Physical Layer Redundancy Method for Fault-Tolerant Networks and Its Application to an Autonomous Mobile Robot

Jae Min Lee, Dong Sung Kim, Wook Hyun Kwon
Control Information Systems Lab.
School of Electrical Eng. and ERC-ACI
Seoul National University
Seoul, 151-742, Korea

Hong-Ju Moon, Myung-Hyun Yoon
Nuclear I & C Group, Nuclear Power Gen R. L.
Korea Electric Power Research Inst.
Korea Electric Power Corporation
Taejon, 305-380, Korea

ABSTRACT

In this paper, the physical-layer redundancy method is proposed for the fault-tolerant industrial network. The proposed method consists of the fault detection method and the correction method. The fault detection method uses events created by the state transition in IEEE 802.4 MAC sublayer and the periodic status frame check for the detection of fault. The fault correction method corrects the fault with the automatic physical layer switching to the stand-by physical layer due to the event created by the fault detection method. The proposed method is realized with dual physical layers, the Dual Channel Manager for switching and the Redundancy Management Module that has the Fault Detection Sub-module and the Fault Correction Sub-module. The proposed method is applied to a distributed communication architecture of the internal control network of an autonomous mobile robot.

1. INTRODUCTION

One of the most important changes in the process industry has been the innovation of industrial networks. The industrial network is the digital communication link among intelligent field-level devices. The distributed control system or the computer integrated manufacturing system is usually composed of fiels-level devices and the industrial network, which requires high reliability as well as availability. In the embedded system, the network is one of the most important elements since it takes charge of the exchange of information, such as control command or measured value of sensors. However, even for highly reliable networks, faults are inevitable. Therefore, all of industrial networks have fault-tolerance, using H/W or S/W redundancy, such as dual systems, redundant network interface unit(NIU)s and N-version programs, etc[1, 2, 3].

The well-known fault-tolerant industrial networks are as follows. ADMAP duplicated the physical layer of a Mini-MAP system[4]. Many Manufacturing Automation Protocol (MAP) applications duplicated the physical layer of a modified Full-MAP[5, 6]. WorldFIP has achieved fault-tolerance by the medium redundancy[7]. CENTUM uses the pair and spare redundancy that has two CPU boards and two CPUs in one board together with bus and I/O redundancy[8]. On TTP, node failures and communication failures are masked by replicating nodes and two buses and sending the message twice on each bus[9, 10, 11]. LONWORKS realized fault-tolerance by the self-healing ring that will automatically redirect signals in case of a medium's open[12]. The NIU redundancy method that has the dual layer structure from the LLC sublayer down to the physical layer to cope with faults of those layers is proposed by Moon[2]. The fault detection method by the IEEE 802.4 media access control(MAC) protocol is studied also[2, 6].

Although these methods are good for the fault-tolerant system, a more highly reliable and faster method is required especially for the nuclear power plant or embedded systems, such as airplanes, ships, NC machines and mobile robots, etc[13, 14, 15]. The NIU redundancy method is highly reliable but has a little time delay in switching to the stand-by board. The system redundancy method is also high reliable but has time delay in transferring previous information to the stand-by system. Therefore, the faster and higher reliable fault detection and correction method is needed.

In this paper, the physical layer redundancy method is proposed to satisfy these needs. The proposed method duplicates physical-layer and added the Dual Channel Manager (DCM) and the Redundancy Management Module for the faster channel switching. For the fault detection, the proposed method uses events created by the state transition in IEEE 802.4 MAC sublayer and the periodic status frame check. Then, the fault is corrected by the automatic physical layer switching to the stand-by channel during the state transition of the fault correction method.

For proving this method in a practical system, the proposed method is implemented in the Plant Instrumentation and Control Network(PICNET) that was developed by Seoul

National University and KEPRI, Korea. As results of implementation, the proposed method guarantees highly reliable and fast fault-correction. The PICNET will be used for the middle-level network in nuclear power plant. The proposed method is also applied to the internal control network of an autonomous mobile robot and simulations prove its availability. Even if under more complicated and dangerous circumstances, such as the nuclear power plant, the autonomous mobile robot should arrive at its destination without human's control and collisions with other objects. However, this requirement may not be satisfied when network faults are occurred during its navigation. Therefore, by adapting the proposed method, the autonomous mobile robot could arrive at its destination even if faults have occurred in the distributed control network.

In Section 2, the faults covered by the proposed method are classified, and the proposed fault detection method is presented. The proposed fault correction method is shown in Section 3. The proposed method is implemented in PICNET in Section 4. Then, its application to the communication architecture of the internal control network of an autonomous mobile robot is shown in Section 5. Finally, the conclusion is drawn in Section 6.

2. FAULT DETECTION METHOD

By the proposed method, faults are detected with two techniques. In first step, faults are detected by events due to the state transition in the MAC sublayer. According to the IEEE 802.4 MAC protocol, events are created when faults are occurred in physical layer[16]. Secondly, the periodic status frame check is used to prepare for the first technique's failure. For the fast and reliable fault detection, we use only six events, instead many events are occurred by the corruption of logical ring. If a fault is occurred in the data link layer, the first method may not detect fault. At this time, the periodic status frame check technique detects fault. The proposed method every nodes transmit its own status frame and receive the others' status frame. If one node had fault and did not transmit status frame, others node can detect the fault. In first, the fault that is covered by the proposed method is defined, then the fault detection method using event and status frame is presented.

Definition of Faults

In a network, each fault can be classified by its location as the physical layer fault, the transmitter and receiver fault, the upper layer fault, and noise. Among the physical layer fault, there is medium open, short and imperfect medium connection. The transmitter or receiver's malfunction also can make fault. Noise can sometimes give distortion to the signal and make transient fault. Host's malfunction or interface error between the host and the NIU is classified as upper layer faults. The proposed method can detect and correct physical layer faults. The transmitter and receiver's fault and the upper layer fault also can be detected and they can be corrected by the system redundancy.

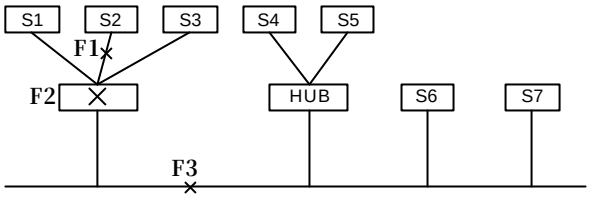

Figure 1: Examples of Faults in Physical Layer.

Figure 1 shows examples of physical layer faults when the network used only single medium. When a medium open is occurred, the single node may be isolated or all of nodes can be separated in a few groups of nodes. F1 shows the single node's isolation. F2 also separates into single nodes, and F3 divide in two groups. These faults made network abnormal and the logical ring corruption by the IEEE 802.4 protocol communication. Therefore, faults in the physical layer can be detected by supervising the operation of LLC sublayer because various errors are reported from the LLC sublayer.

Fault Detection Method by Events

We use MC68824 token bus controller(TBC) as MAC[17]. The state transition in steady state of MAC is showed in Figure 2 and the names of states are listed in Table 1. When each NIU in a network is on or reset, the first state of NIU is OFFLINE. Then, if the token bus controller is initialized, the state transits to the IDLE state, and bus idle timer is started at that time. If no signals are detected in the bus, the timer is reset and restarted. If the value of the timer is larger than six or seven slot time, it can be regarded as no token in logical ring, and the state is transited to ClaimToken. In this state, token contention process can transmit the predefined Claim Token frame according to the address of MAC in NIU. The survived NIU on the contention can achieve the token and transits to the UseToken state. The remained NIUs are transited back to the IDLE state. The NIU that received the token from previous NIU, also transits to UseToken. In this state, the NIU checks whether the transmit time and frames in four transmit queue are remain and can transmit the frame by priority order. At this time, the NIU repeatedly exchange state between Await IFM Response and Check Access Class. If the transit time expired or no frames are remained in queue, it is transited to Pass Token state. If NIU knows the next station, the token is transmitted to the next station. Otherwise, it is transited to CheckTokenPass[16].

In CheckTokenPass state, whether the token is successfully transmitted is checked. If the transmission is succeeded, the NIU transits to IDLE. Otherwise, the token is transmitted again. If the transmission is failed again, the NIU transits to

AwaitResponse. In this state, the NIU transmits solicit_successor_2 frames and determines the next station. The NIUs received frames, such as who_follows, solicit_successor_1 or solicit_successor_2, transmits set_successor frame due to the response window algorithm. If the NIU in AwaitResponse receives the set_successor frame, it determines the NIU that has transmitted set_successor as the next station. It also passed the token to the next station in the PassToken state. When the NIU has passed CheckTokenPass state and transited to IDLE, token pass process is ended. If there is no set_successor frame in the physical layer, no_successor is logged to the network manager[16].

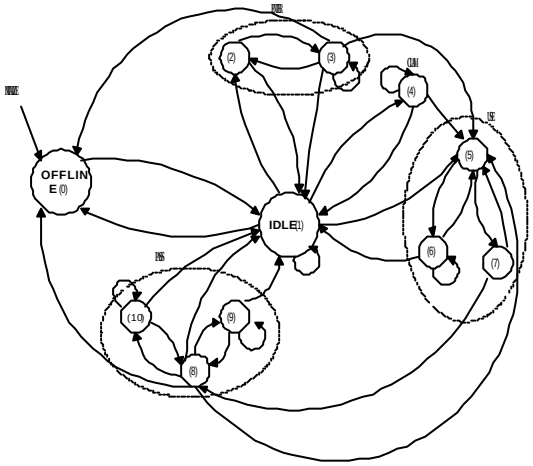

Figure 2: State Transition in IEEE 802.4 MAC

Table 1. State Number and Name

Number	State
0	OFFLINE
1	IDLE
2	DemandIn
3	DemandDelay
4	ClaimToken
5	UseToken
6	AwaitIFMResponse
7	CheckAccessClass
8	PassToken
9	CheckTokenPass
10	AwitResponse

To detect faults in the physical layer, the state transition events in MAC which are occurred by the corruption of the logical ring are used. TBC provides the ability to monitor the events mentioned in the above by the interruption. TBC set the bits of interrupt word by these events. For the fast fault detection, we use only six events, such as new_successor, won_contention, hear_successor, initialize, exit_ring and no_successor_8. The first three events create SC interrupt, and the rest events NS interrupt. Thus, because we programmed the interrupt service routine using only two interrupts, the proposed method is simple and fast to detect faults and realized in the Fault Detection Sub-module.

Fault Detection Method by Status Frame Check

The proposed method also has the other fault detection method, status frame check. Each station produces status frame and broadcasts it periodically. All other station's status frames are received and stored in a certain memory allocated three bytes per one station. Two bytes are for the data of the latest received status frame, and one byte is the previous value of live counter. The received status frame contains the station's status, such as the live count value of the NIU, host's status, the status of two physical layers and the information of dual mode. Figure 3 shows the data in the status frame used in the proposed method. This frame is produced in the Status Frame Production Sub-module and checked in the Status Frame Check Sub-module.

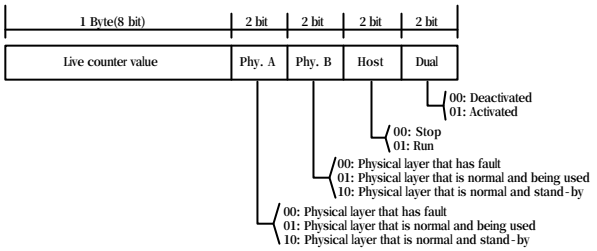

Figure 3: Data in a Status Frame

3. FAULT CORRECTION METHOD

After the fault is detected by the proposed method, the fault is corrected by the automatic physical layer switching. Then, the faulted NIU does its operation in normal status. For the fast fault correction, the station is transmitted frame with both physical layers and received only one physical layer. The physical layer using in transmission and reception is defined as the active physical layer, and using only in transmission as the stand-by physical layer. The proposed fault correction method is the event-based method, and the state, that is specified by the condition of the physical layer and the status of dual mode, is transited by the events created in Fault Detection Sub-module. Figure 4 shows the state transition of the fault correction method.

The proposed method is composed of five states, such as Manual_Normal, Auto_Normal, Config_Error, Medium_Error

and IDLE. If a station's power is off, the station is in IDLE. Then, initialization is finished and the station transits to the Manual_Normal state. At this state, the logical ring is not constructed and some other stations are not finished initialization. Because the dual-mode is not activated, the physical layer is not changed. When the logical ring is constructed and the token passing is normally working, The station's state can be transited to Auto_Normal. If AUTO_SW_MODE that means dual mode is activated or Status Check = OK that is occurred when both physical layers are good in the Status Frame Check Sub-module, is produced, the state transits to Auto_Normal. At this state, because the dual mode is activated, the physical layer can be changed when a fault is detected in the active physical layer. If the active physical layer has fault or NS event is occurred, the state is transited to Medium_Error, and the stand-by physical layer is became the active physical layer. If the stand-by physical layer is faulty, the state is transited back to Manual_Normal and the dual mode is deactivated. Otherwise, the state is not changed.

The SC event means that the next station has changed. It can be occurred by the station's missing or having fault in physical layer. Therefore, the state is transited to the Config_Error. During the transition, The station broadcasts the physical layer switching command to reconstruct the logical ring. At this time, the SC event is occurred in all stations, and the state of all stations is transited to Manual_Normal. This state will not be changed until the faulty station recovered back to normal state. After the faulty station is fixed, the Status Check = OK event is occurred. Then, the state will be transited to Auto_Normal. If both physical layers have fault, the state is transited to IDLE. This state will not be changed until the reconstruction of the logical ring is restarted.

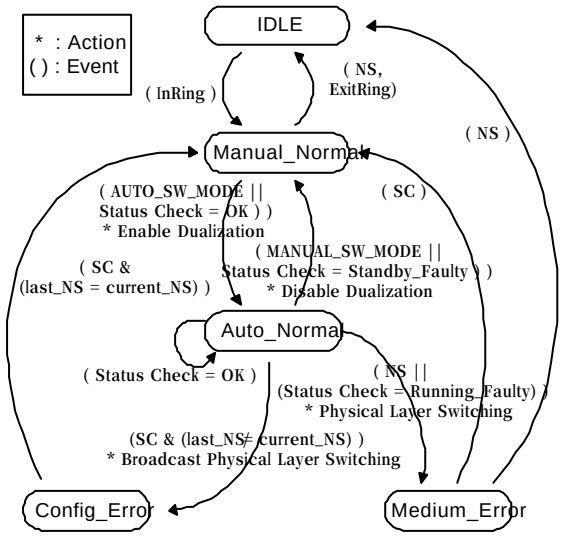

Figure 4: Block Diagram of State Transition of the Fault Correction Method

4. IMPLEMANTATION IN PICNET

The proposed method is implemented in PICNET, a plant instrumentation and control network. Two physical layers are in one NIU board, and added the Redundancy Management Module in network management, the Dual Channel Manager and two physical layers. Figure 5 shows the implementation of the proposed method. The Dual Channel Manager switches the active physical layer to the stand-by physical layer from the order in the Fault Correction Sub-module. The Dual Channel Manager transmits data using both physical layers and receives signals from only one active physical layer. The Dual Channel Manager also monitors the statuses of the active physical layer and the stand-by physical layer that are recorded in the internal status register. This information is read by Physical Layer Status Check Sub-module, and sent to Status Frame Production Sub-module. The received status frames from other station are checked periodically in the Status Frame Check Sub-module. This sub-module creates events and sends them to the Fault Correction Sub-module. The Fault Detection Sub-module also creates events, such as NS and SC based on TBC's interruption, and sends them to the Fault Correction Sub-module. The state transition in the Fault Correction Sub-module is event-triggered. During its transition, the action is executed. The result of Fault Correction Sub-module is recorded and reported to the network manager. Based on this report, the network manager will be fixed the faulted physical layer or replaced it as new one.

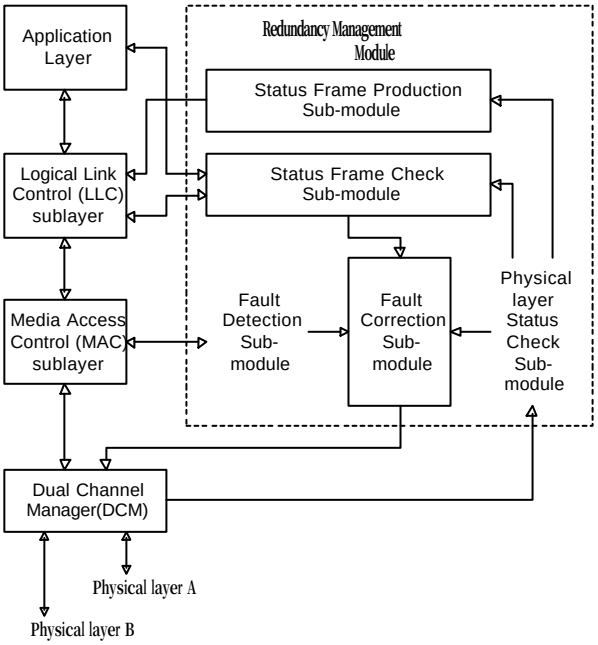

Figure 5: Block Diagram of the Redundancy Management Module

5. APPLICATION TO AN AUTONOMOUS MOBILE ROBOT

The proposed method is applied to the internal control network of an autonomous mobile robot. The autonomous mobile robot uses six AC servo motors, twenty four ultrasonic sensors and vision sensor. Three motors are used for driving purposed and three for steering. Six analog servo drivers are used to control each motor. MVME162 board using MC68040 CPU is adopted as the main controller, Through the NIU, velocity commands of servo drivers and encoder signal counting are transferred to the main controller. The internal control network for the autonomous mobile robot is the fault-tolerant network in which the physical layer redundancy method is applied. All of controllers and sensors, except vision sensor, are connected with duplicated channel with NIUs. The H/W architecture of the applied mobile robot is shown in Figure 6.

When a fault is occurred in the active physical layer, the stand-by layer is used instead of the faulty physical layer. Therefore, the reliable operation of the mobile robot is guaranteed even if under the complicated and dangerous circumstances where the manager may not be enable to approach and control the autonomous mobile robot right after the fault is occurred.

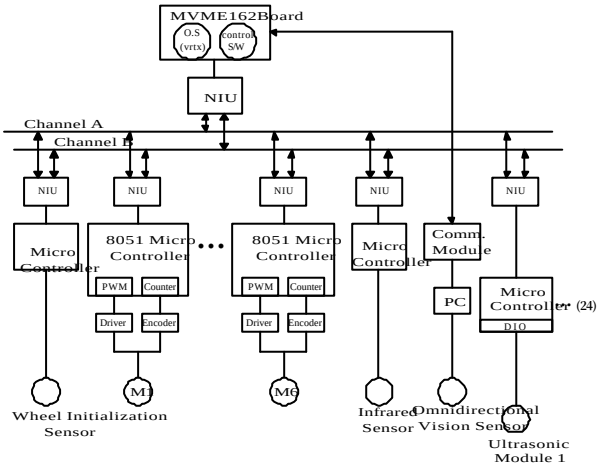

Figure 6: H/W Architecture of Autonomous Mobile Robot with Redundant Physical Layers

6. CONCLUSIONS

In this paper, the physical layer redundancy method is proposed for realization of the fault-tolerant network and it is implemented in PICNET and the internal control network of an autonomous mobile robot. The proposed method duplicated the physical layer and added the Dual Channel Manager and the Redundancy Management Module. For the fault detection, the proposed method uses events created by the state transition in the IEEE 802.4 MAC and the periodic status frame check. Then, the fault correction method is executed using the automatic physical layer switching. Then, the network is again in normal state. As results of implementation, the proposed method guarantees highly reliable and faster fault-correction. This method is also cost-effective because the proposed method realized fault-tolerance only by the physical layer redundancy. The proposed method and the system redundancy method can be simultaneously applied to the internal control network in an airplane or a ship for the higher reliability. In the future, the evaluation of the proposed method will be studied.

6. REFERENCES

[1] J. Laprie, J. Arlet and C. Beoness, "Definition and Analysis of Hardware- and Software-fault-tolerant Architectures", *IEEE Computer, Special Issue on Fault-Tolerant Systems*, vol. 23, no. 7, pp. 39- 51, July 1990.

[2] H. Moon and W. Kwon, "A Fault Detection and Recovery Mechanism for The Fault Tolerance of a Mini-MAP System", *Journal of Control, Automation and Systems Engineering*, vol. 4, no. 2, pp. 264-271, 1998.

[3] V. Nelson , "Fault-tolerant Computing : Fundamental Concepts", *IEEE Computer, Special Issue on Fault-Tolerant Systems*, vol. 23, no. 7, pp.19-25, July 1990.

[4] Y. Shiobara, "Advanced MAP for Real-time Process Control", *Proceedings of IECIN87, Cambridge, Massachusetts*, pp. 883-891, 1987.

[5] H. Kleins and K. Zwoll, "Map mining – a Communications System for Mining Applications", *EMUG MAP/TOP EVENTS Conference Proceedings. SYSYTEC 92*, 1992.

[6] H. Moon, "Performance Analysis and Design of a Communication Network for Industrial Automation", *Ph. D. Dissertation, Seoul National Univ.*, 1998.

[7] P. Laterrier, "The FIP Protocol", WorldFIP internal report, 1995.

[8] CENTUM CS3000 Integrated Production Control System, *Yokogawa Internal Report*, 1998.

[9] G. Gruensteidl and H. Kopetz, "A Reliable Multicast Protocol for Distributed Real-Time Systems", *8-th IEEE Workshop on Real-Time Operating Systems and Software, Atlanta, GA, USA*, May 1991.

[10] H. Kopetz, R. Hexel, A. Krüger, D. Millinger, R. Nossal, A. Steininger, C. Temple, T. Führer, R. Pallierer and M. Krug, "A Prototype Implementation of a TTP/C Controller", *SAE Congress and Exhibition*, Detroit, MI, USA, Feb. 1997.

[11] R. Pallierer and E. Fuchs, "A Tool for The Evaluation of the TTP/C Protocol", *8-th European Workshop on Dependable Computing, Experimental Validation of Dependable Systems, Goeteborg, Sweden*, 1997.

[12] Lonworks for Audio Computer Control Network

Applications, *Echelon Internal Report*, 1995.

[13] Q. Wang and A. M. S. Zalzala, "Transputer Control System with a Gas Motion Planner for the PUMA560 Industrial Robotic Manipulator", *Proceeding of the 13th IFAC Workshop on Distributed Computer Control Systems*, pp. 77-82, Sept. 1995.

[14] G. Yasuda, "Distributed Implementation of Communicating Process Architectures for Autonomous Mobile Robots", *Proceeding of the 14th IFAC Workshop on Distributed Computer Control Systems*, pp. 81-86, July 1997.

[15] J. Yun, S. Nam and S. Lee, "Evaluation of Network Protocol for Automotive Data Communication", *Proceeding of the 14th IFAC Workshop on Distributed Computer Control Systems*, pp. 93-98, July 1997.

[16] ISO/IEC 8802-4, Information processing system –Local Area Networks – Part 4: Token-passing Bus Access Method and Physical Layer Specifications, *IEEE Inc.*, 1990.

[17] MC68824 User's Manual, *Motorola Inc*., 1987.