod_{l=2}^{n-1}(X_l^0 \cup X_l^F)\right] \times X_n^0 \times X_{B1}^0 \quad (19)$$

Then, the analytical expression of the reliability is:

$$\pi_{1n}^{1bus}(t) = e^{-(\lambda_1^f+\lambda_1^p).t}.\left[\prod_{l=2}^{n-1}\left(\frac{\lambda_l^f+\lambda_l^p.e^{-(\lambda_l^f+\lambda_l^p).t}}{\lambda_l^f+\lambda_l^p}\right)\right]$$
$$.e^{-(\lambda_1^f+\lambda_n^p).t}.e^{-\lambda_{B1}.t} \quad (20)$$

Hence:

$$\pi_{1n}(t) = \pi_{1n}^{1bus}(t)\left[1+e^{-\lambda_{B2}.t}(\frac{1}{e^{-\lambda_{B1}.t}}-1)\right] \quad (21)$$

On the assumption that $\lambda_{B1} = \lambda_{B2}$ then $\pi_{1n}(t) = \pi_{1n}^{1bus}(t).(2-e^{-\lambda_{B2}.t})$. As it might be expected, medium redundancy improves reliability by a factor $(2-e^{-\lambda_{B2}.t})$.

Comparison with the reliability of an architecture with bus redundancy but obtained from two-states behavioral models of components To obtain comparable results, the behavioral models of all components are here such as:

- The overall failure rate of the component is unchanged for the terminals $\lambda_l = \lambda_l^p + \lambda_l^a$
- The failure is non-propagating for every component.

Then, the set of allowed states is easily obtained from (15) and is:

$$C_{1n}^{1mode} = X_1^0 \times \left[\prod_{l=2}^{n-1} X_l\right] \times X_n^0$$
$$\times\left[(X_{B1}^0 \times X_{B2}^0) \cup (X_{B1}^0 \times X_{B2}^F) \cup (X_{B1}^F \times X_{B2}^0)\right] \quad (22)$$

This set contains 3.2^{n-2} combinations while 2^{n+2} combinations are possible with the hereabove defined behavioral models.

And the analytical expression of the reliability is:

$$\pi_{1n}^{1mode}(t) = e^{-\lambda_1.t}.e^{-(\lambda_1^f+\lambda_n^p).t}.\left[(e^{-\lambda_{B1}.t}.e^{-\lambda_{B2}.t})\right.$$
$$\left.+(e^{-\lambda_{B1}.t}.(1-e^{-\lambda_{B2}.t})) + ((1-e^{-\lambda_{B1}.t}).e^{-\lambda_{B2}.t})\right] \quad (23)$$

Hence:

$$\pi_{1n}(t) = \pi_{1n}^{1mode}(t).\left[\prod_{l=2}^{n-1}\left(\frac{\lambda_l^f + \lambda_l^p.e^{-(\lambda_l^f+\lambda_l^p).t}}{\lambda_l^f + \lambda_l^p}\right)\right] \quad (24)$$

Expressions (23) and (24) show that:

- the expression obtained with the common two-states terminal model (expression (23)) does not depend on the number of terminals;
- as the multiplier in (24) is smaller than or equal to 1, the reliability obtained with the three-states terminal model is always lower than the other one. The reliability obtained with the novel component model which has been proposed (expression (17)) is then more pessimistic but more realistic; it is in particular impacted by the number of terminals, the larger this number, the smaller its value at a given date. This knowledge is quite useful when designing networks for critical systems.

5 CONCLUSION AND PERSPECTIVES

A method to evaluate the reliability of a data transmission between two terminals of a communication network has been proposed in this paper. The novelty of this contribution is that several failure modes of components, e.g. fail-silent and fail-babbling, as well as failures propagation are considered; hence some failures of a component may entail that every adjacent component becomes unable to ensure any communication, even if it is itself failure-free.

This method provides an analytical expression of the reliability; this permits the analysis of the evolution of this dependability attribute over time, for maintenance planning purposes for instance. This expression is obtained from the knowledge of the allowed components states combinations which are themselves derived from the analysis of the network topology, and not by composition of Markov chains to avoid (or limit) combinatory explosion.

Several outlooks arise from these results. First, more detailed behavioral models of components are to be developed, by distinguishing the states where the component is active, used for data transmission, from those where it is idle, waiting for a request to be used. Then it will be possible to consider the application of these proposals to design of communication networks for critical systems.

REFERENCES

Ball, M. O. (1976). Computing network reliability. *Operations Research 27*(4), 823–838.

Barranco, M., L. Almeida, & J. Proenza (2005). ReCANcentrate: a replicated star topology for CAN networks. In *Emerging Technologies and Factory Automation, 2005. ETFA 2005.* 10^{th} *IEEE Conference on*, Volume 2, pp. 8 pp. 468–476.

Bauer, H., J.-L. Scharbarg, & C. Fraboul (2010). Improving the worst-case delay analysis of an AFDX network using an optimized trajectory approach. *IEEE Transactions on Industrial Informatics 6*(4), 521–533.

Cassandras, C. G. & S. Lafortune (2006). *Introduction to Discrete Event Systems*. Secaucus, NJ, USA: Springer-Verlag New York, Inc.

Georges, J.-P., N. Krommenacker, T. Divoux, & E. Rondeau (2006). A design process of switched Ethernet architectures according to real-time application constraints. *Engineering Applications of Artificial Intelligence 19*(3), 335–344.

Ghasemzadeh, M., C. Meinel, & S. Khanji (2008). K-terminal network reliability evaluation using Binary Decision Diagram. In 3^{rd} *International Conference on Information and Communication Technologies: From Theory to Applications (ICTTA)*, pp. 1–5.

Marsal, G. (2007). *Evaluation of Time Performances of Ethernet-based Automation Systems by Simulation of High-level Petri Nets*. Shaker Verlag GmbH, Germany.

Papadopoulos, Y., A. Tran, J.-M. Faure, & C. Grante (2006). Component Failure Behaviour: Patterns and Reuse in Automated System Safety Analysis. In *Proceedings of SAE 2006*, Detroit, USA, pp. paper n° 06AE–287.

Rosenthal, A. (1977). Computing the reliability of complex networks. *SIAM Journal on Applied Mathematics 32*(2), pp. 384–393.