AN ANALYTIC EXPRESSION OF THE RELIABILITY OF TRANSMISSIONS IN FIELDBUSES WITH PROPAGATED FAILURES

Damien Aza-Vallina, Jean-Marc Faure

AN ANALYTIC EXPRESSION OF THE RELIABILITY OF TRANSMISSIONS IN FIELDBUSES WITH PROPAGATED FAILURES

Damien AZA-VALLINA * **Jean-Marc FAURE** *

* *LURPA, ENS Cachan, Cachan, France (e-mail: aza-vallina,faure@lurpa.ens-cachan.fr).*

Abstract: This paper shows first that the behaviour of a fieldbus whose terminals can be represented by multi-state components with propagated failures may be described by a set of connected mode automata; the input and output flows of these automata represent either data exchanges or failure propagations. A method to obtain an analytic expression of the reliability of a transmission between two terminals from this model is then proposed.

Keywords: Reliability evaluation, Multi-state component, Failure modes, Mode automata, Communication networks

1. INTRODUCTION

Fieldbuses have replaced the traditional point-to-point connections between the components of the embedded distributed measurement and control systems that perform non-critical functions in many application domains; replacing these connections by fieldbuses reduces wiring cost and weight, what is surely advantageous. However, when critical functions are considered, the reliability of the data transmission between two components is to be thoroughly assessed so that it would be possible to compare the reliability of this transmission with the new technological solution to that obtained with a traditional, point-to-point, solution; cost or weight reduction must not lessen transmission reliability indeed. As detailed in Cauffriez et al. (2004) many kinds of failures may occur in a fieldbus. This paper focuses only on the failures in the physical layer; these failures are the first ones to be considered to develop efficient fault tolerance mechanisms (short- or open-circuit detection, watchdogs, etc.) at the upper layers. With this limitation, two kinds of component faults are to be taken into account to determine the reliability of transmissions:

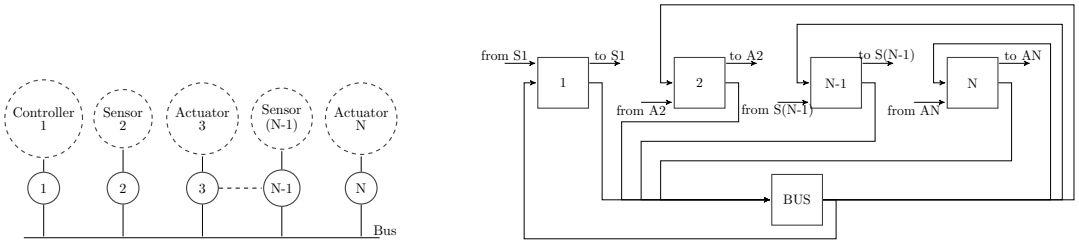
- Omission of data, to represent the absence of signal sent, transmitted or received by a component;
- Commission of data, to represent the unexpected continuous emission of data.

Value and timing failures (erroneous values of data received or data received too late or too early) are outside the scope of this study because they are caused by faults in the upper layers or the environment.

The model of a component must be then multi-state with two failure states. The first one describes a local failure while the second one corresponds to a propagated failure; when a component of the fieldbus is continuously emitting, the bus is indeed no more available for data transmissions between the other components. Once the models of the fieldbus components constructed, the reliability of the transmission is to be assessed. The classical methods for fault forecasting that are based on binary components are no more appropriate; reliability assessment may be based on the analysis of the Markov chain that represents the fieldbus, however. This model may include a very large number of states and its analysis by simulation or formal methods may be very time-consuming or lead to state space explosion. Finding an analytic expression of the considered reliability from this model is far more effective.

This explains why, in previous works Aza-Vallina et al. (2011), a method to obtain the analytic expression of the reliability of a two-terminal data transmission has been developed. This method is based on modelling of the components with multi-state continuous Markov chains and the analysis of the topology of the network to obtain the allowed combinations of components states, i.e. the combinations that allow a correct transmission. The analysis prevents from (or at least limits) the combinatory explosion by providing a limited number of combinations of states. However, this contribution requires two kinds of models, dysfunctional models of the components of the fieldbus and a functional model of the topology of the network, be developed and analysed.

The aim of this paper is to show that the analytic expression can be obtained from a model of the fieldbus in the form of connected mode automata. Mode automata are indeed a powerful formalism that permits to model jointly functional and dysfunctional behaviours and that has been already used for dependability analyses of physical processes Boiteau et al. (2006), but not for communication networks. It will be then shown in what follows (Figure 1) how a fieldbus whose stucture is known and where the terminals have two failure modes can be modelled as a set of connected mode automata; the analysis of this model will permit to obtain the set of allowed combinations



(a) fieldbus structure

(b) model of the fieldbus

$$\pi_{i\leftrightarrow j} = e^{-(\lambda_i^N+\lambda_i^S).t}.\left[\prod_{l\in[1..N]\setminus\{i,j\}}\left(\frac{\lambda_l^N+\lambda_l^S.e^{-(\lambda_l^N+\lambda_l^S).t}}{\lambda_l^N+\lambda_l^S}\right)\right].e^{-(\lambda_j^N+\lambda_j^S).t}\left(e^{-\lambda_B.t}\right)$$

(c) reliability expression

Fig. 1. Aim of the paper

of states, then the analytic expression of the considered reliability.

The outline of this paper is the following. The principle of the construction of the analytic expression when the fieldbus components are modelled as Markov chains is briefly reminded in the next section. The model of the components of the fieldbus by using the formalism of mode automata and the construction of the analytic expression of the two-terminal transmission reliability from these models are presented in the third and fourth sections. The two modelling approaches are discussed in the fifth section then concluding remarks and some perspectives are finally given.

2. BACKGROUND

The aim of this section is to describe briefly a method to obtain the analytic expression of the reliability of a transmission between two terminals connected by a bus, assuming that all terminals of the network are modeled as multi-state components with a propagated failure. More details can be found in Aza-Vallina et al. (2011) and application to bus partitioning is presented in Aza-Vallina et al. (2012)

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) and E is a set of non-directed edges between couples of elements of $\mathcal{N}$ (an edge represents a physical link between two nodes).Two nodes are adjacent if there exists at least one edge between these 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}; this set may contain one or several paths. An element of P_{ij} will be noted P_{ij}^k.

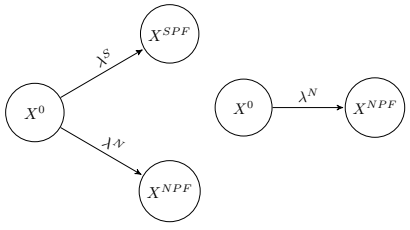
2.2 Component behavior models

The behavior of a network component will be then described by a continuous Markov chain where X_i is the set of states of this chain. The common two-states (faultless or faulty) behavioral component model, also termed binary model, is used for the bus. However the behavioral model of a terminal is a multi-state model which includes three states:

- X_i^0 correct operation state,
- X_i^{SPF} propagated failure state. A component failure is termed "propagated" when its occurrence entails that every adjacent component becomes unable to ensure any communication, even if it is itself failure-free. According to Levitin and Xing (2010) this failure is a propagated failure with a selected effect because only the components which are directly adjacent to the failed component become themselves unable to perform their service.
- X_i^{NPF} non-propagated failure state. A component failure is termed "non-propagated" when its occurrence does not impact the behavior of adjacent components.

The probability that a state of the chain is the active state at date t will be noted respectively $\pi_i^{X_i^0}(t)$, $\pi_i^{X_i^F}(t)$,$\pi_i^{X_i^P}(t)$.

The behavior of a terminal and a bus can be described by the models of Figure 2(a) and 2(b).



(a) (b)

Fig. 2. Markov chains modelling a fieldbus terminal (a) and a bus (b) (λ^N : Non propagated failure rate and λ^S : Selected propagated failure rate)

2.3 Transmission reliability evaluation

From the models given previously, a method to obtain the analytic expression of 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.

This method comprises two steps which are performed sequentially. The first step is aiming at determining for the whole set of paths between i to j, the component state combinations such that the transmission is possible. The analytic expression of the reliability is then constructed.

These two steps will be illustrated below on the example of Figure 1(a) : N terminals connected to a fieldbus.

Research of the component state combinations for all paths
A transmission through the path 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-propagated failure state;
- all other components are in any state.

In the example, there is only one path : $i \rightarrow Bus \rightarrow j$. The three components of this path must be in the correct operation state; the other terminals are adjacent to the bus and must not be in the propagated failure state. The sets of allowed states of the components of the fieldbus for this transmission are listed in Table 1.

Table 1. Set of allowed states for each component

	Path $i \leftrightarrow j$
Component	$P^1_{i \leftrightarrow j}$
i	X_i^0
j	X_j^0
Bus	X_{Bus}^0
for $l \in [1..N], l \neq i, l \neq j$	$X_l^0 \cup X_l^{NPF}$

The active state of the Markov model of the network at a given date is the combination of the active states of the components at this date. The set $C_{ij}^{P_{ij}^k}$ of the allowed combinations for a transmission through a path k is then obtained from the sets $X_l^{P_{ij}^k}$ of the allowed states of the components in the following way:

$$C_{ij}^{P_{ij}^k} = \prod_{l \in \mathcal{N}} X_l^{P_{ij}^k} \tag{1}$$

If several paths from i to j exist, the set of allowed state combinations for all paths noted $C_{ij}$is obtained by conjunction of the sets of allowed combinations for each path:

$$C_{ij} = \bigcup_{P_{ij}^k \in P_{ij}} C_{ij}^{P_{ij}^k} \tag{2}$$

In the example, it comes:

$$C_{ij} = C_{ij}^{P_{ij}^1} = X_i^0 \times \left[\prod_{l \in [1..N] \setminus \{i,j\}} (X_l^0 \cup X_l^F) \right] \times X_j^0 \times X_{Bus}^0 \tag{3}$$

It must be noted that the number of allowed combinations (2^{N-2}) is far smaller than the total number of combinations (3^N). Therefore, the size of the model to analyze is strongly reduced; if N=10 for instance, only 256 combinations are to be considered while the whole Markov chain that represents the fieldbus contains more than 59,000 combinations.

Analytic 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 fieldbus 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:

$$\pi^c(t) = \prod_{l \in \mathcal{N}} \pi_l^{\alpha_l^c}(t) \tag{4}$$

because failures occurrences are independent events.

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

$$\pi_{ij}(t) = \sum_{c \in C_{ij}} \pi^c(t) = \sum_{c \in C_{ij}} \prod_{l \in \mathcal{N}} \pi_l^{\alpha_l^c}(t) \tag{5}$$

For the example, and assuming that every failure rate is constant, the analytic expression of the reliability of the transmission between the terminals i and j is then:

$$\pi_{i \leftrightarrow j} = e^{-(\lambda_i^N + \lambda_i^S).t} . \left[\prod_{l \in [1..N] \setminus \{i,j\}} \left(\frac{\lambda_l^N + \lambda_l^S . e^{-(\lambda_l^N + \lambda_l^S).t}}{\lambda_l^N + \lambda_l^S} \right) \right] . e^{-(\lambda_j^N + \lambda_j^S).t} (e^{-\lambda_B . t}) \tag{6}$$

where λ_l^N and λ_l^S are the non-propagated and propagated constant failure rates of the component l, and λ_B the failure rate of the bus.

3. MODELLING FIELDBUS COMPONENTS WITH MODE AUTOMATA

3.1 Notations

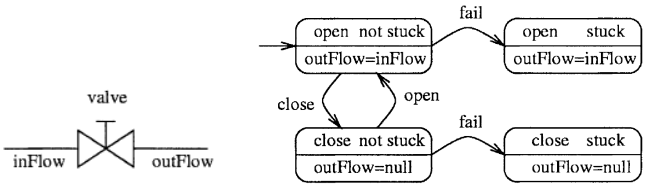
Mode automata are a class of finite state automata with inputs/outputs that has been defined in Rauzy (2002). A state is called mode and at every time only one mode is active. The transitions between two modes are triggered by events and in each mode a transfer function defines the relation between the outputs and the inputs. Formally, a state automaton is a 9-tuple :

$$< \mathbb{D}, dom, S, \mathbb{F}^{in}, \mathbb{F}^{out}, \Sigma, \delta, \sigma, \mathbb{I} > \tag{7}$$

where:

- $\mathbb{D}$ is a set of symbols;
- dom(v) is the set of all possible values of the variable v;
- S is the set of state variables; a combination of values of every state variable defines a mode;
- $\mathbb{F}^{in}$ is the set of input flows;
- $\mathbb{F}^{out}$ is the set of output flows;
- Σ is the set of events;
- δ is a partial function from $dom(S) \times dom(\mathbb{F}^{in}) \times \Sigma$ to $dom(S)$; called transition function; it is used to define the possible transitions between the different modes;
- σ is a total function of $dom(S) \times dom(\mathbb{F}^{in})$ to $dom(\mathbb{F}^{out})$, called transfer function; it is used to define the output flows depending on the mode considered and the input flows;
- $\mathbb{I}$ is the initial mode.

An example of mode automaton from Rauzy (2002) is shown at Figure 3. Modes (states) are depicted by rounded rectangles; the name of the mode is given at the top position and the transfer function for this mode at the bottom position. This example illustrates clearly that a mode may describe both functional and dysfunctional behaviours.



(a) (b)

Fig. 3. A valve (a) and the associated mode automaton (b)

- $S = \{state; stuck\}$; with $dom(state) = \{open; close\}$ and $dom(stuck) = \{true; false\}$;
- $\mathbb{F}^{in} = \{inFlow\}$; $\mathbb{F}^{out} = \{outFlow\}$; with $dom(inFlow) = dom(outFlow) = \{null; low; medium; high\}$;
- $\Sigma = \{open, close, fail\}$;
- δ and σ are defined as pictured Figure 3(b);
- $\mathbb{I} = \{open; false\}$.

3.2 Models of the fieldbus components

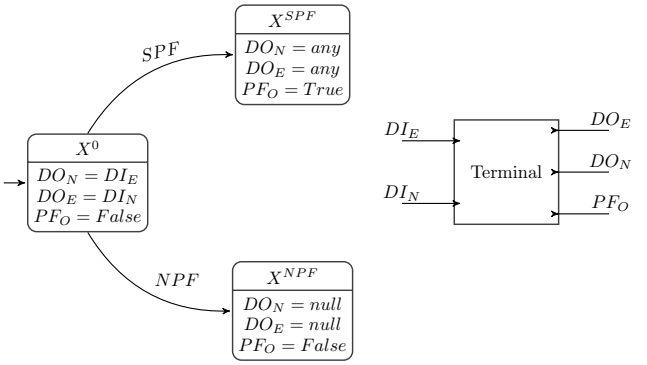
The models of the components (terminals and bus), in the form of mode automata, can be constructed from those presented in section 2 by introducing two kinds of flows:

- Data flows, to represent the data emitted, transmitted or received, what is quite obvious when modelling of communication network components is addressed;
- Failure flows, to represent the propagation of failure from a component with a commission failure to the adjacent components.

Once these two flows introduced, the model of a fieldbus terminal can be set up (Figure 4).

The formal definition of this model is the following:

- $S =< state >$, because only one variable is necessary to characterize the mode; here $dom(state) = \{X^0; X^{SPF}; X^{NPF}\}$;



(a) Internal view (b) External view

Fig. 4. Model of a terminal

- $\mathbb{F}^{in} =< DI_N; DI_E >$:
  - The flow DI_N (Data Input from the Network) represents the data flow coming from the fieldbus (sent by another terminal and transmitted through the bus) with $dom(DI_N) = \{null, any, message\}$. *null* represents the absence of data at the input of the terminal while *message* and *any* represent respectively a correct and incorrect message received by the terminal;
  - The flow DI_E (Data Input from the Environment) represents the data flow coming from a sensor, an actuator or a controller, with $dom(DI_E) = \{null, message\}$. It must be noted that the message is always considered correct in that case;
- $\mathbb{F}^{out} =< DO_N; DO_E; PF_0 >$:
  - The flows DO_N and DO_E represent respectively the outgoing data flow to the bus and to the environment with $dom(DO_N) = dom(DO_E) = \{null, any, message\}$
  - The flow PF_O represents a failure flow sent by a component with a commission failure with $dom(PF_O) = \{True, False\}$;
- $\Sigma = \{NPF; SPF\}$ is the set of the two failure events defined in section 2 (non-propagated failure, selected propagated failure);
- δ : the transition function of the automaton is depicted by the figure 4;
- σ : the transfer function is defined in Table 2. An element of σ will be noted: $(x, (di_n, di_e), (do_n, do_e, pf))$;
- $\mathbb{I}$ is the initial mode that represents the faultless state (X^0).

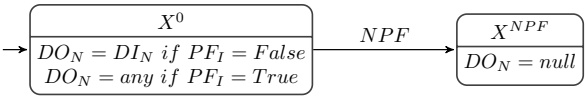
This model represents a bidirectional data transmission (from/to the network). A unidirectional model can be easily obtained by removing a data input, e.g. DI_E, and the corresponding data output, e.g. DO_N.

The model of the bus is shown at Figure 5. In the faultless state, the Data Output is identical to the Data Input if no Propagated Failure flow is received, i.e. no terminal connected to the bus is in a state of propagated failure, and is *any* otherwise. In the faulty state, which represents a non-propagated failure, no data is sent. It must be noted that this model represents a unidirectional data transmission whereas a bus allows bidirectional transmissions; however, this modelling fits the objective of this work: evaluation of the reliability of a data transmission from a given terminal

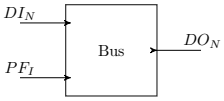
Table 2. Definition of σ for a terminal.

X	DI_N	DI_E	DO_N	DO_E	PF_O
X^0	$null$	$null$	$null$	$null$	$False$
X^0	any	$null$	$null$	any	$False$
X^0	$message$	$null$	$null$	$message$	$False$
X^0	$null$	$message$	$message$	$null$	$False$
X^0	any	$message$	$message$	any	$False$
X^0	$message$	$message$	$message$	$message$	$False$
X^{SPF}	$null$	$null$	any	any	$True$
X^{SPF}	any	$null$	any	any	$True$
X^{SPF}	$message$	$null$	any	any	$True$
X^{SPF}	$null$	$message$	any	any	$True$
X^{SPF}	any	$message$	any	any	$True$
X^{SPF}	$message$	$message$	any	any	$True$
X^{NPF}	$null$	$null$	$null$	$null$	$False$
X^{NPF}	any	$null$	$null$	$null$	$False$
X^{NPF}	$message$	$null$	$null$	$null$	$False$
X^{NPF}	$null$	$message$	$null$	$null$	$False$
X^{NPF}	any	$message$	$null$	$null$	$False$
X^{NPF}	$message$	$message$	$null$	$null$	$False$

to another terminal. Moreover, it will be shown in the next section that this reliability does not depend on the direction of the transmission.



(a) Internal view



(b) External view

Fig. 5. Model of the bus

4. FINDING THE EXPRESSION OF THE RELIABILITY OF A TWO-TERMINAL COMMUNICATION

4.1 Model of the whole fieldbus

Three composition laws of mode automata are defined in (Rauzy, 2002): parallel composition, synchronization and connection. Parallel composition and synchronization are appropriate to compose two mode automata when no input/output flow of one automaton is connected to an output/input flow of the other one; parallel composition is to be used when the two automata do not share any event while synchronization must be selected when at least one event is common to the two automata. In the case of fieldbuses, the mode automata that represent the different components do not share any event because two failures of two components are independent events, but the input/output flows of some components are connected to the output/input flows of other components; this explains why the connection composition law is to be selected. The model of the whole fieldbus is obtained by connecting the models of the components according to the fieldbus topology.

The input DI_N^{Bus} of the bus model may receive data flows DO_N^k from all terminals; however, the assumption that at

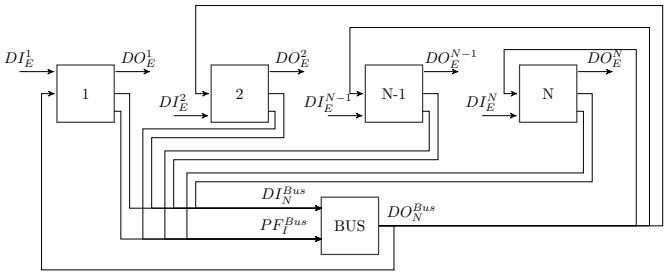


Fig. 6. Connected mode automata that model a fieldbus

any moment one and only one terminal sends data to the bus (correct operation of the bus controller) will be made:

$$\forall t, \exists!\ ^1\ k \in [1..N] | DI_N^{Bus} = DO_N^k \tag{8}$$

The flows which represent propagated failures are binary (True or False). The input PF_I^{Bus} of the bus model becomes True when at least one of the terminals output flow PF_O^k becomes True; therefore PF_I^{Bus} is the disjunction of all propagated failure flows PF_O^k of the terminals:

$$PF_I^{Bus} = PF_O^1 \vee PF_O^2 \vee ... \vee PF_O^{N-1} \vee PF_O^N \tag{9}$$

Last, to represent the links between the input and output flows of the components, the set *connection* must be defined. This set contains three kinds of links:

- (PF_O^m, PF_I^{Bus}) : with $m \in [1...N]$, which represent the propagation of a commission failure from the terminal m to the bus.
- (DO_N^m, DI_N^{Bus}) : which represent the data transmission from the terminal m to the bus.
- (DO_N^{Bus}, DI_N^m) : which represent the data transmission from the bus to the terminal m.

4.2 Algorithm

To obtain the set of allowed states (AS) of every component, states such that a data transmission from terminal i to terminal j is possible, the algorithm below has been developed; this algorithm is based on the transfer functions of the mode automata that model components and the knowledge of the set *connection*.

- The lines 1 to 3 focus on the destination terminal (j). The transfer function shows, lines :
  - $(X^0, (message, null), (null, message, False))$
  - $(X^0, (message, message), (message, message, False))$

  that this terminal transmits correctly a message from the input DI_N^j to the output DO_E^j if and only if its active state is X^0. The set of allowed states is reduced to this only state for this component.
- The rest of the algorithm considers the output flows connected to the input DI_N^j. There is only one such flow, from the bus, in the case study but the approach can deal with more output flows. More precisely:
  - The lines 5 to 7 permit to find the allowed states of the components directly connected to the terminal j. In the example, the bus is capable

[1] $\exists!$ means that there exists one and only one

Algorithm 1 Determination of the allowed states for a transmission from i to j

Require: Set *connection*, Models of the components (in the form of mode automata)

1: **for** $\forall(x,(di_n,di_e),(do_n,do_e,pf)) \in \sigma^j \mid di_n = message, do_e = message$ **do**
2: $AS \leftarrow (j,x)$
3: **end for**
4: **for** $(DO_N^k, DI_N^j) \in connection$ **do**
5: **for** $\forall(x,(di_n,pf),(do_n)) \in \sigma^k \mid di_n = message, do_n = message, pf = False$ **do**
6: $AS \leftarrow (k,x)$
7: **end for**
8: **for** $(PF_O^l, PF_I^k) \in connection$ **do**
9: **for** $\forall(x,(di_n,di_e),(do_n,do_e,pf)) \in \sigma^l \mid pf = False$ **do**
10: $AS \leftarrow (l,x)$
11: **end for**
12: **end for**
13: **for** $(DO_N^i, DI_N^k) \in connection$ **do**
14: **for** $\forall(x,(di_n,di_e),(do_n,do_e,pf)) \in \sigma^j \mid di_e = message, do_n = message$ **do**
15: $AS \leftarrow (i,x)$
16: **end for**
17: **end for**
18: **end for**
19: **return** Set of allowed states (AS)

to transmit the message from DI_N^{Bus} to DO_N^{Bus} (connected to DI_N^j) if and only if its active state is X^0. Then, the set of allowed states is reduced to this only state.

- The lines 8 to 12 consider the propagated failures. The components that are not directly connected to the terminal j but to the components previously analysed must not be in a propagated failure mode.
- Last, the lines 13 to 16 determine the allowed states of the source terminal (i). The conclusion is identical to that obtained for the destination terminal.

The set of allowed states for each component is identical to that given at Table 1. Once these states determined, the combinations of allowed states are known and the analytic expression of the reliability of the transmission can be easily stated according to (4).

5. DISCUSSION

The analytic expression of the reliability of the data transmission between two terminals can be obtained from components models in the form of either Markov chains or mode automata. In the first case, the model of the network topology is required and must be analysed to determine the allowed states for each component. This is no more necessary when the components are modelled by mode automata; all the helpful information is included in the model of the set of connected mode automata that describes the network. It matters however to note that the modelling effort is more important with mode automata mainly because the definition of the transfer function for the model of a component requires two kinds of flows: data and failure flows, be considered. This bigger effort is nevertheless well counterbalanced when looking for the allowed states.

6. CONCLUSION

This paper has shown that connected mode automata can be used to represent a fieldbus in which components failures may be selected propagated. From this model, an analytic expression of the reliability of the data transmission between two terminals has been stated; this expression can be used to compare several technical solutions, with a redundant bus, different failure rates, etc. It must be noted that reliability of the transmission has not been obtained from simulations but from an analysis of the flows between the automata.

A direct perspective of this work is to extend the analysis to the actuators, sensors, controllers connected to the fieldbus components. This will allow a fault forecasting analysis of the whole distributed measurement and control system be performed by using the same modelling formalism and contribute to the development of this formalism.

REFERENCES

Aza-Vallina, D., Denis, B., and Faure, J.M. (2011). Communications reliability analysis in networked embedded systems. In G..G.S. Bérenguer (ed.), *Advances in Safety, Reliability and Risk Management*, 2639–2646. Taylor & Francis Group, Troyes, France.

Aza-Vallina, D., Denis, B., and Faure, J.M. (2012). Influence of bus partitioning on the reliability of transmissions. In *Proceedings of International Joint Conference PSAM'11/ESREL'12*, 02–Mo2–4. Helsinki, Finland.

Boiteau, M., Dutuit, Y., Rauzy, A., and Signoret, J.P. (2006). The altarica data-flow language in use: modeling of production availability of a multi-state system. *Reliability Engineering & System Safety*, 91(7), 747 – 755. doi:10.1016/j.ress.2004.12.004.

Cauffriez, L., Ciccotelli, J., Conrard, B., Bayart, M., and the members of the working-group CIAME (2004). Design of intelligent distributed control systems: a dependability point of view. *Reliability Engineering & System Safety*, 84(1), 19 – 32. doi:10.1016/S0951-8320(03)00174-1.

Levitin, G. and Xing, L. (2010). Reliability and performance of multi-state systems with propagated failures having selective effect. *Reliability Engineering & System Safety*, 95(6), 655 – 661. doi:10.1016/j.ress.2010.02.003.

Rauzy, A. (2002). Mode automata and their compilation into fault trees. *Reliability Engineering and System Safety*, 78(1), 1–12.