Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

A Framework for the Reliability Evaluation of Networked Control Systems

Rony. Ghostine*, Jean-Marc. Thiriet**
Jean-François. Aubry*, Michel. Robert***

**Centre de recherche en automatique de Nancy, Nancy université CNRS UMR 7039*
INPL 2 Av. de la forêt de Haye 54516 Vandoeuvre Lès Nancy, France.
(e-mail: {rony.ghostine, jean-francois.aubry}@ensem.inpl-nancy.fr)
*** Laboratoire GIPSA-Lab (GIPSA-Lab UMR 5216 CNRS-INPG-UJF)*
BP 46, F-38402 Saint Martin d'Hères Cedex
(e-mail :jean-marc.thiriet@ujf-grenoble.fr)
****Centre de recehrche en automatique de Nancy, Nancy-université CNRS 7039*
2, rue Jean Lamour, 54519 Vandoeuvre cedex, France.
(e-mail : michel.robert@esstin.uhp-nancy.fr)

Abstract: this paper presents a framework to enable the analysis of the influence of the transmission faults on the reliability of a networked control system (NCS). The approach is composed of two parts: a modelling part in which all the basic components of a networked control system are modelled and a simulation part in which simulation is done on the models to evaluate the reliability. Due to external perturbations transmission faults may occur on the medium decreasing network quality of service and system performance. These aspects are difficult to assess with traditional dependability method like fault trees and reliability blocks. Our approach is applied to a case study example. The results show that our framework is an effective way for the reliability evaluation of networked control systems (Copyright IFAC 2008).

Keywords: Networked control systems, Reliability analysis, Petri-net, transient faults.

1. INTRODUCTION

Control systems with spatially distributed components have existed for several decades. Examples include chemical processes, power plants, airplanes, etc…. in such systems the components were connected via point-to-point connections and the systems were designed to bring all information from the sensors to a central location to take a decision on how to act (Halevi and Ray, 1988). Physical setups and expanding functionality are pushing the limits of the point-to-point architecture. Hence, such centralized point-to-point control systems are no longer suitable to meet new requirements such as modularity, decentralization of control, integrated diagnostics, quick and easy maintenance, and low cost. Technology advances and the availability of network connectivity have prompted the idea of introducing network facilities to control systems. Such systems are called networked control systems (NCSs): Their sensors, actuators, estimator units, and control units are connected through communication networks. This type of system provides several advantages such as modular and flexible system design, simple and fast implementation, and powerful system diagnosis and maintenance utilities. The disadvantage is that the analysis and design of an NCS becomes complex. Conventional control theory with many ideal assumptions, such as synchronized control and non-delayed sensing and actuation, has to be re-evaluated before it can be applied to NCSs. Specially, the problems of time-varying transmission periods, network schedulability, network induced delay, and packet loss, are of concern (Soglo and Xianhui, 2006).

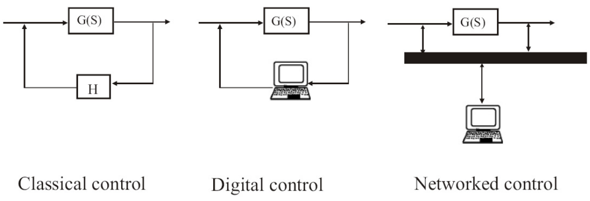


Fig. 1. Networked control system

Networked control systems pose novel challenges to mathematical analysis and design. To analyze the above mentioned issues authors use simulation approach. In (Zhang et al, 2001) Zhang et al. used the Case Western Reserve University campus-wide network (CWRUnet) to simulate the NCS environment and analyse the effect of network-induced delay and packet loss. Branicky et al. (Branicky et al, 2003) developed a simulation tool that combines dynamic-system simulation for the control agents and environment with packet-level network simulation for the communications by extending network simulator-2 (NS2).

Due to the complexity of networked control system architectures, it is not trivial to evaluate their dependability level. The present paper aims at bringing a contribution relative to this aspect.

2. RELIABILIY OF CONTROL SYSTEM

Fault-trees and reliability blocks diagrams are the easiest and most often used techniques in complex systems dependability assessment. Many people have refined these techniques which have been applied to various industries, including aerospace, medical, and nuclear…

These techniques are also called Boolean models. Their aim is to show how a binary system (with two states) state depends on the binary states of the system's components.

These methods are not at all suited to modelling systems in which there are strong dependencies between components. The assumption of components independence is precisely what makes Boolean models so powerful, but this assumption is extremely restrictive, and may prove to be totally unrealistic and lead to grossly erroneous results for some kinds of systems.

These methods can not be directly applied to control systems study for two main reasons:

- These methods do not take into account the transmission delay between nodes. This is a problem since control systems are known to be real time systems and delays are known to be able to degrade or destabilize the system (Zhang et al, 2001).
- The failure definition for control systems depends on the difference between the desired value of a physical property and its actual value, hence the need to calculate this actual value at each step and to compare it with the reference input.

One of the major problems inherent to any reliability study of an industrial system is to take into account, in an effective and realistic way, the dynamic interactions existing between the physical parameters (pressure, temperature, flow rate, level,...) and the nomina1 or dysfunctional behaviour of the components of the system itself. In (Dutuit et al, 1997) the authors present a Petri nets approach for a dependability evaluation of a control process, only permanent faults are considered.

In (Askerdal et al, 2002) the authors developed a control theory methodology for analyzing the effects that data errors may have on the control system dependability. The effect is measured as the resulting control error (defined as the difference between the desired value of a physical property and its actual value).

In (Moncelet et al, 1998) authors proposed an approach to find feared scenarios in control system. Like the works listed below only permanent faults are considered.

Unlike regular control systems, in networked control systems the synchronization between different sensors, actuators and control units is not guaranteed. Furthermore, there is no guarantee for zero delay or even constant delay in sending information from sensors to the control units and control signals from the control units to the actuators; moreover when there is congestion in the communication network, some packets are dropped. In real time systems, particularly control systems, delays or dropped packets may be catastrophic and may cause instability in the control system.

In (Barger et al, 2003), the authors take into consideration the message loss by assigning a fixed probability.

In (Jumel et al, 2004), the authors present a methodology to study the safety of a mechatronic function distributed on a network. They have illustrated this methodology on a brake function mapped on the Time Triggered Architecture (TTA) in presence of transient faults. Thanks to Markov's Chains, they compute some important properties of safety. They take into account different types of faults (byzantine, and non_byzantine) they consider only one type of degradation and they assume that the vehicle's speed is decreased from Mmax in absence of error and Mmin in presence of errors. This assumption tends to simplify the problem and doesn't reflect the real behaviour of a dynamic system, where the faults effect depends on the system dynamics.

Industrial environment is specified by the existence of electromagnetic interferences (EMI). These interferences generate faults in electronic circuits that affect the normal operations. These faults are transient faults which means that the component affected is temporary unavailable, for example if a communication network is affected by a transient fault it may be unable to transmit data for a certain interval of time. These faults lunch the error detection, fault location and recovery mechanism, during this time the component is unavailable for the system mission, this time degrades the system performance and may even lead to a dynamic failure if the delay exceeds a certain limit. In communication systems, transient faults usually affect the medium leading to transmission error. In this study we try to propose an approach to include the influence of transmission error in the reliability analysis of networked control system. Note that external interference occur stochastically in time, this will lead to variable delays on affected messages.

Our work can be seen as an extension of Barger et al work by including variable delays in the dependability study, and Jumel et al work by taking into account the real behaviour of dynamic systems. While this study can be extended to other networks, only one network is considered which is the Control Area Network (CAN).

The failure definition for control systems depends on the actual output of the system. It is no more a simple Boolean function on the components failure. Hence the need to calculate the actual output at each step to decide if the system is in a failure situation or not. This remark makes the analysis very difficult for networked control system, especially when delays are variable.

General approaches to reliability evaluation and fault tolerant design may resort to analytical methods or to experimental evaluations. In the latter case, fault injection techniques are commonly adopted, and can basically be grouped into simulation-based or hardware-based techniques.

The purpose adopted in this paper is to use a simulation model for the entire system. First we model all the components of the traditional control system (sensor, controller, actuator, process…), second we model the behaviour of the network and the whole system, and since we are interested on the transmission faults, we will add a third model to inject perturbations on the network. The goal is to evaluate the impact of external perturbations and additional traffic on the reliability of networked control systems.

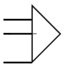
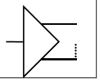
At the beginning of this paragraph we have shown why traditional technique like fault trees and block diagrams can't be used for our approach. A solution is to recur to dynamic models. The most popular are Markov processes, because of their numerous nice mathematical properties. In practice, the direct use of Markov processes has virtually been given up, to be replaced by some higher level formalisms (i.e. Stochastic Petri Net) that enable the automatic generation of a (potentially huge) Markov process. In our work we decided to work with Petri Net extensions which are well known in reliability evaluation, and well adapted to model complex systems (Malhotra and Trivedi, 1995).After the modelling phase variables to evaluate are declared by means of reward function (Malhotra and Trivedi, 1995).

3. STOCHASTIC ACTIVITY NETWORK

Stochastic activity networks (SANs) are a stochastic generalization of Petri nets. These models permit the representation of concurrency timeliness, fault-tolerance and degradable performance in a single model. They conserve all the modelling power of Petri nets, and in the same time give the possibility for a compact representation. Structurally, they consist of activities, places, input gates, and output gates. Activities which are similar to transitions in normal Petri nets are of two types: timed and instantaneous. Timed activities represent activities of the modelled system whose duration impact the performance of the modelled system. Instantaneous activities, on the other hand, represent system activities which occur immediately. Input gates and output gates control the enabling of activities and define the marking changes that will occur when an activity completes. SAN models have been used to evaluate a wide range of systems and are supported by several powerful modelling tools such as *UltraSAN* and *Möbius.* SAN is defined with the express purpose of facilitating unified Performance/dependability evaluation as

well as more traditional performance and dependability evaluation. Dependability evaluation is performed by defining a set of measures in the model.

Table 1. Graphical notations of the elements

Element	Place	Timed Activity	Instantaneus Activity	Input gate	Output gate
Graphical Notation	○	▮	│		

4. NETWORKS

A model is always a compromise between faithfulness and simplicity. A model can be very faithful and represents all the details, but on the other hand it can be intractable. In general assumptions are taken to simplify the model, while leaving it relatively faithful and easily tractable.

Many modelling levels of abstraction can be chosen, with different characteristics and precision. In particular, for network communications we may have:
• *Bit-accurate models* that reproduce the actual clock cycles in the network interfaces.
• *Message-accurate models* that represent network messages as atomic entities and abstract about detailed timings, while still explicitly representing the protocol implementation.
For our model we have chosen the message-accurate models; it is sufficient to our need and can express all the features of the networks (delays, collision, priorities, and errors).

4.1 Controller Area Network

CAN is a broadcast bus, with a priority-based access to the medium and non destructive collision resolution. Data to be transferred is encapsulated within communication objects called frame. Each frame contains an identifier (Id), unique to the whole system, which serves two purposes: assigning a priority for the transmission and allowing messages filtering upon reception. The following section presents the CAN behaviour in Fault Scenarios, and some related works.

In (Unruh, et al, 1989) the authors estimate the expected number of undetected transmission errors during lifetime of a vehicle is lower than 10^{-12}. This performance is the result of a very efficient error detection mechanism being used in CAN. This mechanism can be divided into: a message level like CRC code, and a bit level. At the bit level, the transmitter monitors the bus signals and detects errors. Each transmitting station observes the signal on the bus and thus, detects the difference between the bit sent and the bit received. If one error is discovered by at least one station using the above mechanisms, the current transmission is aborted by sending an error flag. This prevents other messages to accept this message. After sending the error flag, the sender automatically re-attempts transmission, and the message re-enters a scheduling list, and the one with the highest priority is selected and transmitted on the bus. The number of retransmissions is an important parameter. In the specification of CAN, this number is not defined. To calculate the worst response time, the authors in (Cheong,

2003) include the number of retransmission as a variable that characterizes the frame periodic. As cited below, the EMI can affect the medium and produce a transmission error. A detection mechanism is added to cope with these errors. Error recovery mechanisms take some time in detecting and retransmitting the affected message. This lost time is defined as an inaccessibility period where the network isn't ready to provide its service. This behaviour and its consequences are studied in (Rufino and Verissimo, 1995). A scheduling analysis of CAN is done by (Tindell, et al., 1995). Tindell extended his study to integrate the presence of faults, by adding an additional term error recovery function. The main disadvantage of the analysis is the use of a deterministic model to represent the fault occurrence, which is not realistic. A stochastic fault model which is closer to EMI behaviour and more realistic was proposed by (Navet, et al., 2000). Generalized Poisson Process is used to model the frequency of interference, as well as their duration (single errors and error bursts). In this work the authors introduced for the first time the WCDFP (worst case deadline failure probability) which provides a valuable knowledge on the system's reliability. This information is very important when dealing with a hard real time system where losing a message can lead to a global failure of the whole system.

As it was mentioned early, in this study we assume that transmission errors due to interferences on the medium are always detected and directly proclaimed by the error recovery mechanisms.

We assume also that messages can be lost if one of these conditions is satisfied:
1) the maximum number of retransmission (Cheong, 2003) for this message is reached,
2) a new message of the same type is ready to be sent (arrival of a new message always deletes the old one.)

4.2 Network model

The Network model is the central model, all other models are linked to it by sharing places (Figure 2). It represents a model of a CAN network. This model takes account of the CSMA/AMP strategy used in CAN that is mainly the management of the priorities. Lines at the left represent station linked to the network. The model can be easily modified to support new components by adding one line to each component.
TM place represents the transmission medium, the medium is idle if there is a token inside, and otherwise the medium is busy. The CSMA/AMP *inputcase* gives the access to the medium to one station; it is done by assigning priority to the places. The activity *on_ the_medium* is fired to indicate the beginning of a message transmission. If an interference occurred (presence of a token in *IN*), an error is produced, transmission is aborted, and a token is removed to the error place which will activate the model *error_mechanism*, this model will send an error frame on the network.

As we mentioned before this model is linked to other models, like sensors, controllers, actuators, and other components. These components will send and receive messages over the network. For a running time, some performance parameters on the network can be evaluated from this model like:
- the sum and the average time delays for each node on the network,
- the efficiency of the network, defined as the ratio of the total transmitting time to the time used to send messages, including queuing time, blocking time, etc.,
- network utilization defined by the ratio of the total time used to transmit data and the total running time,
- The ratio of lost messages for each node on the network…

These parameters were defined by (Lian et al, 2001) to analyze and compare three control networks: Ethernet, ControlNet and DeviceNet.

Note that the only considered faults are the perturbations on the network. The *fault_injection* model injects faults representing an EMI via the medium. We consider that faults have a fixed duration, time between faults is assumed to be exponentially distributed. Since little is known about the frequency of transient faults on local area networks, we will vary their rate occurrence and evaluate their influence.

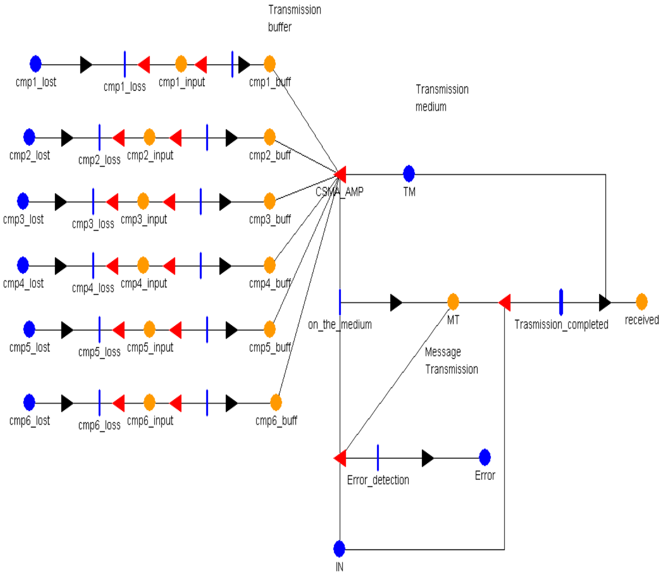


Fig. 2 Network model

5. CASE STUDY

All above reliability for networked control systems can't be evaluated in an analytical way. We propose to evaluate it by Monte-Carlo simulation. The method proposed is described with an example of an NCS with three independent loops that are closed over a control network.

The process controllers, which execute PID algorithms, are well-designed respectively based on different timing parameters. Before the evaluation, we must define the failure definition of a control loop. We based our failure definition

on thresholds of the magnitude of the control error, i.e., the difference between the reference output[1] and the actual value.
Failure test:
 If (|ref (t)-actual (t)| > bound)
Then 'detect a failure situation'

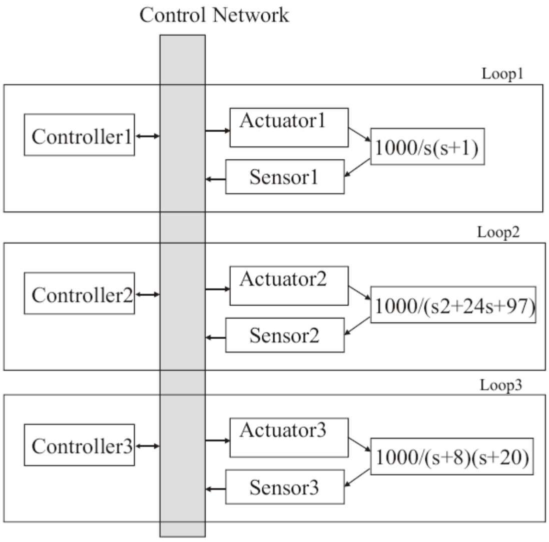


Fig. 3. NCS with three control loops

We evaluate the reliability of the first loop by changing two parameters: the priority given to the first loop components and the perturbation fault rate.

All the results are obtained by simulation under Möbius tools (Deavours, et al,. 2002) with a confidence interval of 0.1 and a confidence level of 0.95.

Case 1: higher priority attributed to loop_1 components.

Table 2. Priority assignment

component	period	Priority
Sensor1	0.01	1
Controller1	Event-driven	2
Sensor2	0.011	3
Controller2	Event-driven	4
Sensor3	0.012	5
Controller3	Event-driven	6

Figure.4 shows the reliability curve for loop_1, under priority assignment given in Table 2, and for two different values for perturbation fault rate.

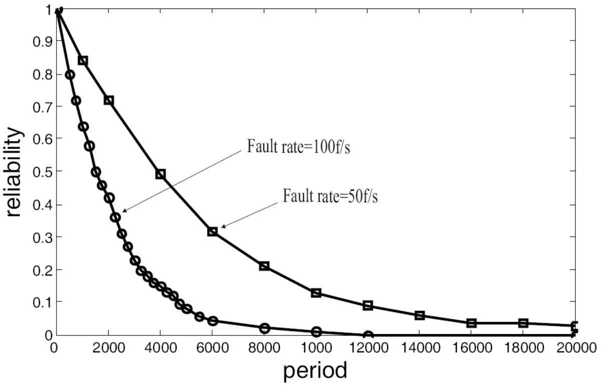


Figure. 4 case 1 reliability

Case 2: higher priority attributed to loop_2 components.

Table 3. priority assignment

component	period	priority
Sensor1	0.01	3
Controller1	Event-driven	4
Sensor2	0.011	1
Controller2	Event-driven	2
Sensor3	0.012	5
Controller3	Event-driven	6

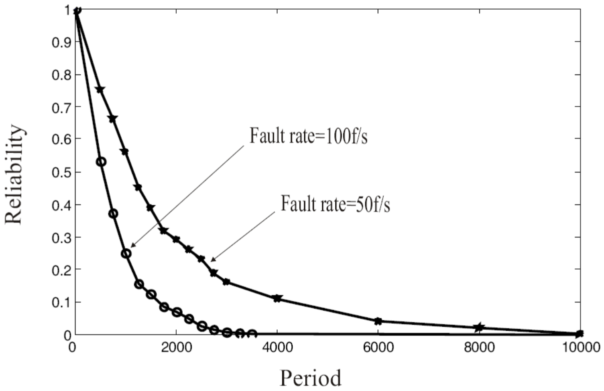


Figure. 5 case 2 reliability

Figure.5 shows the reliability curve for loop_1, under priority assignment given in Table 3 and for two different values of the perturbation fault rate. To understand the results, we evaluate some performance on the network. Table 4 summarizes network parameter in each case. Perturbation on network decrease the network performance, leading to more delay, and high loss probability. For the same value of fault rate results are different, in fact due to the priority assignment in case 2, loop-1 messages are delayed by the higher priority messages of loop_2.

[1] Outputs without perturbations on the network are called reference outputs.

Table 4. Network performance

		Average delay Loop_1	efficiency	utilization	Lost probability
Case1	λ_{tf}=75	0.0013	0.6670	0.873	0.0041
	λ_{tf}=100	0.0014	0.6181	0.9706	0.0071
Case2	λ_{tf}=75	0.00132	0.6611	0.8738	0.0044

6. CONCLUSIONS

The In this paper, we have presented an environment to assess the impact of the transmission errors on the reliability of a NCS. The approach consists in modelling the functional behaviour of classical control system components, and both functional and dysfunctional behaviour of the network. We base our definition of system failure on thresholds of the magnitude of the control error. Thanks to our environment we were able to predict how the transmission errors on the network may affect the system reliability. Special focus was given to the network; all the other components are considered as free fail.

One extension will be the integration of faulty components, with the possibility to analyse the consequences on the failure of the system of various sequences of related or unrelated faults. The possibility to introduce variable in the modelling phase and the ease of joining atomic model in Möbius give the possibility to make a library of models ready to be use in other studies. Implementing this library and adding other models is one of our perspectives.

REFERENCES

Askerdal, O., M. Gavert, M. Hiller, N. Suri, A Control Theory Approach for analysing the effects of data errors in safety-critical control system. Proceedings of the Pacific Rim International Symposium on Dependable Computing. 2002

Barger, P., J.M. Thiriet, M. Robert. Safety analysis and reliability estimation of a networkedcontrol system In: SAFEPROCESS 2003, Washington, D.C, USA, 2003.

Branicky M S, Liberatore V, Philips S M. Networked controlsystem co-simulation for co-design. In: Proceedings of the American Control Conference. Denver, Colorado, USA, 2003: 3341-3346.

Cheong SO, J.K (2003). Delay Modelling And Controller design for networked Control systems. Master of applied thesis. Department of Electrical and Computer Engineering University of Toronto.

Dutuit, Y., E. Chatelet, J.P. Signoret, and P. Thomas. Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases. Reliability Engineering & System Safety, Vol 55, Pages:117-124, 1997

Jumel, F., K. Gorday, and I. Augé-Blum, Safety Evaluation of controlled system distributed on TTA Architecture, International Conference on Advanced in Vehicule Control and Safety (AVCS'04), Italy, October 2004

Lian, F.L., R. James, M.Tilbury., 2001. Performance evalaution of control networks, Ethernet, ControlNet, and DeviceNet. IEEE Control systems magazine February 2001.

Malhotra, M. and K. Trivedi (1995). Dependability Modelling Using Petri-Nets, *IEEE Transaction on reliability*, Vol. 44, No. 3, pp. 428-440.

Moncelet, G., S. Christensen, H. Demmou, M. Pauldetto and J. Porras. Dependability evaluation of a simple mechatronic system using coloured Petri nets In: Workshop on Practical Use of Coloured Petri Nets and Design CPN (Jensen, K.), pp. 189-198. Aarhus University, Aarhus, Denmark. 1998.

Navet, N., Y. Song and F. Simonot (2000). Worst- Case Deadline Probability in Real-Time Applications Distributed over Controller Area Network. In: Journal of systems Architecture, Vol. 46, No. 1, pp. 607-617.

Rufino, J. And P. Verissimo (1995), A study on the inaccessibility characteristics of the controller area network, Proceeding of the 2nd International CAN Conference .

Sanders W.H., John F. Meyer. Stochastic activity networks: formal definitions and concepts, *Lectures on formal methods and performance analysis: first EEF/Euro summer school on trends in computer science,* pp 315-343. Springer-Verlag New York, Inc., New York, NY. 2002

Soglo A.B. and Y. Xianhui, Networked Control System Simulation Design and Its Application, in TSINGHUA SCIENCE AND TECHNOLOGY ISSN 1007-0214 05/16 pp287-294 Volume 11, Number 3, June 2006

Unruh, J. H.J. Mathony and K.H. Kaiser (1989). Error detection analysis of automotive communication networks, Technical report, Robert Bosh GmbH.

Zhang W, Branicky M S, Philips S M. Stability of networked control systems. *IEEE Control Systems Magazine*, 2001, 21(1): 84-99.