Proceedings of Korean Nuclear Society Autumn Meeting
Seoul, Korea, October 1998

CPN Based Fault-Tolerance Performance Evaluation of Fieldbus for KNGR NPCS Network

Hyun Gi Jung and Poong Hyun Seong

Dept. of Nuclear Eng., Korea Advanced Institute of Science and Technology
373-1 Ku-song Dong, Yu-song Gu, Taejon 305-701, Korea

ABSTRACT

In contrast with conventional Fieldbus researches which are focused on real time performanc ignoring fault-tolerant mechanisms, the aim of this work is real-time performance evaluation of the system including fault. Because the communication network will be applied to Next Generation NPP, maintaining performance in presence of recoverable fault is important. To guarantee this in NPP Control Network, we should investigate the time characteristics of the target system in case of recoverable fault. If the time characteristics meet the requirements of the system, the faults will be recovered by Fieldbus recovery mechanisms and the system will be safe. But, if time characteristics can not meet the requirements, the faults in the Fieldbus can propagate to system failure. For this purpose, we classified the recoverable faults, made the formula which represents delays including recovery mechaisms and made simulation model. We appied the simulation model to KNGR NPCS with some assumptions. The outcome of the simulation is reallistic delays of the fault cases which have been classified. From the outcome of the simulation and the system requirements, we can calculate failure propagation probability from Fieldbus to outer system.

1. Introduction

The development of the computer and communication technologies is strongly influencing the progress of process control and manufacturing automation systems. Advanced automation systems require interconnection of computer-based systems and intelligent devices. This systems provide flexibility in design and operation, ease of maintenance, diagnostics and monitoring. In this advanced systems, networks make it possible to exchange data among distributed intelligent devices[1]. In NPP(Nuclear Power Plant), network will be used for this purpose. The best example of the network application is CIM(Control Integrated Manufacturing) model. In CIM model, there is hierarchy composed of several sub-networks. The Fieldbus is lowest level in this hierarchy. Fieldbus provide data communication among sensors, actuators, controllers, PLCs, etc. Therefore, Fieldbus must performs as a real-time communication system.

In real-time systems, it is also failure if the system do not meet time requirements[2]. It is the reason why the delays in real-time system are very important parameters of performance. If time characteristics can not meet the requirements, the faults in the Fieldbus can propagate to system failure. In safety critical system, it is important to maintain performance in presence of recoverable fault.

In this work, as the target system is KNGR(Korean Next Generation Reactor) NPCS(NSSS Process Control System), the fault classification and recovery mechanisms are influenced by the system topology. For example, the group controllers in NPCS connect two token rotation path playing the role of bridge. In general meaning of communication, loop controllers play the role of node.

To evaluate fault-tolerant performance of Fieldbus, we investigate the time characteristics of the target system in case of recoverable faults. To do this, In chapter 2 we present the definition of LCD(Loop Communication Delay) and relationship between LCD & system response time, classify the recoverable faults and calculate the maximum delays of the recoverable failure cases. Simulation model to show the realistic fault situations and the outcome and the meaning of the result are shown in chapter 3. Finally the conclusion is presented in chapter 4.

2. Recoverable Faults and Max Communication Delays

Among several Fieldbuses, IEC/ISA Fieldbus was proposed as international standard[3]. The Profibus which is German standard and FIP which is French standard are the reference model of IEC/ISA Fieldbus. The focus of this research is the frame work which provides the methodology to find time-delay of recoverable fault cases. So, we selected the international standard as a reference. The structure of NPCS is shown in Figure 1.

2.1 Definition of LCD and Relationship Between LCD & System Response Time

We define two concepts, TCD(Task Communication Delay) and LCD(Loop Communication Delay). This definitions enable to understand the relationship between communication delay and system response time more clearly.

- Communication Delay : Time between creation of information to be delivered in one node and use of the information in another node
- TCD : Sum of communication delays for one task that has some meaning in application layer
- LCD : Several tasks make up one functional role in a system. LCD is sum of the task communication delays needed to perform one functional role

$$LCD=\sum_{k=1}^{\#of\ tasks}(TCD)_k$$

- Response Time of a System : Time which is needed to perform one function, if other conditions are ready, the time between action signal and system response

Response time = Total Processing Time + Loop Communication Delay

$$ResponseTime=\sum_{i=1}^{\#of\ processes}(T_{process})_i+\sum_{k=1}^{\#of\ tasks}(T_{task})_k$$

Therefore, if we can find the total processing time and LCD, it is possible to calculate the system response time which is functional concept such as the time needed to start actuator or the time needed to monitor the plant parameters. There is various failure cases which is not recoverable. In case of recoverable fault, if the calculated system response time is over the required value, we say that the system will fail. But, if the system response time including recovery mechanism is not over the requirements of the system, the system will not fail. So, it is necessary for system designers to know the fault-tolerant characteristics of the Fieldbus.

2.2 Classification of Recoverable Failure Cases (Recoverable Faults)

Generally speaking, communication failure cases can be divided in 3 categories, communication failure, node failure and link failure. The communication failures are the failures which can occur in data transmission such as bit errors caused by EMI, RFI, etc. This transient faults can be recovered by retransmission. Node failure is the case that communication node which can be communication object(sender of receiver) do not work. The case when the bridges or network cables is not normal situation is Link failure.

Communication failures can be recovered by retransmission. When the node which is not communication object fail, other nodes can communication by recovering the new logical ring except the failed node. But, if the failed node is the communication object itself, it is impossible to recover in fieldbus protocol. Therefore recoverable node failure case is node failure which is not communication object or have hot stand-by recovery mechanism. Link failures can occur when cable is cut or bridge do not work. The connection problem can not recoverable, but the bridge which have hot stand-by mechanism can be recovered[3],[4].

Table 1 is the classification of recoverable failure cases(recoverable faults) and each case is labeled such as A,B,C,D,DB,DC according to recovery mechanism. We will use this label in Max-TCD analysis in next chapter.

2.3 Max-Communication-Delay Analysis

2.3.1 Delay Parameters

- TRT(Token Rotation Time) : the time it takes a token packet to travel around network one time
- TTT(Token Transmission Time) : the time needed to pass token to next node in logical ring
- T_trans (Transmission Time) : the time it takes one node to transmit a physical signal to another node
- T_cp (Communication Processing Time) : delays within PhL/DLL interface
- T_slot (solt time) : worst case delays within media, PhL and PhL/DLL interfaces for one task i.e. worst case time any station must wait for an immediate ACK

  T_slot = 2*(T_trans+T_cp)
- T_process (Processing Time) : the time needed for one node to process, except communication parts i.e. delays within CPU, Memory, internal bus, etc..
- T_reaction (Reaction Time) : the interval between for one node to obtain token and to sending physical output signal

  T_reaction = 2*T_cp + T_processing
- T_timeout (Timeout Time) : waiting time for one node to confirm next node's failure

  T_timeout = 3*(T_slot+T_process) + △δ(safety factor)
- T_networkout (Network Time out) : setting value in each node which is used for a node to monitor the activity of network

  T_networkout > T_timeout
- T_turnover (Address Turnover Time) : address turnover time in hot-standby
- T_hotbit (Hot Bit Deliver Time) : time to recognize main node failure

Recoverable fault description	Label	Category	Recoverable fault description	Label	Category
Bit error, EMI, RFI, etc	A	CF	<- All are recoverable		
Not communication object Fail without token No hot-standby mechanism	B	NF	Communication object Fail without token No hot-standby mechanism		Can not recover
Not communication object Fail with token No hot-standby mechanism	C	NF	Communication object Fail with token No hot-standby mechanism		Can not recover
Not communication object Fail without token Have hot-standby mechanism	DB	NF	Communication object Fail without token Have hot-standby mechanism	D	NF, LF
Not communication object Fail with token Have hot-standby mechanism	DC	NF	Communication object Fail with token Have hot-standby mechanism	D	NF, LF

Possible category : Communication Failure-CF, Node Failure-NF, Link Failure-LF

Table 1. Classification of recoverable failures

2.3.2 Recovery Mechanisms & Max-TCD

This chapter describe the recovery mechanisms and the TCDs. The formulas of case by case TCD calculation is presented. That is, when the recoverable failures(case A to DC) occur, the TCD is calculated like those below. This formula was made up by referencing ISA standard[3], Modbus+ Manual[4] and other papers[5], [6].

- A : timeout -> retransmission
  T_delay_a = TRT + 2T_cp + (T_reaction+2T_trans+ △δ) + T_slot
  = TRT + 2T_cp + 2T_slot + T_process + △δ

- B : node timeout -> node out (new ring without failed node) -> next node have token
  T_delay_b = TRT + 2T_cp + T_timeout + T_slot

- C : network timeout -> node out (new ring without failed node) -> lowest address have token
  T_delay_c = TRT + 2T_cp + T_timeout +TRT + T_slot

- D : G/C fail -> node out -> Turnover -> join
  T_delay_d = TRT + 2T_cp + 1/2T_slot + T_hotbit + T_slot + T_turnover + [#of remained task*(TRT+T_slot+T_process) + #of remained address sequence*(T_slot)] +TRT +1/2T_slot

- DB : G/C fail -> node out -> next node have token
  T_delay_db = TRT + 2T_cp + T_hotbit + T_slot + T_slot

- DC : G/C fail -> node out -> lowest address have token
  T_delay_dc = TRT + 2T_cp + T_hotbit + T_slot + TRT +T_slot

If we know the max-value of the parameters, we can calculate the max-response-time of recoverable fault cases. But, because several parameters such as TRT, T_slot, T_cp and T_process are random number, we can guess only the min and max values. The parameters such as number of G/C, L/C, T_timeout, T_networkout and T_hotbit are determined by designer. Therefore, even though the design plan exist, we can not get the data of the response times. The profile of the response time in fault case can be the important data of system safety. For example, it enables to find the failure propagation probability from Fieldbus to outer system. to determine wether the system including Fieldbus is designed considering fault-tolerant functions of Fieldbus or not.

3. CPN Simulation Analysis

CPN is good graphical language for system V/V[7][8]. CPN have good computerized tool support, Design CPN. CPN make it easy to verify th correctness of the modeling. By hierarchical structure, it is easy to apply given sub-model to another system analysis. As we focus on time delay, we used time label in Design CPN.

The modeling scope is the Fieldbus which is composed of 1-token-rotation path. In fact, NPCS have several token rotation path structure. The longest communication distance is composed of 3 token rotation path, across the G/C (we call : 3-path-communication). Even though 3-path-communication is more complex and have longer delays, it can be made up of 1-path-communication sub-models. As a matter of fact, TCD can be from 1 to 3-path-communication-delay.

In this model, it is possible to select the failure cases. The inputs of this model are many tokens labeled 'time = 0'. The outputs are tokens which have difference delay time. The hierarchical structure is represented in Figure 2. The main-models are represented in Figure 3. The other sub-model is not shown because of limited space.

If we assume the parameters as Table 2[3].[4]. the outcome profile of 1000 cases is shown in Figure 4. From the polynomial regression, we can get the relationship between delay times and number of cases.

$$Y = -0.0341 + 0.66764X - 0.00767\ X^2 + (3.48354 * 10^{-5})\ X^3 - (5.44507 * 10^{-8})\ X^4$$

where, Y is number of cases and X is time delay.

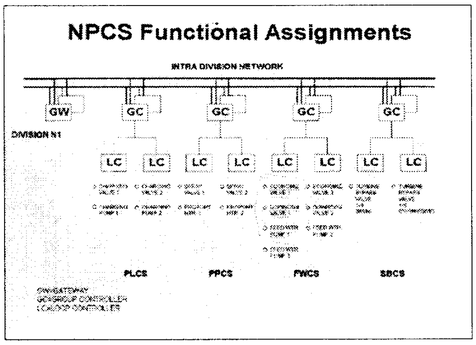
In this case, if the requirement of system is given, such as 300ms, we can calculate the probability of the failure propagation to outer system. From the TCD calculation formula, we can calculate the min and max delays, 25ms and 320ms.

$$\text{Failure Propagation Probability} = \frac{\int_{300}^{320} Ydx}{\int_{25}^{320} Ydx} = 0.01816$$

Therefore, we can say that if the failure case D is occur in 1-path-communication process and the requirement of the TCD is 300ms, the probability that the failure propagate from Fieldbus to outer system is 1.8%.

Parameter	Assumed time(ms)	Parameter	Assumed time(ms)
TRT	2-16	T_slot	1-4
T_cp	0.5-2	T_process	10
T_reaction	15	T_timeout	45
T_networkout	50	T_hotbit	1
T_turnover	10	T_trans	0
# of G/C	4	# of L/C per G/C	8

Table 2. Assumed Parameters



NPCS Functional Assignments

Figure 1. NPCS Scheme

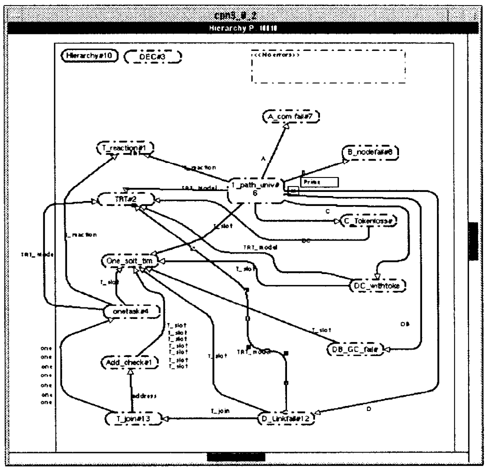


Figure 2. CPN Hierarchy Page

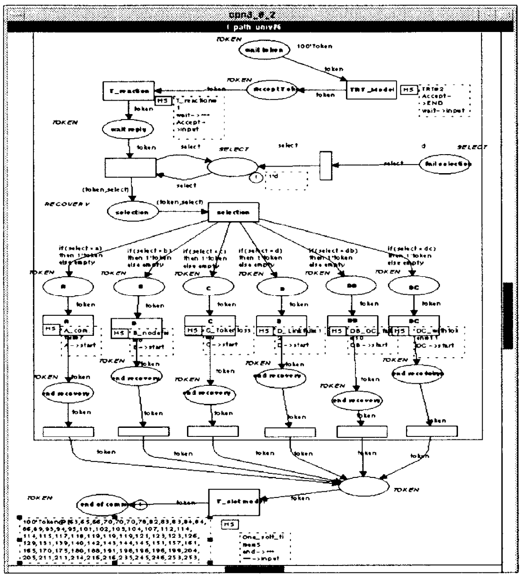


Figure 3. CPN Main Page

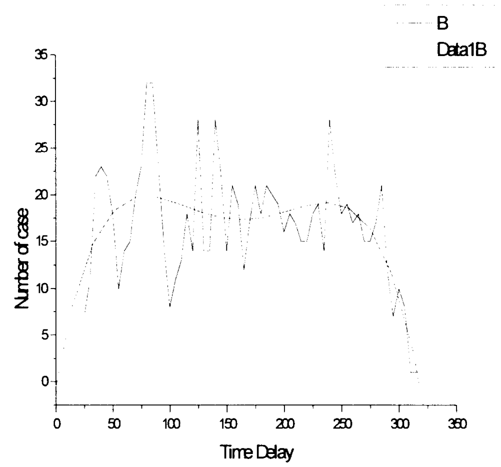


Figure 4. Case D Simulation Output

4. Conclusion

To find the delays of recoverable fault cases in general Fieldbus protocol, we defined TCD, LCD and several parameters. we classified recoverable faults in Table 1. and made formula to calculate recovery delays. Because of random variables in this formula, we use CPN simulation model to find realistic delays caused by recoverable faults. The outcome of this, analysis can be used to calculate failure propagation probability.

Only 1_path_communication model is considered in this research, but the sum of TCDs leads LCD. Therefore we can calculate the response time of the system. Before prototype testing, the response time enable for designer to estimate the performance of the planing system.

References

1. Seung Ho Hong and Seong Geun Lee, **Performance Analysis of the Data Link Layer in IEC/ISA Fieldbus by Simulation Model**, Proceeding of the 1996 IEEE Conference of Emerging Technology and Factory Automation V2. November 96.
2. Michel Banatre and Peter A Lee , Hardware and Software Archtectures for Fault Tolerance, pp 237-249 : Farnam Jahanian, **Fault-Tolerance in Embeded Real-Time Systems**.
3. ANSI/ISA-dS50.02-1997 **Fieldbus Standard for Use in Industrial Control Systems, Part 4 : Data Link Protocol Specificatio**n, ISA 1998
4. AEG Schneider automation, **Modbus Plus Network Planing and Installation Guide** 890 USE 100 00 Version 2.0
5. Andrew S. Tanenbaum, Computer Networks, Third Edition, Prentice Hall, 1997.
6. Theresa A. Baker, **Modbus Plus Response Time Analysis of Layered Network**, Group Schneider

7. Bernard Berthomieu and Michel Diaz, **Modeling and Verification of Time Dependent Systems Using Time Petri Nets**, IEEE Transaction on Software Engineering, VOL 17, NO.3, March 1991.
8. Kurt Jensen, **Coloured Petri Nets**, Volume 1, Second Edition, 1997.
9. Seong Ho Hong, **Performance Evaluation of Fieldbus Networks in the Distributed Computer Control of Power Generation Systems**, IEEE International Symposium on Industrial Electronics, July 97