Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

Verification of failover effects from distributed control system communication networks in digitalized nuclear power plants

Moon-Gi Min*, Jae-Ki Lee, Kwang-Hyun Lee, Dongil Lee, Hee-Taek Lim

Korea Hydro & Nuclear Power Co., Ltd, 1312-70 Yuesong-daero, Yuseong-Gu, Daejeon 305-343, Republic of Korea

ARTICLE INFO

Article history:
Received 27 July 2016
Received in revised form
28 February 2017
Accepted 15 March 2017
Available online 15 April 2017

Keywords:
Network Failover
Network Verification Methodology
Network Test
Redundant Network Verification
Packets loss rate
Packets error rate
Protocol Data Unit
Non-deterministic Network
Ethernet Network
TCP/IP Network

ABSTRACT

Distributed Control System (DCS) communication networks, which use Fast Ethernet with redundant networks for the transmission of information, have been installed in digitalized nuclear power plants. Normally, failover tests are performed to verify the reliability of redundant networks during design and manufacturing phases; however, systematic integrity tests of DCS networks cannot be fully performed during these phases because all relevant equipment is not installed completely during these two phases. In additions, practical verification tests are insufficient, and there is a need to test the actual failover function of DCS redundant networks in the target environment. The purpose of this study is to verify that the failover functions works correctly in certain abnormal conditions during installation and commissioning phase and identify the influence of network failover on the entire DCS. To quantify the effects of network failover in the DCS, the packets (Protocol Data Units) must be collected and resource usage of the system has to be monitored and analyzed. This study introduces the use of a new methodology for verification of DCS network failover during the installation and commissioning phases. This study is expected to provide insight into verification methodology and the failover effects from DCS redundant networks. It also provides test results of network performance from DCS network failover in digitalized domestic nuclear power plants (NPPs).

1. Introduction

Digital instrumentation and control systems, distributed control systems (DCSs), and programmable logic controllers have replaced the original analog control components and systems in nuclear power plants. The main concerns associated with analog systems are the effects of aging, such as mechanical failure and functional degradation. However, digital electronic components provide enhanced performance in terms of accuracy and computational capabilities, and have achieved higher data handling and storage capabilities; thus, they allow operating conditions to be more thoroughly measured and displayed [1,2].

To achieve technical self-reliance for nuclear instrumentation and control systems in South Korea, the Advanced Power Reactor 1400 man–machine interface system architecture was developed [3]. This system, which is illustrated in Fig. 1, is based on a communication network system [4]. A DCS redundant backbone network links all process controllers, operator and engineer interface functions, and associated equipment and systems, in such a manner that all information or commands appear totally integrated, reliable, and nearly instantaneous. At the highest level of hierarchy is the plant operational staff, and at the lowest level are the thousands of sensors and control devices that interface with these processes.

DCS communication networks exhibit more unpredictable performance compared with that of state-based communication systems, which communicate using a fixed set of data at regular intervals. The communication load of the state-based communication system is constant no matter what the system is doing, and the maximum communication load of the safety system is approximately equal to the normal load of the safety system. Data communication systems used in reactor protection systems and display systems for important safety information should also have a state-based, rather than an event-based, architecture [5,6]. Advanced Power Reactor 1400 man–machine interface system DCS redundant networks use a Transmission Control Protocol/Internet

* Corresponding author.
E-mail address: besteffort@khnp.co.kr (M.-G. Min).

http://dx.doi.org/10.1016/j.net.2017.03.002

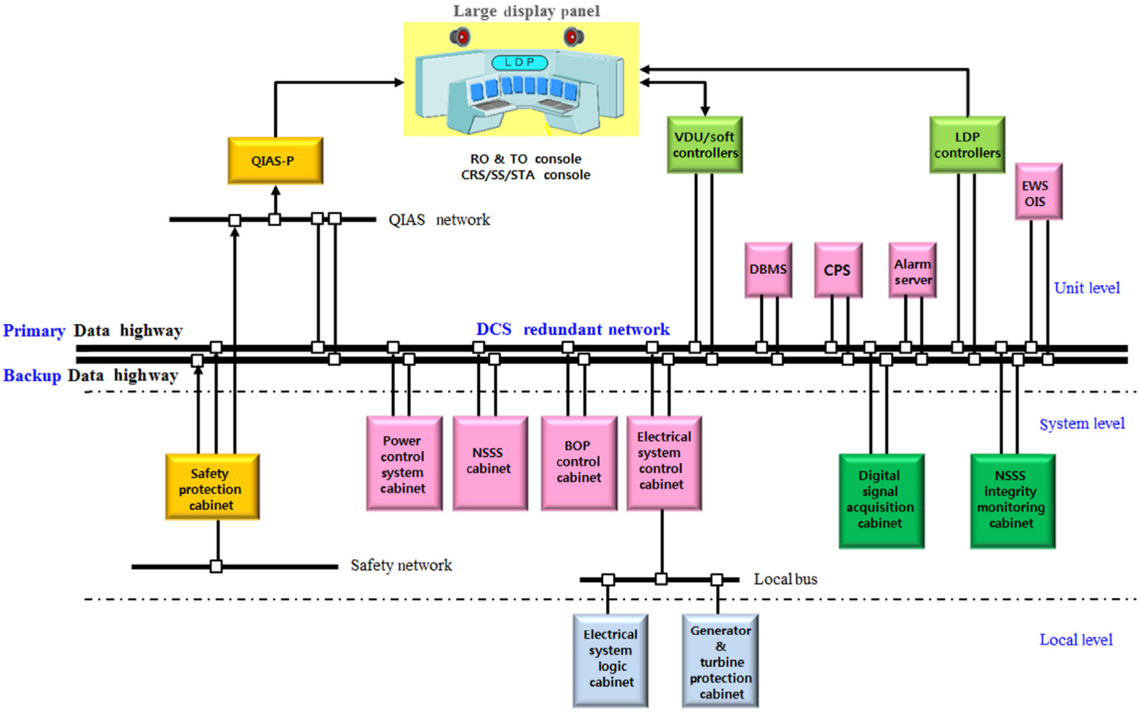


Fig. 1. ARR-1400 MMIS schematic diagram [4]. APR-1400, Advanced Power Reactor 1400; BOP, Balance of Plant; CPS, Computerized Procedure System; CRS, Control Room Supervisor; DBMS, Database Management System; DCS, distributed control system; EWS, engineering workstation system; LDP, large display panel; MMIS, man–machine interface system; NSSS, Nuclear Steam System Supplier; OIS, operator interface system; PAMI, Post Accident Monitoring Instrumentation; QIAS, Qualified Indication and Alarm System; QIAS-P, Qualified Indication and Alarm System-PAMI; RO, Reactor Operator; SS, Shift Supervisor; STA, Shift Technical Advisor; TP, Trubine Operator; VDU, Visual Display Unit.

Protocol stack, which brings the likelihood of lost or delayed packets [7]. Man–machine interface system DCS networks, which are linked redundant systems and buffered network switches, have the potential for congestion and overload during peak load periods; thus, redundant DCS networks should be verified in a manner different from that used for state-based networks [8,9].

DCS redundant network failover is an important factor for determining the reliability of data transmission of a digital instrumentation and control system because network redundancy in the DCS network infrastructure helps avoid unplanned operation stoppages. The data communication network structure has been designed to satisfy the requirements of redundancy [10]. Redundancy is typically applied to DCS communication networks to provide fault tolerance that increases system reliability in the form of backup or fail-safe. However, redundancy structures can sometimes create more complex configurations that increase the likelihood of failures and errors. Although, in the design and manufacturing phases, a reliability analysis is performed to verify the reliability of the redundant networks [11,12], the reliability analysis must be performed to verify the redundant network failover function of the DCS architecture during the installation and commissioning phases. The actual failover of redundant networks can be verified to meet communication-related requirements in actual field-installed conditions. The actual measurement of the performance and reliability of the DCS network system gives confidence that redundant networks are reliable.

In this study, a verification methodology for network failover is developed and verification tests are conducted in accordance with design-based events. This study is expected to provide insight into the verification methodology and ensure the failover effects, and to provide test results on network performance for DCS network failover in digitalized domestic nuclear power plants.

2. Review of network failover requirements

2.1. Failover of DCS redundant networks

In order to maintain the network integrity of each train and channel separately, DCS networks are configured independently for each safety train and nonsafety channel. A DCS has redundant communication networks that are continuously checked for failure. The network configuration is completely redundant, including all communication devices, interface cards, cables, and optical and electronic equipment. Communication between the various types of equipment of the DCS is ensured by these redundant communication networks. If there is no error in redundancy, one of the redundant networks is always active and the other is always in hot standby. A DCS is designed such that no single point of failure exists that can result in the failure of the entire communication system. Faults in any single component that interfaces with the data communication subsystem cannot cause both networks to fail.

The failover function is a switch to a redundant network upon failure or abnormal termination of a network. Failover and switchover are essentially the same operation, except that failover is automatic and usually operates without warning, while switchover requires human intervention. Failover requires no manual intervention to perform the check to restore operation to a previously faulted network after completion of repairs. Systems designers provide failover capacity in networks requiring continuous availability and a high degree of reliability. At the controller level, failover automation uses a heartbeat system that connects the main and backup controllers using a network connection. As long as a regular heartbeat continues between the main and the backup controller, the backup controller will not bring its systems online. The backup controller takes over the work of the main controller only when it detects an alteration in the heartbeat of the main controller [13].

2.2. Requirements of DCS networks related to failover

Communication networks can be defined by packet error rate, response time, application performance, and bandwidth, or in many other different ways. DCS communication networks have design specifications that include requirements of automatic transfer, response time, processor performance, and network bandwidth under the worst conditions (Table 1). Response time is the major element of network performance criteria.

2.2.1. Automatic transfer to redundant communication network

Redundant networks automatically and continuously check for operability. The failure of the primary network results in failover to the secondary network, and the secondary network continues to perform data communications. If one of the redundant communication networks fails, notifications should occur without interruption of communication or system performance degradation. Transfer to the secondary communication network is to be automatic, without disturbing system operation. The correctness of automatic transfer can be validated by examining the information, functions, and internal errors of the DCS.

2.2.2. Response time requirements

Response time is defined as the time from sending a request to receiving a message completely. It is often used to characterize the performance of a network.

Response time = T_response − T_request

Response time can be checked using response time test equipment, precision chronometer, or packet timestamp. Response time differs depending on how fast the system requires a response. Individual response times are combined to define overall response time, which must be within the requirements defined for the system [14].

A DCS exhibits response times that do not adversely impact the operation of plant equipment nor impede operator responses to events. The response time is the time lag between the input and the output signal, including the loop time, transmission time, and update time under worst-case communication conditions. According to system requirements, the response time for fast control loops is <0.25 seconds and for alarms on information display system it is <2.5 seconds.

2.2.3. Processor performance

DCS controllers are microprocessor-based electronic modules that interface with system communication networks. The controllers continue to perform their functional requirements successfully under the maximum expected loading conditions. One example of a processor requirement is that all controllers are not to be loaded >60%, with 40% idle time under worst-case conditions and 40% spare memory after performance tests. The load of DCS processors shall be <60% under the most stressful anticipated operating conditions, including 25% capacity for future expansion.

Table 1
Failover requirements in DCS networks.

Item	Requirement	Condition
Transfer	Automatic transfer	No disturbing system operation
Response time	0.001–2.5 sec	Worst communication situation
Processor usage	Less than 35–60%	Most stressed anticipated operating conditions
Network traffic	Less than 15–60%	Worst conditions

DCS, distributed control system.

2.2.4. Network traffic

Data communication networks shall be designed with sufficient performance margins to perform under conditions of maximum stress. Loading shall be based on plant transients and events that cause the highest transmission, such as plant data, failures, operator actions, etc. Data communication networks have approximately 40% additional capacity: 10% for the uncertainty of stressing the hardware to its limit and 30% for system expansion accommodation. For a DCS communication network, the communication system shall be designed and operated with a load not more than 15–60%; this is done to ensure that cyclical and noncyclical data transmit reliably and to meet the response time requirement in the case of using 20–40% capacity for future expansion under the worst conditions.

3. Proposed verification methodology for redundant network failover

3.1. Conventional verification for network failover

The performance of DCS redundant communication networks is verified by tests to show reliable performance under the worst anticipated conditions. One of the worst unanticipated cases in DCS communication networks is failover from redundant networks. Engineers must check the stability of equipment during network failover. The first things to be checked are the information, functions, and internal errors of the DCS during automatic transfer. When delayed information, malfunction, and internal errors occur, the DCS generates events or alarms. Burst traffic, packet error rate, resource usage, response time, and network independence during network failover from redundant networks are verified in the design and manufacturing phases, but not fully verified in the installation and commissioning phases.

3.2. Verification method for network failover

There is a need to enhance network verification methodology for network failover and quantify the communication margin during network failover. To quantify the effects of network failover in DCS redundant communication, packets Protocol Data Unit (PDU) were captured and the resource usage of the system was monitored. Verification tests were conducted to identify potential risks and failover effects based on a specified range of inspection periods for redundant networks (Table 2).

Table 2
Proposed verification method for DCS network failover.

Item	Requirement	Verification method
Transfer	No disturbing the system operation	Checking function and errors
Independence	No interfering with other network	Identifying network packets
Response time	0.001–2.5 sec	Monitoring packet timestamps etc.
Processor usage	Less than 35–60%	CPU trends using task manager
Memory usage	Less than 40–60%	Memory trends using task manager
Network traffic	Less than 15–60%	Network traffic with network analyzer

CPU, central processing unit; DCS, distributed control system.

3.3. Proposed verification methodology for network failover

This study proposes a verification methodology for network failover by field tests. The verification methodology consists of four tests: analyzing the packets, checking packet error and loss rates, monitoring resources, and evaluating response time (Fig. 2).

Transmission time can be delayed by packet errors and losses, or by network traffic if that traffic is higher than the communication bandwidth limits; thus, port mirroring is used on a network switch to send copies of network packets seen on one switch port to a network monitoring connection on another switch port. This method is used to monitor network traffic, analyze the packets, check packet error and loss rates, and evaluate network independence. A packet analyzer also provides detailed information about the packet errors and losses.

Monitoring of processor and memory usage can be accomplished by the system monitor. Processor and memory usage that exceeds requirements has a significant influence on the response time of a DCS system. A system monitor is a hardware or software component used to monitor resources and performance, such as central processing unit usage and memory usage.

Response time can be checked using response time test equipment, precision chronometer, or packet timestamps. Response time is the total amount of time taken to respond to a request for service. As the DCS becomes busier, the response time increases.

4. Failover verification test results for redundant DCS networks

When verifying network failover of DCS redundant communication networks, it is necessary to analyze the network traffic, packet loss and error rates, DCS resource usage, and response time. There was no delayed or corrupt information, degraded functionality, and internal DCS errors during automatic transfer.

4.1. Network traffic

Generally, when testing the network traffic of network failover, it is necessary to first capture the packets where there is the largest traffic and also to select equipment that is most sensitive to sudden traffic change. A network analyzer can be the most effective piece of equipment for capturing packets. A network analyzer monitors and captures all ports in a network switch and is mainly connected to the spare port of a network switch (port mirroring) in a DCS redundant network (Fig. 3). The test conditions in Fig. 3 simulate the failure of one redundant network when all equipment, including communication devices, is operating normally. The power of the root switch is forcibly turned off to simulate the root switch failure.

Burstiness is a commonly used measure of how infrequently a source sends traffic. A source that infrequently sends traffic is said to be very bursty. Burstiness is defined as the ratio of the peak to the average rate of traffic based on a specific sampling period for the data.

$$\text{Burstiness} = \frac{\text{peak rate}}{\text{average rate}}$$

A traffic test of network failover was conducted for the DCS redundant networks. A network analyzer was connected to the root switch through which most packets were passing. Packets of the secondary network were captured as soon as the primary network failed. Despite the increase of network traffic, the overall traffic was less than the data communication bandwidth limits of 60% (60 Mbps) of the DCS networks (Fig. 4).

$$\text{Burstiness of network failover} = \frac{39.40\ \text{Mbps}}{15.61\ \text{Mbps}} = 2.52$$

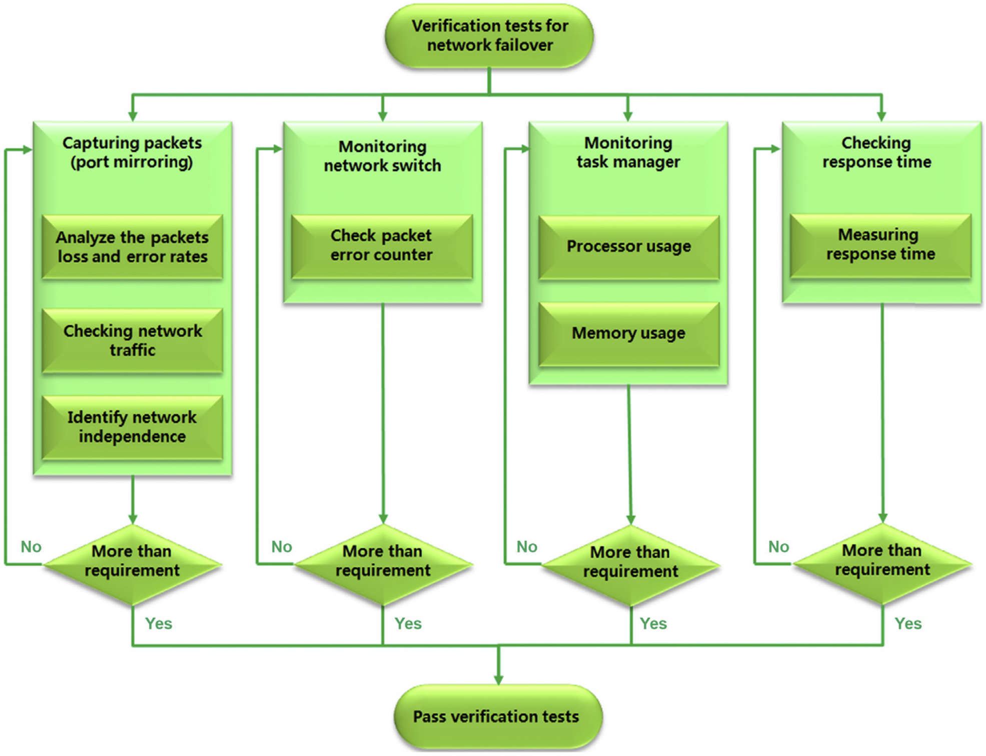

Verification tests for network failover
Capturing packets (port mirroring)
Analyze the packets loss and error rates
Checking network traffic
Identify network independence
Monitoring network switch
Check packet error counter
Monitoring task manager
Processor usage
Memory usage
Checking response time
Measuring response time
More than requirement
No
Yes
Pass verification tests

Fig. 2. Test verification methodology for network failover.

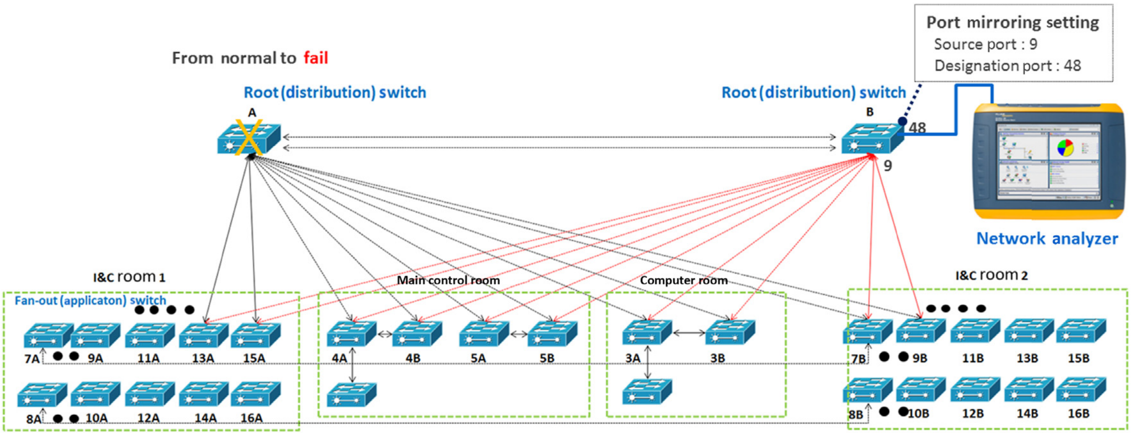


Fig. 3. Packet capture method for network failover. I&C, instrumentation and control.

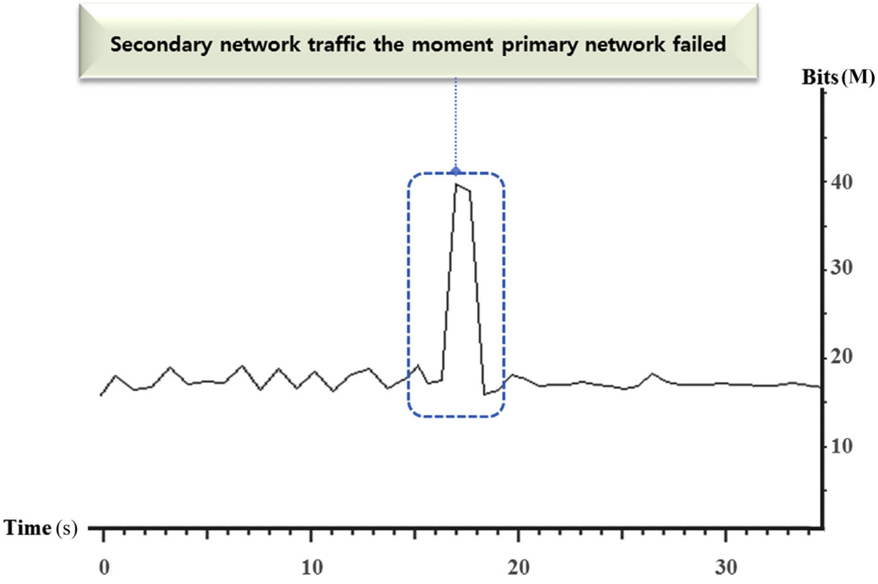


Fig. 4. Network traffic test for network failover.

4.2. *Resources usage of DCS*

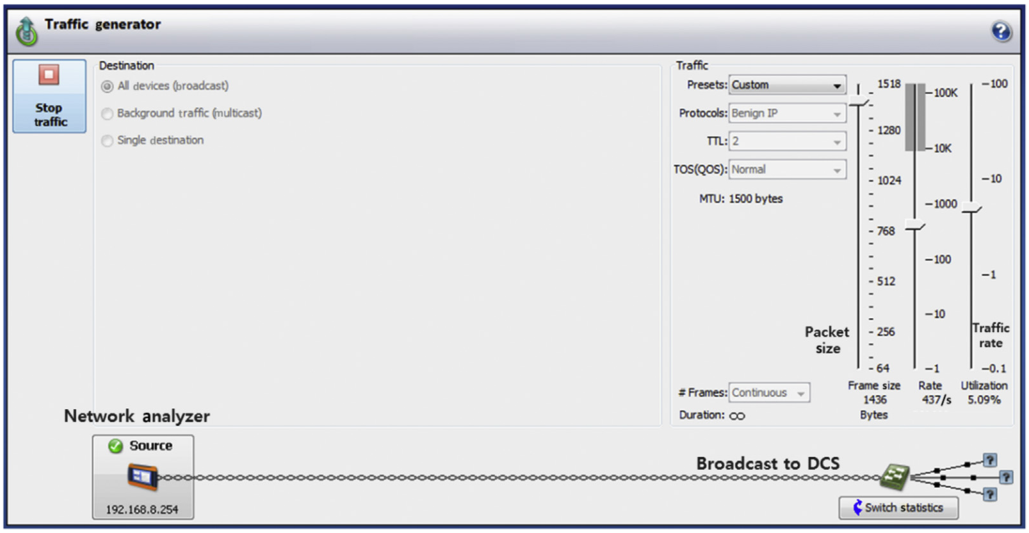
A DCS is a control system in which control elements are distributed throughout the plant. In a DCS, a hierarchy of controllers, servers, operator interface systems (OISs), and engineering workstation systems (EWSs) are connected by communication networks for command and monitoring. Therefore, it is very difficult to check the resource usage of each controller, server, OIS, and EWS in the brief span of the network failover function.

There is an alternative method to monitor DCS resource usage by simulating network failover conditions. Network failover conditions can be simulated by generating packets to networks. A network analyzer helps inject the packets into the DCS networks (Fig. 5). The size of the injected packets should be the average length of the packets captured, and the simulated network traffic should be the peak rate (i.e., 39.40 Mbps) of failover during the network traffic test.

The processor and memory usage of DCS controllers, servers, OISs, and EWSs was checked to meet performance requirements while generating network traffic to DCS networks. Processor and memory usage can be monitored using the task manager, which provides information on the running of the DCS. Tables 3 and 4 show the processor and memory usage of controllers, Main Database (MDB) servers, OISs, and EWSs when network traffic is inflicted DCS networks. The identified process controllers, servers, OISs, and EWSs continued to perform their functions and were loaded to levels lower than the maximum levels under network failover conditions.

4.3. *Packet loss and error rate*

Packets can be lost; this process includes both failures to receive an uncorrupted packet and failures to acknowledge the receipt of a packet. Packets can be corrupted due to errors in communication processors and errors introduced in buffer interfaces, in the transmission media, or from the interface. Packets can be delayed beyond their permitted arrival time window, including through errors in the transmission medium, congested transmission lines, faulty interface devices, or delays in sending buffered packets [15].



Destination
- ● All devices (broadcast)
- ○ Background traffic (multicast)
- ○ Single destination

Traffic
- Presets: Custom
- Protocols: Benign IP
- TTL: 2
- TOS(QOS): Normal
- MTU: 1500 bytes
- # Frames: Continuous
- Duration: ∞

Frame size 1436 Bytes
Rate 437/s
Utilization 5.09%

192.168.8.254

Fig. 5. Traffic generating test for DCS networks. DCS, distributed control system; IP, Internet Protocol; MTU, Maximum Transmission Unit; QOS, Qaulity of Service; TOS, Type of Service; TTL, Time to Live.

Table 3
Processor usage of controllers, MDB server, OIS, and EWS generating traffic to DCS networks.

Traffic	Controller A	Controller B	Main DB server	OIS	EWS
Requirement	Less than 60%	Less than 60%	No requirement	No requirement	No requirement
Average rate (15.61 Mbps)	24%	31%	6.4%	13%	12%
Average rate + 10 Mbps	28%	36%	6.8%	14%	13%
Average rate + 20 Mbps	33%	42%	6.9%	14%	13%
Average rate + 23.79 Mbps (network failover condition)	34%	43%	7.0%	14%	13%
Average rate + 30 Mbps (for the reference)	37%	44%	7.1%	14%	13%
Average rate + 40 Mbps (for the reference)	39%	54%	7.4%	14%	13%

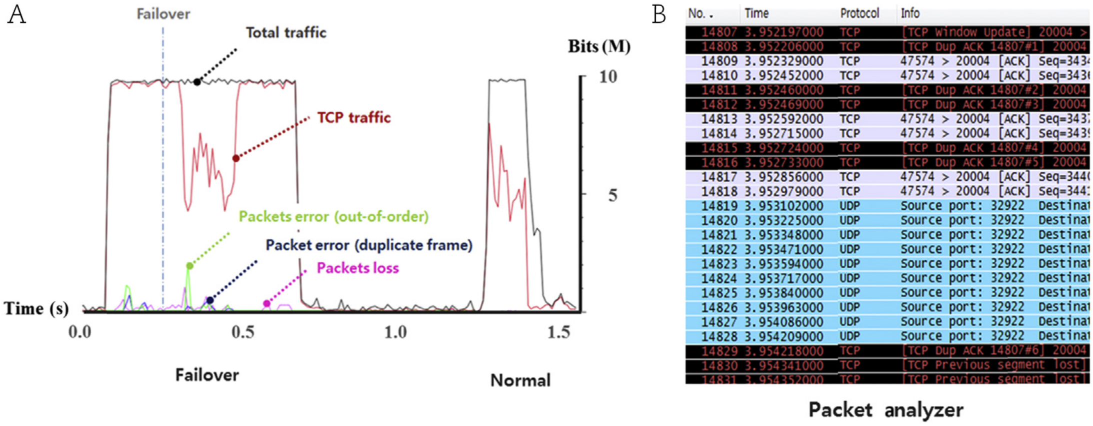
DB, Database; DCS, distributed control system; EWS, engineering workstation system; MDB, Main Database; OIS, operator interface system.

Table 4
Memory usage of controllers, MDB server, OIS, and EWS generating traffic to DCS networks.

Traffic	Controller A	Controller B	Main DB server	OIS	EWS
Requirement	Less than 60%	Less than 60%	No requirement	No requirement	No requirement
Average rate (15.61 Mbps)	22%	24%	39%	26%	25%
Average rate + 23.79 Mbps (network failover condition)	22%	24%	39%	26%	25%
Average rate + 30 Mbps (for the reference)	22%	24%	39%	26%	25%

DB, Database; DCS, distributed control system; EWS, engineering workstation system; MDB, Main Database; OIS, operator interface system.

The increment of packet error or loss can cause the delay of DCS signals. Packet error or loss can generate retransmission of a packet in the Transmission Control Protocol/Internet Protocol, and the retransmission can cause a delay in the response time of DCS. The tolerance limits for packet error or loss rate can be identified through response time measurement. Packet errors or losses can be monitored by port mirroring at network switches using a network analyzer. A managed network switch also provides packet error



```
No.   Time         Protocol  Info
14807 3.952197000  TCP       [TCP Window Update] 20004 >
14808 3.952206000  TCP       [TCP Dup ACK 14807#1] 20004
14809 3.952329000  TCP       47574 > 20004 [ACK] Seq=343
14810 3.952452000  TCP       47574 > 20004 [ACK] Seq=343
14811 3.952460000  TCP       [TCP Dup ACK 14807#2] 20004
14812 3.952469000  TCP       [TCP Dup ACK 14807#3] 20004
14813 3.952592000  TCP       47574 > 20004 [ACK] Seq=343
14814 3.952715000  TCP       47574 > 20004 [ACK] Seq=343
14815 3.952724000  TCP       [TCP Dup ACK 14807#4] 20004
14816 3.952733000  TCP       [TCP Dup ACK 14807#5] 20004
14817 3.952856000  TCP       47574 > 20004 [ACK] Seq=344
14818 3.952979000  TCP       47574 > 20004 [ACK] Seq=344
14819 3.953102000  UDP       Source port: 32922  Destinat
14820 3.953225000  UDP       Source port: 32922  Destinat
14821 3.953348000  UDP       Source port: 32922  Destinat
14822 3.953471000  UDP       Source port: 32922  Destinat
14823 3.953594000  UDP       Source port: 32922  Destinat
14824 3.953717000  UDP       Source port: 32922  Destinat
14825 3.953840000  UDP       Source port: 32922  Destinat
14826 3.953963000  UDP       Source port: 32922  Destinat
14827 3.954086000  UDP       Source port: 32922  Destinat
14828 3.954209000  UDP       Source port: 32922  Destinat
14829 3.954218000  TCP       [TCP Dup ACK 14807#6] 20004
14830 3.954341000  TCP       [TCP Previous segment lost]
14831 3.954352000  TCP       [TCP Previous segment lost]
```

Fig. 6. Packet error and loss rates. (A) Trend and (B) detailed information of packet losses and errors. TCP, Transmission Control Protocol; UDP, User Datagram Protocol.

information on error type. Each port of a managed network switch can separately display an error counter, and this gives the engineer the ability to see what kinds of errors are going over ports.

Packet error and loss rates were accumulated at fan-out (application), root (distribution), and core switches. The highest rates recorded were 0.9% for packet error rate caused by out-of-order segment and duplicate to the ACKs, and 2.1% for packet loss rate at a root switch during network failover (Fig. 6). Packet error and loss rates can affect DCS response times for hundreds of milliseconds, but can be ignored in terms of meeting the response time requirements, as shown in Table 1.

5. Conclusions

Unplanned failover of DCS networks is an important factor in determining the reliability of data transmission. Data communication bandwidth, processor performance, packet loss, and error rates during network failover from redundant networks can be causes of data delay or transient transmission stoppage. Network failover was verified to meet communication-related requirements during the design and manufacturing phases. However, integrity tests of DCS redundant networks have not yet been fully verified because not all relevant subsystems and equipment were completely installed in the target environment during these phases.

In this study, network verification tests and a methodology for network failover were developed; verification tests for DCS networks were carried out during the installation and commissioning phases. Network traffic increased 2.52 times and processor usage of controllers generally increased 13% at an additional 30% traffic, but all values remained under the specified requirements. When the response time test was conducted using Transmission Control Protocol transaction packets, packets also arrived within the specified response time, despite a 2.1% packet loss rate.

This study is expected to provide verification tests and methodology that can ensure the effects of network failover. When applying failover verification to new DCS redundant networks, this method maintains high reliability of DCS redundant networks in digitalized nuclear power plants.

Conflicts of interest

There is no conflict of interest statement.

References

[1] Electric Power Research Institute, Technical Results 1011711 Final Program on Technology Innovation Network Management Technology Applied to Power Plant Instrumentation, Control, and Maintenance, July 2005.

[2] National Research Council, Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, National Academy Press, Washinton DC, U.S, 1997.

[3] D.-Y. Lee, K.-C. Kwon, C.-H. Kin, D.-H. Kim, S. Hur, J.-S. Lee, Development experience of a digital safety system in Korea, in: Proceedings of the IAEA Technical Meeting on the Impact of Digital I&C Technology on the Operation and Licensing of NPP, 2008.

[4] S.-H. Lee, H.E. Kim, K.S. Son, S.M. Shin, S.J. Lee, H.G. Kang, Reliability modeling of safety-critical network communication in a digitalized nuclear power plant, Reliab. Eng. Sys. Saf. 144 (2015) 285–295.

[5] G.G. Preckshot, NUREG/CR-6082 Data Communications, U.S. Nuclear Regulatory Commission, August 1993.

[6] D.-H. Kim, A Safety-Based Protocol for Data Communication Network Structure in Nuclear Power Plants, Hannam Press, Daejeon, South Korea, August 2006.

[7] H.-S. Ryu, M.-G. Min, M.-S. Kim, H.-K. Jung, Packet data analysis of non-safety network system for power plant, in: Proceedings of the ICS2014 Information and Control, April 2014.

[8] LAN/MAN Standards Committee of the IEEE Computer Society, Carrier sense multiple access with collision detection access method and physical layer specifications, in: IEEE 802.3 Section 3, December 2012.

[9] E. Halepovic, C. Williamson, M. Ghaderi, Enhancing redundant network traffic elimination, Comput. Netw. 56 (2012) 795–809.

[10] S.-W. Lee, Design of a Communication Network Protocol for the Distributed Control System of Nuclear Power Plant, Konkuk Press, Seoul, South Korea, August 1999.

[11] Y.-C. Shin, Design and Analysis of High Reliability Data Communication Network Structure for Nuclear Power Plant, Yonsei Press, Seoul, South Korea, June 2002.

[12] J.-Y. Byeok, Design of Fault-Tolerance Communication Network for Nuclear Safety System, Inha Press, Incheon, South Korea, December 2011.

[13] K. Jayaswai, Administration Data Center: Servers, Storage, and Voice Over IP, Wiley Publishing, New Jersey, U.S, 2006.

[14] Y.C. Shin, J.Y. Lee, H.Y. Park, S.H. Seong, Response time test for the application of the data communication network to nuclear power plant, in: 2002 International Congress on Advances in Nuclear Power Plants, American Nuclear Society, June 2002.

[15] IEEE Power & Energy, Criteria for digital computers in safety systems of nuclear power generating stations, in: IEEE Std 7–4.3.2, Nuclear Power Engineering Committee, August 2010.