Reliability and credibility evaluation of networked control systems

Christophe Simon, Jean-Marc Thiriet, Pavol Barger, Jean-François Aubry

Reliability and credibility evaluation of networked control systems

C. Simon, J.M. Thiriet, P. Barger
CRAN - Nancy Research Centre for Automatic Control, ESSTIN, 2, rue Jean Lamour - 54519 Vandoeuvre-les-Nancy, France, e-mail: christophe.simon@esstin.uhp-nancy.fr

J.F. Aubry
INPL - Polytechnic National Institute of Lorraine, Nancy, France,
e-mail: Jean-Francois.Aubry@ensem.inpl.fr

ABSTRACT: The evaluation of system reliability is often based on classic probabilistic tools such as fault trees or reliability diagrams. But with few information or with low probability events, probability distributions are weakly defined and the probability theory is not well fitted. The idea is to use the possibility theory applied to classic tools of the reliability evaluation (De Cooman & Cappelle 1994, De Cooman 1996) to obtain the system reliability with some information on the credibility of results. Similarly, the control of systems evolves to distributed architectures with the integration of communication systems (Ligusova et al. 2004). The proposed study concerns the evaluation of the reliability of a networked control system by a possibility theory approach with the evaluation of the results credibility.

1 INTRODUCTION

Networked Control Systems (NCS) are an extension of classical distributed control systems. The main difference is the presence of a communication network. It could be considered as a particular component interacting with all the other components of the system. In this way, the communication network takes a central place in control systems. This strategic position is not without consequences for the safety point of view. Thus, meticulous studies have to be done with a set of appropriate criteria (Juanole 2002). Mainly, studies have been done on the communication network itself and are part of the performances evaluation of the communication. The dependability study is not really taken into account.

The study of the reliability of an NCS is so a particularly complex problem and need the use of appropriate evaluation methods. A solution to this problem thanks to Monte-Carlo simulations and colored Petri nets is proposed in (Barger et al. 2003).

The study of reliability is generally achieved under the frame of the probability theory. This formal and rigorous frame is mastered when we dispose of reliable failure probabilities for the various components. More, the reliability index is a probability value which does not provide any information on the sensitivity or credibility of the index. The possibility theory is then a formal frame which is more open because it takes into account the uncertainty on the initial probability precision and the result credibility. These points interest our study.

In this paper, we describe in the first section the NCS application process to which we have implemented the study. In a second section, we recall the frame of the study of this NCS thanks to colored Petri nets in order to get a probabilistic reliability index. In the third section, we propose the formal frame of the possibility theory and this frame is used for the study of the reliability of the NCS. The last section concerns our study of the NCS reliability with the possibility theory and we propose some analysis.

2 NETWORKED CONTROL SYSTEM

In order to show the interest of probabilistic and possibilistic methods to study the reliability of NCSs, we propose to focus on a simple control loop showing all the complexity of the study.

We define a small NCS which is designed to control the liquid level in a tank. In order to achieve this, the NCS is composed of (Fig. 1):
- a sensor,
- a controller,
- an actuator,
- a communication network.

The mission of the NCS is to maintain the required liquid level in the tank. For this reason an analogue liquid level value is provided by the sensor. Its measure is communicated via the network to the controller which determines the new control value and sends it to the actuator which represents a pump on the entry of the tank and which conditions the input flow of the tank. A small additional pertur-

bation (a leak or evaporation) affects the controlled system.

In the initial state the tank is empty and has to be filled. The required final liquid level is fixed at *500* height units.

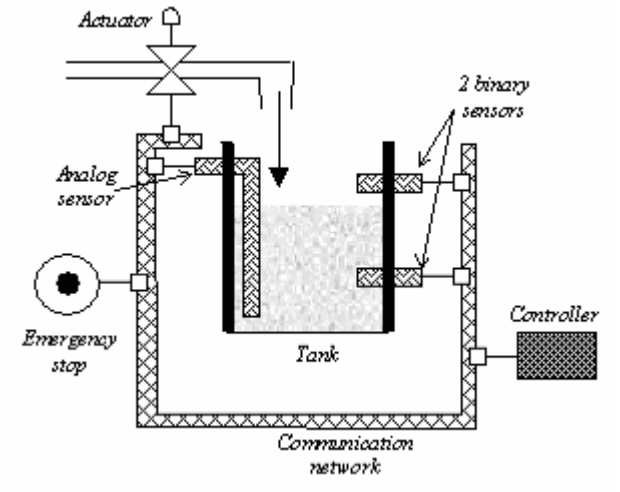

Figure 1. NCS application process

All the components are represented as discrete systems with *Ts* as the sampling period. All through this work *Ts* is considered constant and equal to *10* time units. The sensor, the controller and the actuator are time triggered. The communication network is an event triggered element. In order to combine these two different triggers, input and output buffers are placed at the junctions between the communication network and the other components.

Different failures chosen arbitrarily can occur on any of these components. No reparations of component failures are considered. A detailed description of each component of the NCS follows.

2.1 *Sensor*

In this example a periodic sensor is considered. An hypothesis of measuring the true value is done but does not affect the scope of the proposed method. Every *Ts* a new measure is obtained and prepared to be sent. Two different functionalities can be distinguished on the sensor:

1 measurement,
2 communication.

The sensor failure does not affect the communication capacity. The consequence is that the sensor is unable to send the measured value and sends instead a frame informing of the sensor failure. The probability (uniform distribution) of this failure is fixed as a constant equal to 1/100 *Ts* where *Ts* is the sampling period of the system. This measuring element failure is referred to as the *Sensor_failure* in the following.

2.2 *Controller*

The design of a controller for an NCS is a problem beyond the scope of this communication. A proposition can be found in Walsh & Ye (2001). The controller implemented is a Smith predictor with a PI algorithm. The supposed pure delay is 2**Ts* which corresponds to one *Ts* delay for transmission for each information from the sensor to the controller and from the controller to the actuator. All over this study the communication network respects these delays.

During the failure of the controller, the communication functionality is stopped. Thus no message is sent to the actuator. The corresponding failure rate is constant and placed arbitrarily as 1/100 *Ts*. The failure described is referred to as the *Controller_failure* in the following.

If the controller does not obtain a measure from the sensor, either because the later has failed or because the information is lost during the transmission, it continues to determine the control value using the last measure obtained.

2.3 *Actuator*

A discrete 1st order system represents the actuator inspired by a pump. Two basic states are distinguished: idle and acting. The actuator is declared to be idle if its input (a value from the controller) and its output (actual pumping throughput) are equal. Otherwise, its state becomes acting.

Two different failures are considered with the actuator: a start failure and a functioning failure both of them with constant, uniform probability distributions. The first one is caused by the blocking of the system while initiating an action after the idle state of the actuator. The second one is a typical wear-out problem for which the occurrence probability is increased by the continuous action.

The start failure (referred to as *Actuator_blocked*) is an error which is not dependent on the time of run but rather on the number of solicitations. The failure probability is defined as one blocking over 100 start requests. Thus it is dependent on the chosen control algorithm. This failure is more important when a binary control law is applied (pump either on 100% or closed) than with a PI algorithm where starts and stops are less frequent.

The functioning failure (or *Actuator_wearout*) is represented with a stochastic failure appearance while the pump is functioning. A uniform distribution of the probability is considered and the failure rate is fixed as 1/50 *Ts*. This failure rate is also a function of the control algorithm, but its dependence varies from the *Actuator_blocked* failure function.

The co-existence of these two different kinds of failure rates is rather problematic in traditional

safety evaluation methods but can be resolved easily in a CPN model.

2.4 *Communication network*

The communication network is the only event triggered component in the modeled example. The transport delay of a transmission of each communication frame is considered constant and is fixed as 1/10 *Ts*. In each macrocycle two communication frames are transmitted: one containing the measured value, sent from the sensor to the controller and the second one with the control value from the controller to the actuator. In case of need, this model can be modified to represent a random delay (such as a jitter). The medium access protocol is of little importance for this study, as the network bandwidth is guaranteed to be highly superior to the bandwidth needed.

The interest of a communication network in this example is in the errors appearing during the transmission. Two errors are integrated and studied in this case:

- communication *Frame_loss*,
- *Frame_alternation.*

In this study it consists in erasing the data field in the frame.

The probabilities are constant and identical for both errors and fixed at 1 *Frame_loss* out of 20 frames transmitted and 1 *Frame_alternation* out of 20 frames. Thus statistically every 10^{th} frame transmitted is not received correctly.

All occurrence rates of previously defined failures are presented in table 1.

Table 1. Failure and errors review

Event name	Event code	Failure probability
Sensor_low_failure	1	1/100 *Ts*
Sensor_high_failure	2	1/100 *Ts*
Sensor_analog_failure	3	1/100 *Ts*
Controller_failure	4	1/100 *Ts*
Actuator_blocked	5	1/100 requests
Actuator_wearout	6	1/50 *Ts*
Frame_alternation	7	1/20 frames
Frame_loss	8	1/20 frames
Alarm_activated	9	
Alarm_applied	10	

2.5 *Evaluating failure rate*

The study of the reliability of an NCS from the failures of its components is a complex problem, which can be considered as an hybrid system. Table 1 shows indeed some failure rates expressed as a function of time or as a function of events. Moreover, the determination of the global reliability of the system does not depend only on the time but also on the system state, the nature of the network failure, and the type of lost information. We want to add that the type of information is not taken into account in the present study.

For this study, it is not possible to use the traditional reliability tools such as functional diagrams or failure trees … We consider the failure of the system as its inability to accomplish its mission, i.e. to keep the level of the liquid close to the set plus or minus 10% as it is shown in figure 2. Two behaviors are considered:

1 the tank is not filled and the liquid height is not closed to the desired value,
2 the liquid level has approached the desired valued but leaves it.

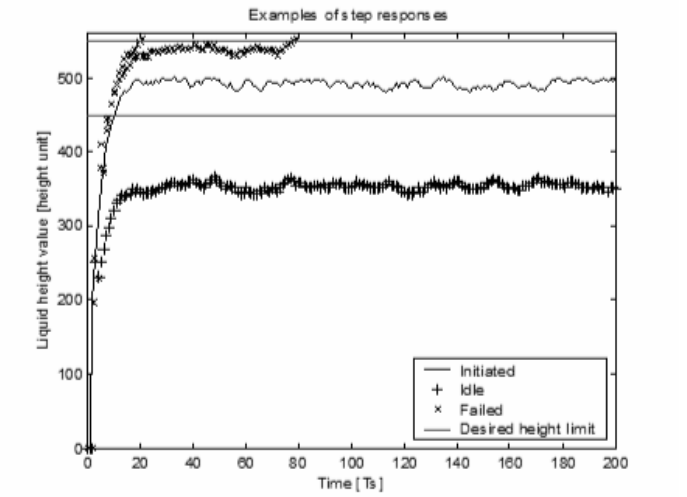

Figure 2. 4 simulation examples

The study is essentially centered on the reliability analysis according to an information point of view and the mission. So, events like medium interferences or electrical spikes are not taken into account because it overcomes the information point of view of the study.

Now the context is defined, the aim is to find the relationship between the elementary failures defined in table 1 and the global failure of the system. To reach this end, we have used a quantitative approach thanks to simulation (Barger et al. 2003). Considering the system as a hybrid one, we have chosen to use colored Petri nets for a functional and malfunctioning model of the NCS. The Petri net-based model of the system is built from the models of the components with a modular architecture (producer-consumer type) because of the existence of the communication network. The Petri net models can integrate any network behaviors even for low level protocols. But the more complex is the behavior, the more complex the model is.

The functional and malfunctioning models of the subparts having a stochastic nature, the analysis of the complete system can be achieved only through Monte-Carlo simulations (Labeau & Zio 2002). It consists in repeating a single simulation a certain number of times. This number has to be rather high

in order to be able to consider the results as statistically reliable and has to be closed to the curse of dimensionality expresses by Bellman (1961). So the number of simulation increases exponentially with the number of events and the time when they occurred. Moreover, as other reliability analysis based on models simulations, the complexity of the model is linked to the complexity of the system modeled. Then, for a reliable analysis, the number of simulation should tend to infinity!!

As the simulation is the way we choose for reliability analysis and as a simulation is time consuming, our study of the reliability of the NCS is based on a finite number of simulations. In Barger et al. (2003), we operate 6734 simulations where each event code was stored with its occurrence time that defines a scenario. Over all simulations, 1114 scenarios induce a global system failure. For this study, we increase the number of simulations to 10000 and obtain 1782 failed scenarios. We note that with 32% of more simulations, the malfunctioning states are more than 1% up as in the previous study. As a conclusion, the number of simulation is too small to obtain a reliable and credible rate of malfunctioning. So, analyzing scenarios in the normative framework of probability theory becomes difficult due to the lack of Monte-Carlo simulations. Then, we choose to investigate the normative framework of possibility theory.

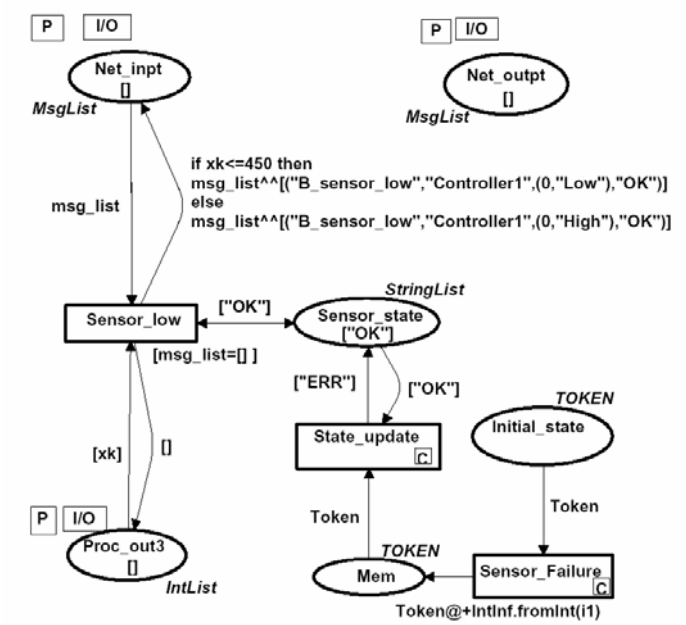

Figure 3. Sensor part of Petri net simulation

3 SAFETY ANALYSIS AND POSSIBILITY THEORY

Zimmerman (2000) classified the causes of uncertainty as: lack of information, abundance of information, measurement and subjective belief. In our case, simulations are missing and do not allow a reliable analysis of scenarios thanks to the probability theory; it is not possible to take into account the uncertainties of the event occurrences on the evaluation of their influence on the global failure.

Other normative theory can be used as interval theory (Moore 1966), certainty theory (Kanal & Lemmer 1986), possibility theory (Dubois & Prade 1988), evidence theory (Shafer 1976) and fuzzy set theory (Zimmerman 1985).

We have chosen to investigate the possibility theory in this context of missing information. Let's recall some principles of this theory we want to exploit here. X is a variable which is not completely known, and Ω is the set of all the possible values for X. We can then define a distribution of possibilities on ω such as $\pi x(\omega):\Omega\rightarrow[0,1]$ that expresses the degree with which it is possible that the current value of a poorly known variable X is ω. If A is an event, in other words a subset of ω, the possibility measure that A be x is: $\Pi(A)=\sup_{\omega\in A}\pi_X(\omega)$. The dual measure of the possibility is the necessity measure defines by:

$N(A)=1-\Pi(\neg A)$. It allows characterizing the uncertainty on the decision attached to A in specifying with what possibility degree the opposite proposal is possible. Possibility distributions are always normalized to 1 in order to always define a possible event from two opposite ones.

These differences are important compared to the probability theory where the definition of the probability of an event defines immediately the value of its contrary. However, a certain amount of constraints is associated to the measurement of possibility or necessity:

$$\begin{aligned}&\Pi(A)<1\Rightarrow N(A)=0\\&N(A)>0\Rightarrow\Pi(A)=1\end{aligned}\qquad(1)$$

These constraints express the fact that one event which is not completely possible is not certain, and that an event which is at least a little necessary is completely possible. This duality allows associating credibility to the decision taken from the couple possibility - necessity.

3.1 *Composition of measure*

The operators for conjunction and disjunction get different properties for the probability theory and the possibility theory. In the possibility theory, we should respect the duality of possibility and necessity measures. This duality is part of the inference rules:

- Disjunction: $\Pi(A\vee B)=\max(\Pi(A),\Pi(B))$ is the possibility that at least one of the two hypotheses be correct is equal to the greatest possibility. In probability theory, the disjunction inference is defined as: $p(A\vee B)=p(A)+p(B)-p(A\wedge(B)$.
- Conjunction: $\Pi(A\wedge B)\leq\min(\Pi(A),\Pi(B))$. Two events are possible but their intersection is less possible than the lowest possibility.

$N(A \wedge B)=\min(N(A),N(B))$. The certainty that the two hypotheses be correct is equal to the certainty of the less certain hypothesis.

4 NCS RELIABILITY ANALYSIS WITH POSSIBILITY THEORY

There is not a sufficient amount of Monte-Carlo simulations to allow us having a frequency view of the reliability study of the NCS. Moreover, probability theory does not allow us to define if a proposition on the system state according to elementary events is credible.

4.1 *Analysis of stories: events/time*

During Monte-Carlo simulations of the NCS, elementary events that define scenarios are time recorded. Our first analysis of these scenarios has consisted in searching a relation between event type, event occurrence time and the final state of the system {*Fail*, *Work*}.

All events with their code in ordinates as defined in table 1 and their occurrences time in abscissa are shown in figure 4. The system final state is represented by a '*' for the *Work* state or by a 'o' for *Fail* state. Each event is coded as previously defined in order to show if it contributes or not to the *Fail* state of the system.

The simulation time does not exceed *900uT* and 1st order system reach the steady state after *120uT* where *uT* is the simulation quantum time. A first analysis of figure 4 is that events 9 and 10 seem to conduct to a general system failure when they occur after *500uT*. The event 4 occurrence did not conduct to a malfunctioning when it occurs after *300uT*. Moreover, we note that events 7 and 8 are the most met events and their occurrences include working scenarios as well as failed scenarios with similar occurrence rate.

From figure 4, it is difficult to define a credible calculus probability structure. But, one can use the possibility theory by defining two possibility distributions for each event. These distributions explain how much it is possible to an event E_i to induce or not a general failure of the NCS.

Without introducing experts' knowledge in the decision process on the reliability analysis, we have proposed a couple of possibility distributions $\pi_{Fail}(E_i,t)$, $\pi_{Work}(E_i,t)$ for each event as shown in figure 5. Each distribution has been heuristically proposed from event occurrences and by taking account the final state of the NCS. Moreover, if no data permits a precise definition of the distribution, no risk is made and we consider that all can occur {*Fail* or *Work*}.

From proposed possibility distributions, one can compute the possibility of a general failure of the NCS *S* or not. For each scenario, one should infer the possibility measure of event E_i at its occurred time *t* as defined in equation 2.

$$\begin{aligned}\Pi_{Fail}(S) &= \wedge_{E_i \in story}\, \pi_{Fail}(E_i,t)\\ \Pi_{Work}(S) &= \wedge_{E_i \in story}\, \pi_{Work}(E_i,t)\end{aligned} \tag{2}$$

The two propositions of equation 2 define the degree of possibility that the NCS is in failure or not from the conjunction of possibility measures of events.

As defined in the previous paragraph, the possibility theory is a more open frame than the probability theory and the calculus of necessity measures by equation 3 allows us to evaluate the credibility of propositions given by equation 2.

$$\begin{aligned}N_{Fail}(S) &= 1 - \wedge_{E_i \in story}\, \pi_{Work}(E_i,t)\\ N_{Work}(S) &= 1 - \wedge_{E_i \in story}\, \pi_{Fail}(E_i,t)\end{aligned} \tag{3}$$

The calculus of necessity measures is dual to possibility measures and allows computing the degree of possibility of the opposite proposition in this context of binary states. Then, the necessity measure defines how a proposition is credible by taking into account how its opposite is possible.

If the proposition $\Pi_{Work}(S)\approx 1$ which explains it is very possible that the NCS is functioning and if $N_{Work}(S)\approx 0$ then the proposition $\Pi_{Work}(S)\approx 1$ is not credible.

Let's taking an example with the following scenario: $\{(E_1,50uT), (E_7,200uT), (E_8,300uT), (E_7,400uT), (E_6,600uT), (E_{10},700uT)\}$. If we compute the possibility and necessity measures from the distributions shown in figure 5, we obtain:

$$\begin{aligned}\Pi_{\mathrm{Work}}(S) &= \begin{cases} \pi_{Work}(E_1,50uT) \wedge \pi_{Work}(E_7,200uT) \\ \wedge\, \pi_{Work}(E_8,300uT) \wedge \pi_{Work}(E_7,400uT) \\ \wedge\, \pi_{Work}(E_9,600uT) \wedge \pi_{Work}(E_{10},700uT) \end{cases}\\ N_{\mathrm{Work}}(S) &= \begin{cases} 1-(\pi_{Fail}(E_1,50uT) \wedge \pi_{Fail}(E_7,200uT) \\ \wedge\, \pi_{Fail}(E_8,300uT) \wedge \pi_{Fail}(E_7,400uT) \\ \wedge\, \pi_{Fail}(E_9,600uT) \wedge \pi_{Fail}(E_{10},700uT)) \end{cases}\end{aligned} \tag{4}$$

This example shows how it is important to use both the possibility and necessity. As one can see according to distributions of figure 5, it is fully possible that the system goes to the *Work* state but it is not credible because the necessity measure is 0.

This analysis of simulation results in figure 4 remains too general. One can note that each event can induce a general failure and that the possibility theory gives complementary information on the credibility of results. But, the chosen representation of events doesn't show the elementary contribution of each event to the general failure. Moreover, the importance of the contribution depending on the occurrence order of events in a story is hidden. The im-

portance of an elementary is context dependant and it induces a more complex analysis.

4.2 *Analysis of the scenarios: scheduled events vs. time*

To make a better analysis and begin to answer to the previous note, we choose to represent events according to their occurrence time and their order positions in a story. The goal of this new representation is to show that events positions in a scenario according to the occurrence time have a great influence on the general failure. Moreover, one can observe in figure 6 that the event code '1' (*Sensor_low_failure*) doesn't induce a general system failure if it is the first event and if it occurs after the beginning of the story. When it occurs in the second position (see Fig.7), the mission failure is possible if its occurrence time is less than *50uT*. The same analysis can be done for event code '2' (*Sensor_high_failure*).

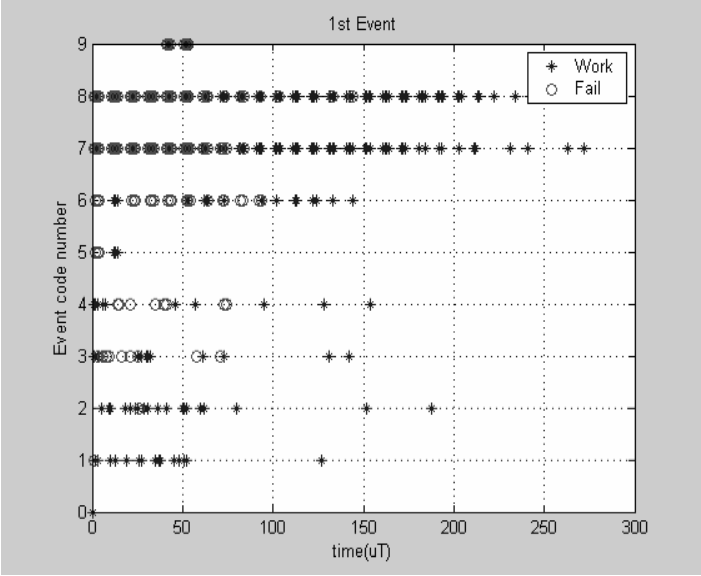

Figure 6. First events

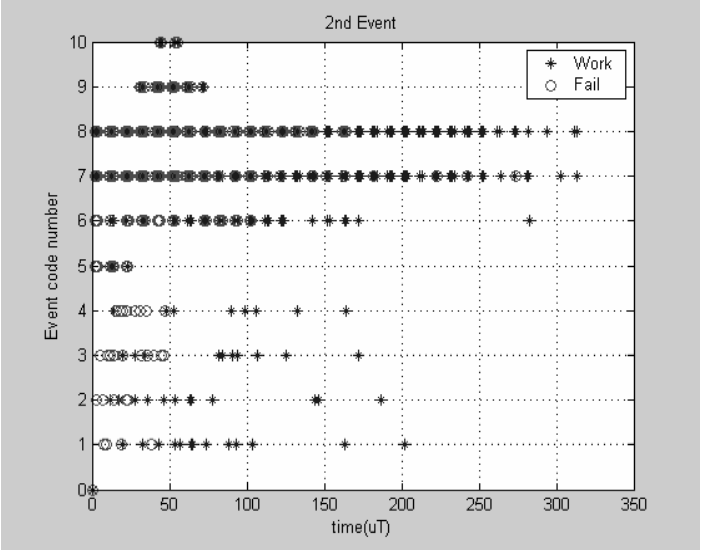

Figure 7. Second events

One can note that this analysis is more precise than the one of the previous paragraph. It is clear that the type of events, the events order and the occurrences times play an important role in the general failure. Computing the system failure possibility $\Pi_{Fail}(S)$ is conditioned by the schedule of events. So, we should define possibility distributions with the following procedure but by taking into account the event order in the story. Figures 8 and 9 show the possibility distributions for the two first events.

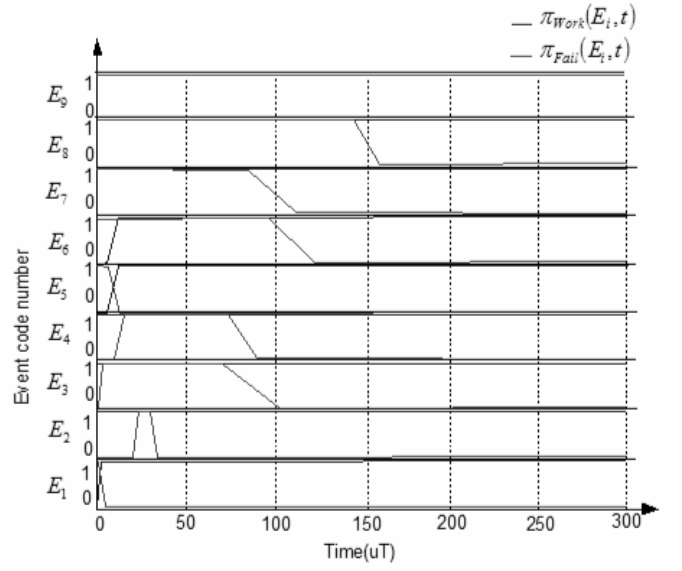

Figure 8. First events possibility distributions

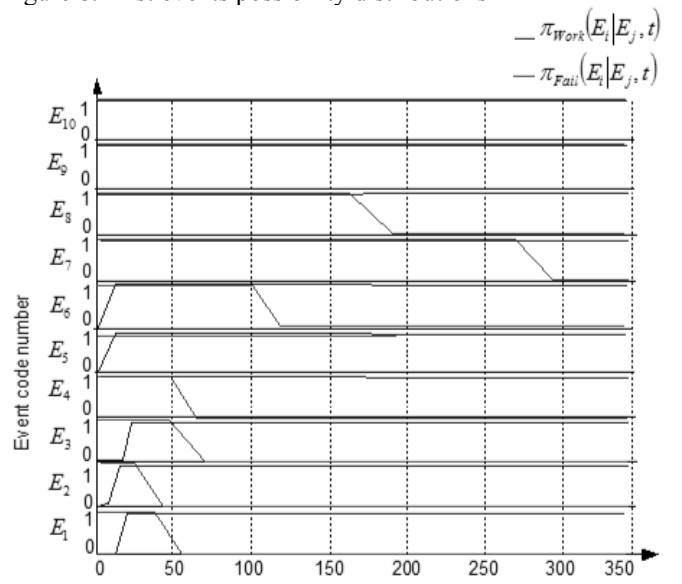

Figure 9. Second events possibility distributions

The possibility measure of system failing or working is defined by equation 5.

$$\Pi_{Fail}(S) = \wedge_{E_i \in story}\ \pi_{Fail}(E_i|j,t)$$
$$\Pi_{Work}(S) = \wedge_{E_i \in story}\ \pi_{Work}(E_i|j,t) \quad (5)$$

where *i* is the event code and *j* is the index of the event in the story.

5 CONCLUSION

In this paper, we have investigated a NCS reliability analysis by the possibility theory with Monte-Carlo

simulations and an information point of view. By using Monte-Carlo simulations we eliminate the formal definition of a structure function which is difficult to obtain with this kind of NCS. We have analyzed simulations story by the possibility theory which find here a good application because there is not a sufficient amount of simulations for a probabilistic point of view.

The proposed analysis remains imperfect. Stories are made of a large number of events and it is impossible to condition possibilities when this number tends to infinity. Moreover, some sequences can be identified in many stories and our analysis does not show neither them nor their relation to the possibility of failure. To take into account this information, we should analyze stories with the new equation 6 where a possibility distribution of an event is conditioned by the previous event as in Bayesian networks (Weber & Jouffe 2003) or Markov chains.

$$\begin{aligned} \Pi_{Fail}(S) &= \wedge_{E_i \in story} \pi_{Fail}(E_i | E_{i-1}, t) \\ \Pi_{Work}(S) &= \wedge_{E_i \in story} \pi_{Work}(E_i | E_{i-1}, t) \end{aligned} \quad (6)$$

For this kind of analysis, we should take a more comfortable tool like possibilistic graphs (Borgelt & Kruse 2003) where conditional possibilities are well manipulated. Moreover, we are interested in cycles of events that seem to be classical in our simulations.

We should also integrate in our analysis the system dynamic, its robustness and its state. In this work the system dynamic is characterized by time because all the simulations are step responses of a 1st order (low time value → high dynamic; large time value → low dynamic).

Finally, we should integrate in our analysis the nature of the corrupted information because the kind of corruption plays a role in maintaining or not the NCS in function.

REFERENCES

Barger, P., Thiriet, J.-M & Robert, M. 2003. Safety analysis and reliability estimation of a networked control system, *IFAC/SafeProcess'2003*, Washington, pp. 1047—1052.

Bellman, R. 1961. *Adaptive Control Processes: A Guided Tour*, Princeton University Press.

Borgelt, C. & Kruse, R. 2003. Learning Possibilistic Graphical Models from Data, *IEEE Transactions on Fuzzy Systems*, vol. 11(2):159-172, IEEE Press, Piscataway, NJ, USA.

De Cooman, G. & Cappelle, B. 1994. A possibilistic uncertainty model in classical reliability theory, *Fuzzy Logic and Intelligent Technologies in Nuclear Science, Proceedings of the First International FLINS Workshop* (Mol, Belgium, September 14-16,), pp. 19—25.

De Cooman, G. 1996. On modelling possibilistic uncertainty in two-state reliability theory, *Fuzzy Sets and Systems*, vol. 83, pp. 215—238.

Dubois, D. & Prade, H. 1988. *Possibility theory. An approach to computerized processing of uncertainty*, Plenum Press, New-York.

Juanole, G. 2002. Quality of service of communication networks and distributed automation: models and performances, Invited paper, *15th Triennal World Congress of the IFAC*, Barcelona, Spain.

Kanal, L. & Lemmer, J. 1986. *Uncertainty in artificial intelligence*, North Holland, Amsterdam.

Labeau, P.E. & Zio, E., 2002. Procedures of Monte Carlo transport simulation for applications in system engineering, *Reliability Engineering and System Safety*, pp. 217—228.

Ligusova, L., Thiriet, J-M., Ligus, J &, Barger, P. 2004. Effect of Element Initialization in Synchronous Networked Control System to Control Quality, *RAMS 2004*

Moore, R.E. 1966. *Interval Analysis*, Prentice-Hall, Englewood Cliffs, NJ.

Schafer, G. 1976, *A mathematical theory of evidence*, Princeton University Press.

Walsh, G.C. & Ye, H. 2001. Scheduling of networked control systems, *IEEE control systems magazine*, pp. 57—65.

Weber, P. & Jouffe, L. 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.

Zadeh, L.A., 1978. Fuzzy sets as a basis for a theory of possibility, *Fuzzy Sets and Systems*, vol. 1, pp. 3—28

Zimmerman, H.-J. 2000. An application-oriented view of modeling uncertainty, *European Journal of Operational Research*, 122, pp. 190—198.

Zimmerman, H.-J. 1985. *Fuzzy Set Theory-and its applications*, Kluwer Academic Publishers.

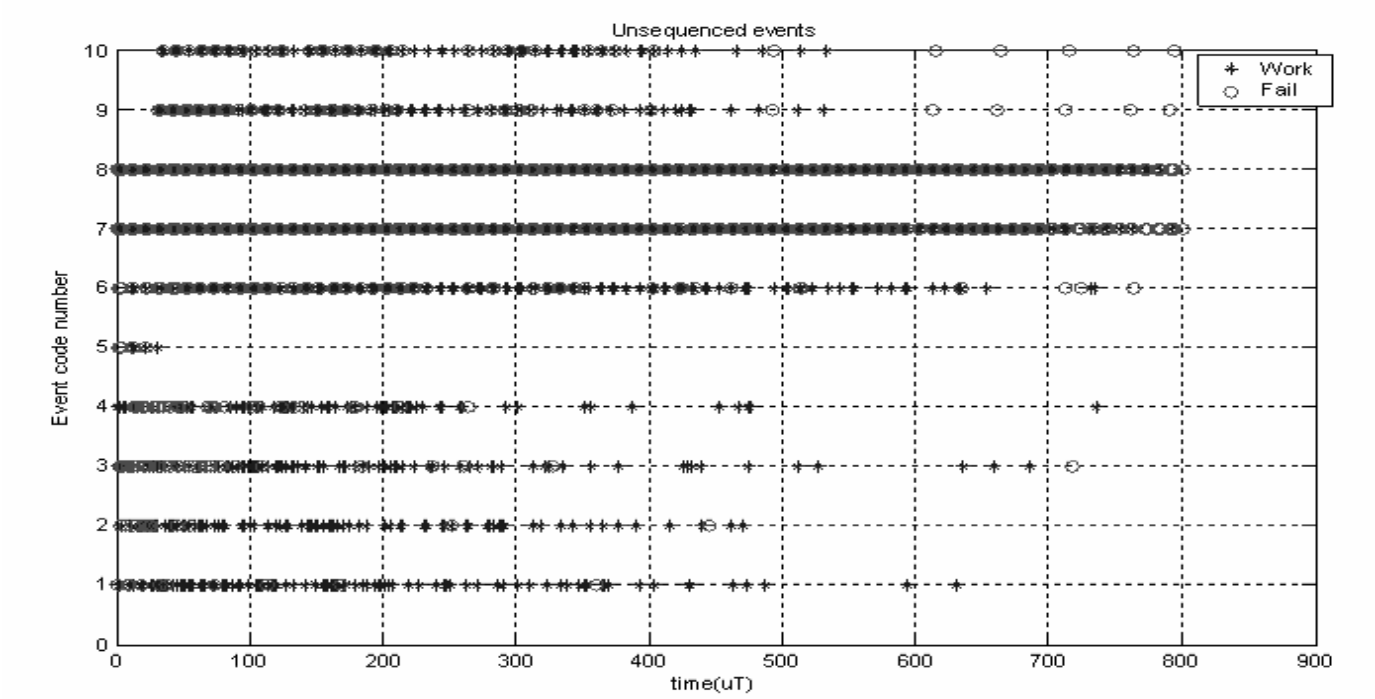

Figure 4. Unsequenced event representation

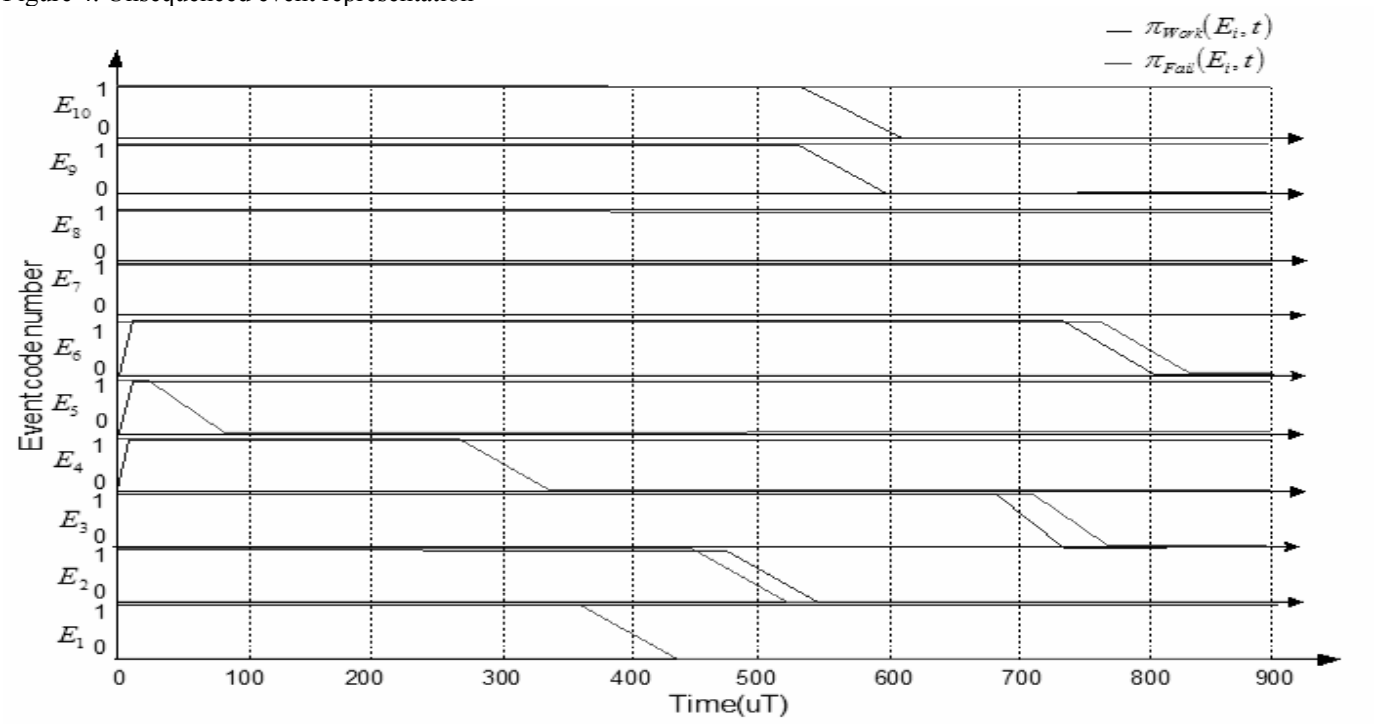

Figure 5. Possibility distributions