Journal of the Korean Nuclear Society
Volume 33, Number 1, pp.1 ~ 11, February, 2001

Fault-tolerance Performance Evaluation of Fieldbus for NPCS Network of KNGR

Hyun Gi Jung and Poong Hyun Seong

Korea Advanced Institute of Science and Technology
373-1 Kusong-Dong, Yusong-Gu, Taejon 305-701, Korea

(Received January 22, 1999)

Abstract

In contrast with conventional fieldbus researches which are focused merely on real-time performance, this study aims to evaluate the real-time performance of the communication system including fault-tolerant mechanisms. Maintaining performance in presence of recoverable faults is very important in case that the communication network is applied to a highly reliable system such as next generation Nuclear Power Plant (NPP). 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. If the time characteristics can not meet the requirements, the faults in the fieldbus can propagate to the system failure. In this study, for the purpose of investigating the time characteristics of fieldbus, the recoverable faults are classified and then the formulas that represent delays including recovery mechanisms are developed. In order to validate the proposed approach, we have developed a simulation model that represents the Korea Next Generation Reactor (KNGR) NSSS Process Control System (NPCS). The results of the simulation show us the reasonable delay characteristics of the fault cases with recovery mechanisms. Using the simulation results and the system requirements, we also can calculate the failure propagation probability from fieldbus to outer system.

Key Words : fieldbus, fault-tolerance, colored petri net, NPCS

1. Introduction

The progress of the computer and communication technologies is strongly influencing that of process control and manufacturing automation systems. Advanced automation systems require interconnection of computer-based systems and intelligent devices. These systems provide ease of maintenance, diagnostics and monitoring as well as flexibility in design and operation. In these advanced systems, networks make it possible to exchange data among distributed intelligent devices[1]. The best example of the network application is Control Integrated Manufacturing (CIM) Pyramid Model. In CIM Pyramid Model, there is a hierarchy which is

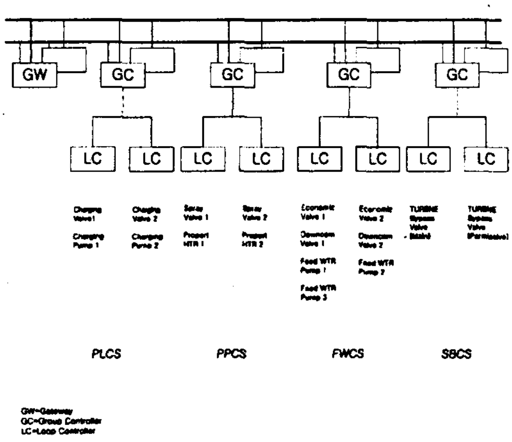

Fig. 1. NPCS Scheme

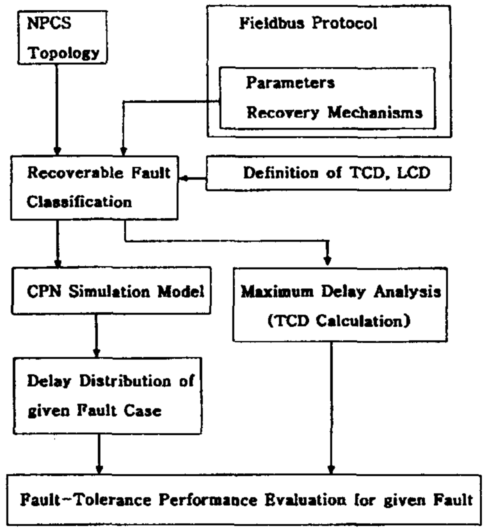

Fig. 2. The Schematic Diagram of Fault-Tolerance Performance Evaluation

composed of several sub-networks. The fieldbus is a network of the lowest level in this hierarchy. Fieldbus provides data communication among sensors, actuators, controllers, Programmable Logic Controllers (PLCs), etc. Therefore, fieldbus must operate as a real-time communication system.

In Nuclear Power Plant (NPP), network will be used for data communication among intelligent field devices. The data communication among field devices in NPP is required to meet real-time requirements. In real-time systems, it is considered to be a failure that the system do not meet the time requirements[2]. This is the reason why the delays are very important in real-time system performance. If the time characteristics can not meet the time requirements, the faults in the fieldbus can propagate to system failure. Safety critical system, in particular, it is required to be more reliable and fault-tolerant. Therefore, it is important to maintain acceptable performance in presence of recoverable faults.

In this study, the evaluation target system is NSSS Process Control System (NPCS) in KNGR, which is currently in the design stage. The fault classification and recoverable fault recovery mechanisms are influenced by the system structure, the connection among nodes. In the NPCS, there are many Group Controllers (G/C) and Loop Controllers (L/C) as shown in Figure 1. The G/Cs in NPCS connect two token rotation paths playing the role of bridge. On the other hand, L/Cs play the role of nodes.

The schematic diagram outlining this study is shown in Figure 2. In order to evaluate fault-tolerant performance of fieldbus, we investigated the time characteristics of the target system in view of recoverable faults. As shown in Figure 2, the communication structure of NPCS and fieldbus protocols are used to classify the recoverable faults. Task Communication Delay (TCD) and Loop Communication Delay (LCD) are defined to show the relationship between communication delay and system response time. From the classification of recoverable faults, the maximum delays of the recoverable failure cases are calculated in chapter 2. A Colored Petri Net (CPN) simulation model is developed to show the reasonable delays of recovery mechanisms of the recoverable faults. The outcome of the simulation can be handled to represent the distribution of the delays. The results have the meaning of 'fault-tolerance performance evaluation' as described in chapter 3.

2. Recoverable Faults and Max Communication Delays

Among several fieldbuses, IEC/ISA Fieldbus was proposed as an international standard[3]. The Profibus which is German standard and the FIP which is French standard are the reference models of IEC/ISA Fieldbus. The international standard, IEC/ISA Fieldbus, is selected as a reference model in this research, focused on establishing the framework which provides the methodology to find time-delay of recoverable fault cases and to find profile of the delays. The profile enable us to evaluate the recovery ratio of the recoverable faults.

In section 2.1, several definitions will be presented. The relationship between communication delays and system response time will be described more clearly by the definition of LCD and TCD. In section 2.2, the classification of fault cases is described. Several parameters and Max-TCD calculation will be descused in section 2.3.

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

We define two kinds of time delays, TCD and LCD. These definitions enable us to understand the relationship between communication delay and system response time more clearly.

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

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

- Response Time of a System : The time between action signal and system response

$$ResponseTime = \sum_{i=1}^{\#of\ processes} (T_{process})_i + \sum_{k=1}^{\#of\ tasks} (TCD)_k \quad (2)$$

Therefore, if we can find out 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.

In this study, fault-tolerant performance of NPCS communication network means the possibility that the recoverable faults in fieldbus of NPCS are recovered without propagating to outer fieldbus. If there is a non-recoverable fault, the fault must propagate to outer system failure. Therefore, the non-recoverable fault has no meaning in the fault-tolerance performance evaluation.

Token is a packet that gives a node an authority to start communication. In one token rotation path, only one node can have a Token Packet(PAK). The 'Token Rotation Path' means a virtual ring that is constructed by nodes. Only one token can exist in this group of nodes.

Some definitions of path_communication and path TCD are shown as follows:

1_path_communication : a communication between two nodes that are in the same token rotation path.

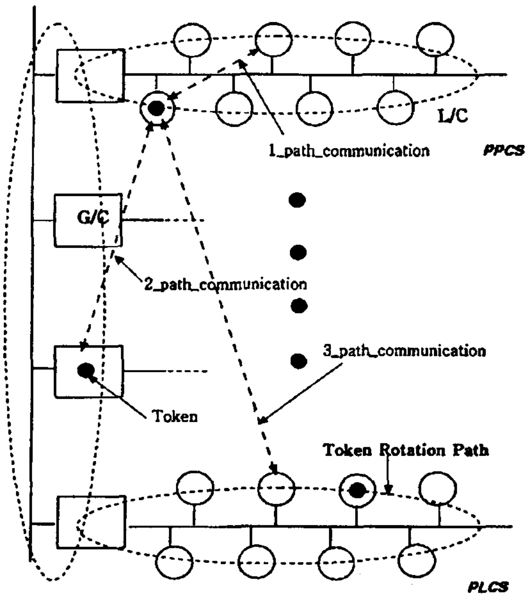

Fig. 3. The Token Rotation Path and The Path Communication

2_path_communication : a communication between two nodes that are in the adjacent two token rotation paths.

3_path_communication : a communication between two nodes which are in the different two token rotation paths and the communication process is performed across three token rotation paths.

n_path TCD : a TCD that is in n_path_communication process, where n is 1, 2, or 3

The relationship among the path_communication and token rotation path is shown in Figure 3. Because the TCD can be one of the three path communication cases, we should simulate these TCDs with different models such as 1_path TCD simulation model, 2_path TCD simulation model and 3_path TCD simulation model.

There are three kinds of TCD (1_path, 2_path and 3_path) in NPCS structure. In Figure 1, the communication between L/Cs in Pressurizer Pressure Control System (PPCS) is the example of

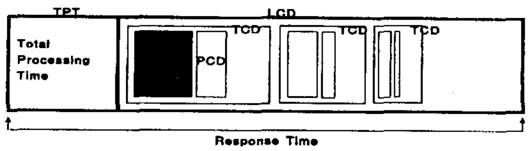

Fig. 4. TCD and System Response Time

1_path_communication. The communication between L/C and G/C in the PPCS is the example of 2_path_communication. The communication between L/Cs in PPCS and Pressurizer Level Control System (PLCS) is the example of the 3_path_communication. These concepts are also shown in Figure 3.

From the definition of LCD, the LCD can be evaluated by calculating TCDs as shown in Figure 4. TCD is composed of 1_path TCDs. Therefore, only 1_path TCD is considered in the simulation model in chapter 3.

2.2. Classification of Recoverable Failure

In general, failures in communication can be divided into three categories such as communication failure, node failure and link failure. The communication failure is the failure in data transmission such as bit error caused by Electro Magnetic Interference (EMI), Radio Frequency Interference (RFI), etc. Node failure is the case that some communication nodes, which can be communication object(sender or receiver), are out of order. The cases where the bridges or network cables are not in the normal state are called link failure.

Communication failures can be recovered by retransmission. In case of node failure, however, the situation is quite different. When the node, which is not a communication object, fail, other nodes can communicate by recovering the new logical ring except the failed node. On the other hand, if the failed node is the communication object itself, it is impossible to recover the fault

Table 1. Classification of Recoverable Failures Recoverable Fault Description

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	B	NF	Communication object Fail without token No hot-standby		Can not recover
Not communication object Fail with token No hot-standby	C	NF	Communication object Fail with token No hot-standby		Can not recover
Not communicatio object Fail without token Have hot-standby	DB	NF	Communication object Fail without token Have hot-standby	D	NF, LF
Not communication object Fail with token Have hot-standby	DC	NF	Communication object Fail with token Have hot-standby	D	NF, LF

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

with fieldbus protocol. In case that the failed node has hot-standby mechanism, however, it can be recovered by the hot-standby mechanism. Therefore, the recoverable node failure is the failure of the nodes which are not communication objects or have hot-standby recovery mechanism. Link failures can occur when the communication cable is cut or when the bridge is out of order. The bridge problems, however, can be recoverable case that the bridge that has a hot-standby mechanism[3][4].

Table 1 shows the classification of recoverable failure cases(recoverable faults) and each cases are labeled as A, B, C, D, DB, or DC. This label will be used in Max-TCD analysis in section 2.3.

2.3. Max-Task Communication Delay Analysis

As mentioned in section 2.1 equation (1), LCD is calculated from TCDs. In other words, if it is needed to calculate the response time of an arbitrary functional response of NPCS, the sum of the processing times and the TCDs should be calculated in advance.

Several parameters for calculating TCD will be introduced in section 2.3.1. These parameters are refered from IEC/ISA Fieldbus Standard and other Fieldbus Standards[3][4][6]. In these parameters, There are random variables with specific ranges such as TRT, T_trans, T_cp, T_reaction and T_turnover. The other parameters are variables to be determined by system designer.

The recovery mechanisms of the failure cases and the formulas to calculate the Max-TCDs of the failure cases will be introduced in section 2.3.3. In the ranges of the delay parameters, maximum value will be used in Max-TCD calculation.

2.3.1. Delay Parameters

- TRT (Token Rotation Time) : the time it takes a token packet to travel around network one time

- 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 Physical Layer (PhL)/Data Link Layer (DLL) interface
- T_slot (slot 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 acknowledgement

$$T\_slot = 2*(T\_trans+T\_cp)$$

- T_process (Processing Time) : the time needed for one node to process, except communication delay 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

$$T\_reaction = 2*T\_cp + T\_process$$

- T_timeout (Timeout Time) : waiting time for one node to confirm next node' s failure

$$T\_timeout = 3*(T\_slot+T\_process) + \Delta\delta \text{ (safety factor)}$$

- 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 Delivery Time) : time to recognize main node failure

2.3.2. Recovery Mechanisms and TCD

This section describes the recovery mechanisms and the TCDs. The formulas of the TCD calculations are presented. The recovery mechanisms shown in this section concern 1_path TCD (i.e. the TCD that is composed of one token rotation path). Actually, the other TCDs such as 2_path TCD and 3_path TCD can be represented by 1_path TCD. The recovery mechanisms of 2 or 3_path TCDs will be the composition of the recovery mechanisms of 1_path TCD. Therefore, the recovery mechanisms and delay calculation formulas of 1_path TCDs are introduced in this section. The relationship between Max-TCD and maximum system response time will be presented in the next section.

The formulas were made up by referencing ISA Standard[3], Modbus+ Manual[4] and the other researches[5], [6].

Case A is the communication failure situation. The fault of Case A can be recovered by retransmission.

- A : timeout -> retransmission

$$\begin{aligned} T\_delay\_a &= TRT + 2T\_cp + (T\_reaction+ 2T\_trans+\Delta\delta)+T\_slot \\ &= TRT + 2T\_cp + 2T\_slot + T\_process + \Delta\delta \end{aligned} \quad (3)$$

Case B can be recovered by constructing the new logical ring.

- B : node timeout -> node out (new ring without failed node) -> next node have token

$$T\_delay\_b = TRT + 2T\_cp + T\_timeout + T\_slot \quad (4)$$

Case C can be recovered by constructing the new logical ring. Because the node failed with token, new token must be generated.

- C : network timeout -> node out (new ring without failed node) -> lowest address have token

$$T\_delay\_c = TRT+ 2T\_cp + T\_networko +TRT + T\_slot \quad (5)$$

Table 2. Assumed Parameters

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	39	T_trans	0
# of G/C	4	# of L/C per G/C	8

Table 3. Max-TCDs

Case of fault	Max-TCD [ms]	Note
A	$38 + \Delta\delta$	
B	69	
C	90	
D	366	Max value of #of Task and # of Address Sequence is '8'
DB	29	
DC	45	

Case D can be recovered by actuating hot-standby mechanism and rejoining in the logical ring. In the join process, it is needed to handle the task queue.

- D : G/C fail -> node out -> Address Turnover -> join(remained tasks handling and 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 (6)

Case DB can be recovered by constructing the new logical ring. In case of the node which has hot-standby mechanism, the conforming of the node failure situation is performed by hotbit(T_hotbit).

- DB : G/C fail -> node out -> next node have token

T_delay_db = TRT + 2T_cp + T_hotbit + T_slot + T_slot (7)

Case DC can be recovered by constructing the new logical ring. This case also conforms the failure situation by hotbit. But, it is also needed to generate new token in the logical ring.

- DC : G/C fail -> node out -> lowest address has token

T_delay_dc = TRT + 2T_cp + T_hotbit + T_slot + TRT +T_slot (8)

2.3.3. Max-TCD and Max System Response Time

In the above section, the formulas of TCD calculation in recoverable fault cases are investigated. As we presented, there are three kinds of TCDs. If we assume the parameters shown in Table 2 and take the maximum values, we can calculate system response time from equation (2).

For example, if 1_path_communication is needed in outlet economizer valve position signal in Feed Water Control System (FWCS), and the Case A failure is occurred. The Max-LCD which is composed of one TCD in equation (2), can be calculated as follows:

$$= TRT+2T\_cp+2{*}T\_slot+T\_process+\Delta\delta$$
$$= 16+2{*}2+2{*}4+10+\Delta\delta$$
$$= 38+\Delta\delta \text{ [ms]} \quad (9)$$

Equation (9) means that, although Case A fault occurs during processing in FWCS(Feed Water Control System) for economizer valve signal, the system response time will be lower than Total Processing Time + 30[ms].

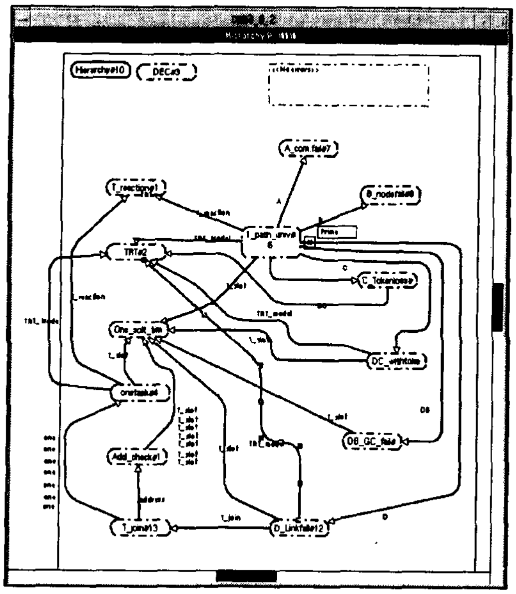

Fig. 5. CPN Hierarchy Page for 1_path TCD

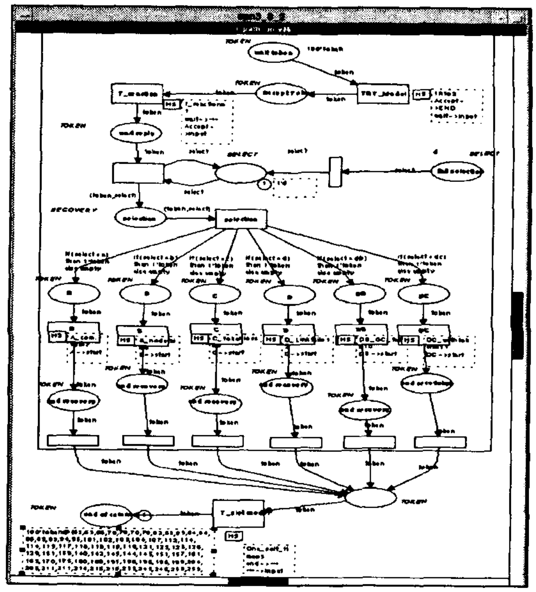

Fig. 6. CPN Main Page for 1_path TCD

Max-TCDs, whose parameter values are shown in Table 2, are presented in Table 3.

3. CPN Simulation Analysis

If we know the maximum values of the parameters, we can calculate the maximum response time of recoverable fault cases. However, because several parameters such as TRT, T_slot, T_cp and T_process are random variables, only the minimum and maximum values can be guessed. The designer, according to their need for the target system, should determine the parameters such as the number of G/C, the number of L/C, T_timeout, T_networkout and T_hotbit. Therefore, even though the design plan exists, we can not get the exact response times.

The profiles of the response time in fault cases can be the important data for system safety. For example, in real-time system with time constraints, it enables one to find the failure propagation probability from fieldbus to outer system and determine whether the system including fieldbus is designed considering fault-tolerant functions of fieldbus or not. In this work, we constructed a CPN based simulation model to find the probability distribution of TCD delays.

CPN is a good graphical language for system verification and validation (V/V)[7][8]. CPN has a computerized tool support, Design/CPN. CPN make it easy to verify the correctness of the modeling. By hierarchical structure, it is easy to apply given sub-models to another system analysis.

As we focus on time delay, we have used time label in Design/CPN. In Design/CPN, there is a time label in token in CPN diagram. Each transition in CPN diagram has the time region. The time in Design/CPN can be real number as well as integer. The time label of intial marking is '0' . With the firing of a place, token moves to the transition connected by arc. In transition, the time label of the token is summed with the value of the time region. Through this process, the time labels of final token indicate the sum of the values of time responses that the token passed.

The modeling scope is focused on the fieldbus TCDs which are composed of one token rotation path. In fact, NPCS have several token rotation paths as shown in Figure 3. The longest communication distance is composed of three token rotation paths across the G/Cs (3_path_communication). Even though 3_path_communication is more complex and has longer delay time, it can be made up of 1_path_communication sub-models. As a matter of fact, TCD can be established by 1_path_communication delay, 2_path_communication delays or 3_path TCD delays. These concepts have been introduced in Figure 3.

As this study is focused on inside NPCS network, the communication delays or the fault recovery delays outside the NPCS fieldbus network are not considered in this work. Strictly speaking, the communication, which is inside NPCS fieldbus network, is the limitation of this study.

In the model of Figure 6, it is possible to select the failure cases per one path communication. The inputs of this model are many tokens labeled 'time = 0' . The outputs are tokens which have difference time labels. This time label means the delay time. The hierarchical structure is represented in Figure 5. The main model for 1_path_communication simulation model is represented in Figure 6.

The output of this simulation can be obtained by using ML-Extraction Program. Because the Design/CPN is programed by CPN-ML Language, extraction of data from Design/CPN diagram can be performed by CPN-ML program. The CPN-ML is a language built upon Standard ML which is a kind of functional language. The extracted data can be handled to represent the probability distribution of TCD delays of the fault cases.

From the 1_path TCD simulation outcome, we can determine whether the fault can be recovered within time constraint of the real-time system or not. If it can be recovered, we can calculate fault propagation probability from the regression polynomial. The meaning of the simulation outcome is represented in the following example.

Example :

In NPCS, the response time of valve #1 is required to be less then 80ms. From equation (2), we found that LCD should be less than 30[ms] and LCD is composed of one TCD. We also found that the task, actuating valve #1, requires 1_path communication.

In this case, the time limit of 1_path TCD is 30[ms]. Therefore, TCD which is above the time limit indicate that the fault case is not recoverable. Whether the fault cases are recoverable or not can be determined from the range of the TCD. It is described in Table 4.

The fault Cases such as A, DB and DC are determined to be recoverable. The Case DB can be recovered perfectly, because the range of the case is less than 29[ms]. In other words, the recovery ratio of Case DB is 1. Then it is interesting to find out the recovery ratios of the cases A and DC.

In cases of A and DC, CPN based simulation can provide the recovery raito of the failure cases. Figure 7 and 8 are the outcomes of the CPN simulation. The dotted line represents the 5th-order regression of the simulation outcome. The regression polynomials for the cases of A and DC are equation (10) and equation (11), respectively.

Table 4. Recovery Decision of each Fault Cases

Case	Decision	Case	Decision
A	Recoverable	D	Not Recoverable
B	Not Recoverable	DB	Recoverable
C	Not Recoverable	DC	Recoverable

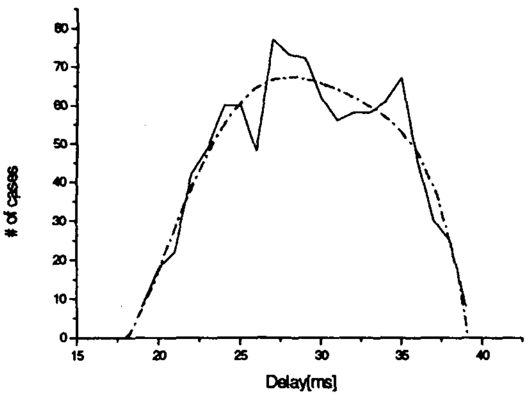

Fig. 7. Case A

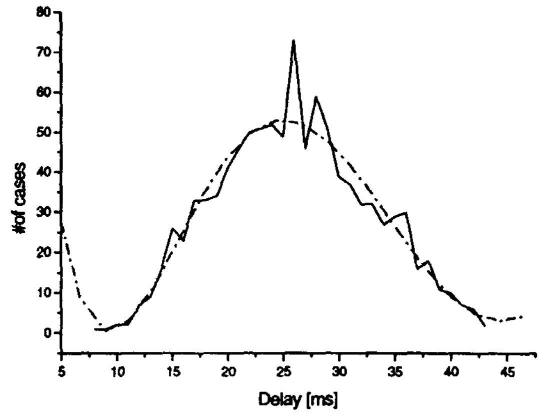

Fig. 8. Case DC

Case A :

-4.5547e-4*X^5+0.06368*X^4-3.50254*X^3+94.12567*X^2-1224.53787*X+6147.33646 (10)

Case DC :

-1.49391e-5*X^5+0.00254*X^4-0.15582*X^3+4.14226*X^2-44.31517*X+161.69056 (11)

In Case A and DC, the calculation formulas of recovery ratio are presented in equation (12) and equation (13), respectively.

$$\text{Recovery Ratio of Case A} = \frac{\int_{19}^{30} Y_A}{\int_{19}^{38} Y_A} = \frac{566.3}{1035.9} = 0.5467 \quad (12)$$

$$\text{Recovery Ratio of Case DC} = \frac{\int_{8}^{30} Y_{DC}}{\int_{8}^{45} Y_{DC}} = \frac{726.2}{1114.6} = 0.6515 \quad (13)$$

From the meaning of 'Recovery Ratio', the meaning of '1-Recovery Ratio' is 'Fault propagation probability to outside fieldbus system'. Therefore, Fault propagation probabilities to outer fieldbus system of this example are equation (14) and equation (15).

Fault propagation probability of Case A = 0.4533 (14)

Fault propagation probability of Case DC = 0.3485 (15)

4. Conclusions

In order to find the delays of recoverable fault cases in general fieldbus protocol, the definitions of TCD, LCD and several concepts are introduced. Recoverable faults are classified in Table 1 and formulas for calculating recovery delays are established. Because of random variables in delay calculation formulas, the Design/CPN simulation model is used to find realistic delay data caused by recoverable faults. The outcome of this simulation can be used to calculate failure recovery ratio for given recoverable faults and failure propagation probability to outer fieldbus system. The program coded by CPN-ML language, which enables to extract data from CPN diagram, is also developed in this study.

The 1_path TCD model is investigated in this research. If the total processing time of the response is known, the response time of the system can be calculated. Before prototype testing, the estimation of the response time enables for designer to design a system more efficiently. If we adapt this work to existing system, we can evaluate the fault-tolerance performance of the system for recoverable faults.

In this study, the CPN simulation model is designed for the fieldbus of NPCS. The model is adaptable to another fieldbus system. In adapting another system, it is also required to classify recoverable faults for the target system. Then the simulation model can be modified. The simulation model of NPCS is the example of the framework to evaluate fault-tolerance performance.

The framework of fault-tolerance performance evaluation in this study is confined to inter fieldbus system of the target system. The communication delay and response time of outer the target system is not considered in this study. This is a limit of this study. The study for inter fieldbus system is also improtant because the performance of the total communication system is caused from the performance of small groups such as inter fieldbus systems. As the example of a fault-tolerant performance evaluation for a small group communication system, we investigated the NPCS fieldbus in KNGR NPP.

The communication delay to communicate outer NPCS system is influenced by many factors such as traffic flows, physical distance between two nodes, the communication priority, etc. These factors mainly depend upon the target system characteristics. Therefore it will be very specific work. The communication delay and response time including outer NPCS fieldbus system should be investigated in a further study.

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, (1996).
2. Michel Banatre and Peter A Lee , "Hardware and Software Architectures for Fault Tolerance: Farnam Jahanian, Fault-Tolerance in Embedded Real-Time Systems," pp 237-249, Lecture Note on Computer Science, Springer, (1994).
3. ANSI/ISA-dS50.02-1997, "Fieldbus Standard for Use in Industrial Control Systems, Part 4 : Data Link Protocol Specification," ISA (1998).
4. "Modbus Plus Network Planing and Installation Guide 890 USE 10000 Version 2.0", AEG Schneider automation.
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," (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, (1997).