Design and Implementation of Fault Tolerance Network in Launch Control System

Il-Hyung Jung, Jae-Chel Ahn, Kyung-Rok Moon, Jae-Yong Lee, Byung-Chul Kim

Abstract— Because the network of Launch Control System (LCS) handles a volume of critical data in a server environment and a minor fault in the network can cause uncontrollable status during periods of launch campaign time, the network should provide the very reliable service. To achieve the goal, this paper discusses what requirements the network expects and what differences the network has comparing to other common networks. After considering requirements, differences and compatibility with Supervisory Control and Data Acquisition (SCADA) system, the physical and logical configurations for the LCS network are proposed to improve the reliability and efficiency. The experimental results show what values in failover parameters are the most suitable for the LCS network. And other results and traffic shapes which are measured during practical operational period confirm that the traffic and processing load are effectively redistributed as planned.

Index Terms— Fault tolerance network, Industrial network, Launch Complex (LC), LCS, SCADA

I. INTRODUCTION

Korea Space Launch Vehicle-1 (KSLV-1) placing a 100 kg-class satellite into a 300 km low-orbit is the first space launch vehicle in Korea and was jointly developed with Russia as a part of the national space development program. Naro Space Center, the first spaceport in Korea, completed its system installations and tests by June 2009 and performed its launch missions in August 2009, June 2010 and January 2013 respectively with the LC, Assembly Complex (AC), other tracking stations and facilities. After the first and the second stages containing a satellite are integrated and checked in the AC, the Integrated Launch Vehicle (ILV) is moved to the LC. The LC system does the final checks of the ILV and fills it with kerosene and liquid oxygen as well as provides the launching platform. The LC system is mainly composed of three types of ground support equipments, Mechanical Ground Support Equipment (MGSE), Fuel Ground Support Equipment (FGSE) and LCS, which are located in a launch field and a Launch Control Center (LCC) [1]. The MGSE and the FGSE are responsible for mechanical control on the ILV and fuelling processes respectively. The LCS, organized into clusters of computers, controls and monitors the field equipments, MGSE, FGSE and ILV. The LCS enables operators to measure physical parameters from sensors in the remote field as well as issue output signals to valves or pumps using controllers [1], [2]. The LCS performs very complicated and elaborate operations through automatic processes of exchanging information with numerous interconnected devices.

Lots of critical data are expected and every packet wants to be guaranteed in the LCS. But even a minor failure in the network is able to make the LCS out of control for a considerable period of time and cause enormous cost. For this reason, the LCS should contain very reliable network(s) with fault tolerance architecture which enables the persistent data exchange during fault(s). The LCS network is actually hard to adopt common solutions, i.e. network products for office environment, failover mechanism for Internet Service Providers (ISP), etc., because its operating conditions, traffic characteristics, compatibility with a SCADA system and types of faults are significantly different. So, based on differences, this paper focuses on providing a reliable network in the LCS. The organization of this paper is as follows. In section II, previous works are reviewed. In section III, we discuss the requirements which should be considered in the design of a LCS network as well as the basic architecture of the LCS. The proposed configuration of the network is described in section IV. Test results are presented in section V. Finally, conclusions are summarized in section VI.

II. PREVIOUS WORKS

A. Office and Industrial Network

The Ethernet is the most commonly used and has the superior market share in communication technology. But the Ethernet was not considered suitable carrier to deliver the control traffic at the start because delay times can vary, and performance according to traffic volume is difficult to estimate. In spite of innate defects, the Ethernet has been very well developed and is overcoming its weaknesses continuously in both hardware and software due to the powerful advantage of open architecture. Because of worldwide adoption and wide range of application, the Ethernet and its applications have proven to be a robust solution that can meet the unique needs of the manufacturing environment [3], [4], [5], [6]. But the majority of Ethernet solutions had no particular protection against environmental effects because they have been mainly developed for the use of stable environments [7]. For this reason, the Ethernet under harsh environments such as

Revised Version Manuscript Received on April 11, 2016.

Il-Hyung Jung, "Launch Complex Department, Korea Aerospace Research Institute" / "Information and Communication Engineering Department, Chungnam National University", Daejeon, Rep. of Kore.

Jae-Chel Ahn, Launch Complex Department, Korea Aerospace Research Institute, Daejeon, Korea.

Kyung-Rok Moon, Launch Complex Department, Korea Aerospace Research Institute, Daejeon, Rep. of Korea.

Jae-Yong Lee, Information and Communication Engineering Department, Chungnam National University, Daejeon, Rep. of Korea.

Byung-Chul Kim, Information and Communication Engineering Department, Chungnam National University, Daejeon, Rep. of Korea.

Fig. 1. Mechanical Control on ILV by MGSE

industrial fields has been requested to use more long-lasting hardware components with a high degree of

protection. The hardware of industrial Ethernet includes industrial-grade components, redundant power supplies with 24volts DC, convective cooling to provide reliable operation under dusts or other particles and outstanding durability in fluctuant temperature and vibrations which frequently happen in the field.

Many different types of proprietary buses based on the digital signal technology were also developed in the industrial market to take the place of previous analogue to reduce the volume of cabling and cut the costs. But due to the lack of compatibility with other vender's products, the technologies were forced to make a new leap to the standardized protocol. Several additional layers on top of existing standard protocols allow the industrial Ethernet itself to be more deterministic and achieve rapid diffusion of their applications [3], [4], [8]. By providing a standardized format, traditional tools and applications are also available in industrial Ethernet without whole modification.

B. Failover Protocol

A failover of communication network means the ability to switch automatically from active equipment or line to redundant or standby equipment or line(s) when the active one becomes unavailable for processing traffic. Many effective schemes have been proposed and their weaknesses are constantly being addressed because the failover is the most import capability to achieve high availability in a computer network. The Hot Standby Router Protocol (HSRP) proposed by Cisco Company is a very useful switchover protocol in

TABLE I
FAILOVER TIME IN L2 AND L3 PROTOCOLS

Protocol	Failover Time	
SLMT	0.47 sec	[8]
HiPer Ring	0.5~0.8 sec	[14]
HSRP	4~13 sec	[9]
RSTP	1.7~5 sec	[8, 14]
STP	45~60 sec	[10]

layer 3. Because HSRP uses two kinds of messages, i.e. Hello time and Hold time messages, to determine the health status of adjacent routers, it needs several seconds to switchover [9]. [10]. Although Link Aggregation Control Protocol (LACP) is able to increase link speed and availability using multiple ports in a LAN switch, it is faced with the difficulty of providing redundancy schemes in different subnets. Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP), operating at layer 2, have fast recovery performance, but the performance can vary proportionately with the number of nodes in the network topology [10], [12], [13]. The Hiper Ring scheme used for ring topology and the Split Multi Link Trunking (SLMT) algorithm have shortcoming of almost proprietary protocols and their specific devices even though they have the merit of short recovery time as shown in Table I [8], [14].

C. SCADA System

A SCADA system is commonly used to control field equipment automatically in a wide range of industrial sites. A SCADA system usually consists of many parts, i.e. remote terminals and controllers for acquiring and processing signals, network devices for data exchange, application software for data distribution and Human Machine Interface (HMI), end nodes including view nodes and SCADA servers, etc., SCADA systems have evolved gradually with the technologies of network and load distribution. The first generation, standalone SCADA, processed all calculations with no connection to other computing stations, and therefore incurred lots of costs and limitations on processing capability. The second generation was the so-called distributed system which shared information to be processed in real time across multiple stations. But proprietary protocol forced user to use a particular vendor's solution. The third generation, networked SCADA is based on open and standard communication protocols which allow engineers to use a mix-and-match individual product from different vendors rather than a whole vendor-dependant system [15], [16]. Networked SCADA systems are the recent trend in the market of controllers, SCADA servers and application software. The compatibility with standard protocol also has reduced the cost of upgrading a system.

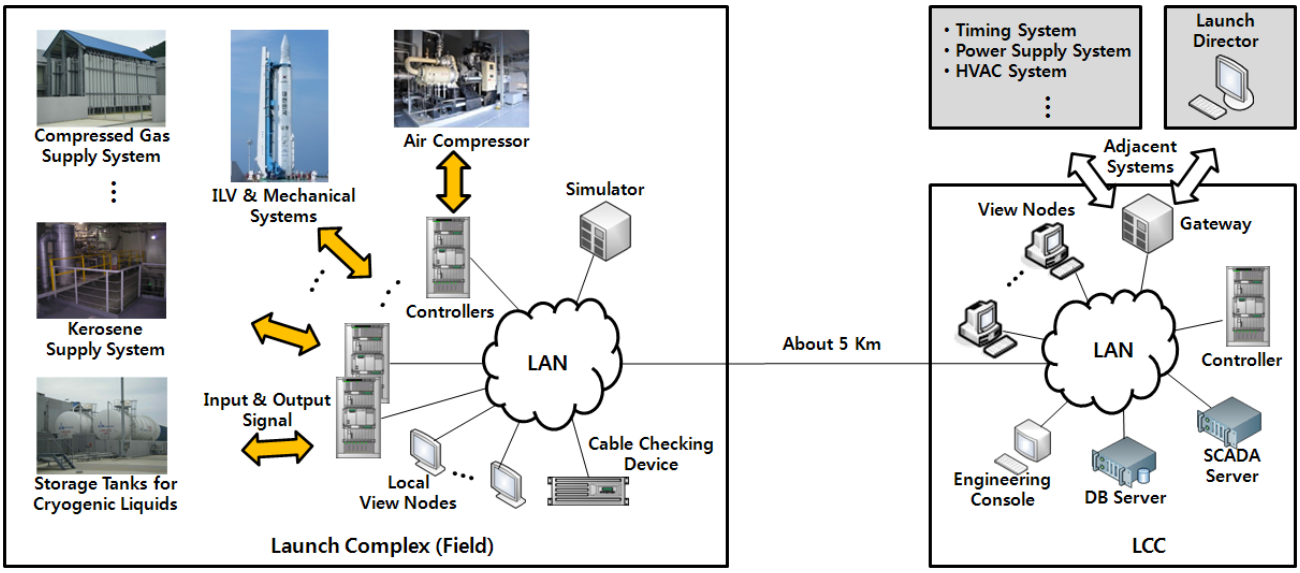

Fig. 2. Basic Architecture of LCS

III. ROLES AND REQUIREMENTS OF LCS NETWORK

A. *Basic Architecture of LCS*

The ILV and LC are composed of a great many pieces of critical and sensitive devices. They require elaborate and time-consuming work including pressure control of an oxygen tank, flow control of gases and propellants, level control of a water tank, temperature control in the ILV, pump control of a nitrogen supply system, hydraulic control of an ILV erector and pneumatic control of umbilical connectors [1]. For that reason, automation is essential to perform such numerous and complicated controls in consecutive order. The main function of the LCS concentrates on providing automatic and flawless control on expensive and dangerous field devices including an ILV.

Figure 2 shows the basic architecture of the LCS. Controllers, the most critical devices mainly installed in the field, perform arithmetic and logical operations through CPU modules. Analog and discrete Input and Output (I/O) modules in controllers directly collect the data from flowmeters or other transducers in the field as well as issue output signals to valves or other actuators according to the algorithms loaded in the CPU modules [2]. SCADA servers collect the data from controllers and allow view nodes to access the acquired information through the shared memory on them. They also deliver the commands from view nodes to corresponding controllers [17]. View nodes, i.e. appropriate workstations, provide HMIs for operators to check the control processes.

In addition to SCADA components, the LCS includes various nodes such as gateways exchanging data with adjacent systems, database servers providing archived data, engineering consoles monitoring the health status of every end device, network devices and simulators. Because the LCS consists of numerous devices on a computer network as mentioned above, the LCS requires both reliable communications and effective processing abilities with open architecture [18].

B. *Network Device*

The LCS carries lots of critical data to be collected, monitored, controlled and presented through various types of nodes on a computer network. Such a huge volume of data can cause processing overload and a considerable data loss in our system. The basis for a reliable LCS network is to select proper network devices with high availability and enough capability in traffic processing. As an engineer, it is necessary to consider which type of devices for data exchanging, i.e. hub, switch and router, are suitable for the LCS on the basis of data exchanging method and operating layer in Open Systems Interconnection (OSI). Furthermore, an engineer must keep in mind that the network of LCS differs from others in that it runs in a severe environment and carries various types of packets such as ModbusEthernet and Object Linking Embedding (OLE) for Process Control (OPC) as well as typical TCP/IP. For these reasons, the network devices should be harmonious with the expected packets and be more durable against shock and vibration during lift-off. When designing the LCS network, an engineer is also requested to calculate the expected traffic volume and disperse bottleneck nodes where traffic congestion can happen.

All components of the network, i.e. a Network Interface Card (NIC), LAN cables and a power supply as well as a switch or router, must support redundant configurations at the physical layer because the high reliability and high availability are our ultimate goals.

C. *Remote Control and Network Domain*

The LCS is required to monitor the status of every controlled field device constantly during prelaunch and launch period to carry out the planned processes flawlessly. However, it is usually difficult to station the operation staff near the launch site during the launch campaign due to safety.

So, the main operating room, LCC, is located far from the dangerous launch site whereas most controllers should be in the field. A computer network with fiber optic cable is suitable for the remote site because it can provide essential infrastructure for remote control. In addition, the attenuation ratio in the fiber optic cables should be measured periodically to check continuity, connector status, and loss value after installation.

An industrial network is recommended to be further divided into several domains to provide independent operation [3]. The LCS network must also be separated into more than two subdomains, control and data subdomains or more, for serving the same purpose. The data domain, i.e. lower level collecting and distributing the acquired data from the field, should be able to carry large amounts of data in the network. A control domain mainly focuses to deliver command and report packets containing main events. Because network delay and jitter are very strict requirements in forwarding the commands and reports, the control domain should be separated from the data domain in LCS even though a very small volume of traffic is expected in the control domain. In addition to domain separation, the LCS also needs to be separated from the outside Internet to prevent operators' distraction and attacks by hackers.

D. Other Requirements

Basically, a SCADA server acts as an inter-mediator between view nodes and controllers in a SCADA system. The SCADA server interchanges data with different types of controllers through various formats of protocols and forwards the processed data to view nodes [6], [17]. In other words, it integrates lots of view nodes with geographically distributed controllers along with network devices supporting various communication protocols. For the reason, both SCADA servers and network devices are important elements to improve flexibility and availability in the network. The engineer should find what the most effective failover scheme for the LCS network based on network size, traffic volume, traffic type, traffic characteristics and expected recovery time.

Another consideration is that the packets on the LCS network don't need to be classified for a certain level of quality using Quality of Service (QoS) or Differentiated Services (Diffserv) because all packets on LCS have their duties and want to be guaranteed. Consequently, the LCS is recommended to pay more attention to calculations of required bandwidth and redistribution of the traffic than queuing policies to provide reliable service.

IV. CONFIGURATION OF LCS NETWORK

Based on the requirements described in section III, in this section, we discuss how network devices in the LCS should be connected to each other in physical and logical level to provide reliable and efficient service.

A. Overall Network Topology

The LCS network is based on industrial Ethernet switches because the industrial products have proven successful in various critical fields and switched Ethernet is able to reduce the risks associated with the non-deterministic nature of the connectionless communication [4], [6], [19]. LCC and LC are

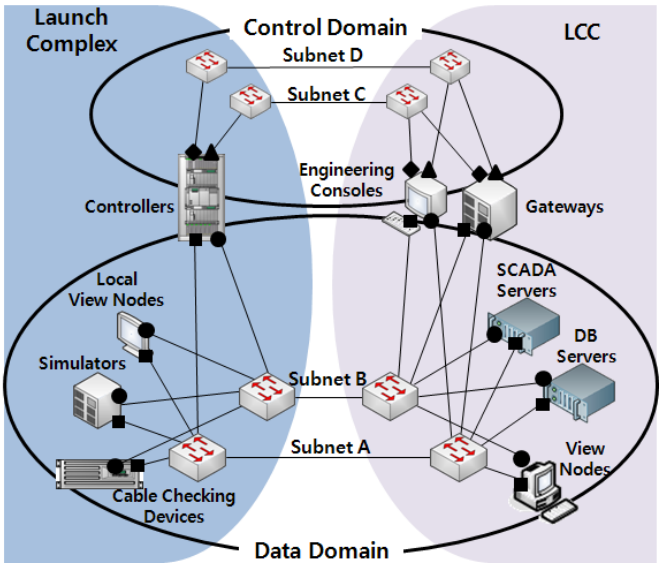

Fig. 3. Physical Configuration of LCS Network

Fig. 4. SCADA Servers and Industrial LAN Switches in LCC

connected by optical fibers to provide high bandwidth and tolerance to Electro Magnetic Interference (EMI). Every end node is wired up to switches with Shielded Twist Pair (STP) cables to block potential EMI from neighboring cables or rotary engines. Whereas a wireless network is able to reduce overall cost and provide mobility due to easy installation and cable free characteristics [20], but it is difficult to apply in the LCS because of its inherent weakness on security, seamless serviceability, its limited application on field devices and

Radio frequency interference with the ILV.

A network topology to be chosen has direct influences on the network performance such as expandability, wiring cost, complexity and reliability as well as the number of network switches to be used. To achieve our ultimate goals, reliability and availability are considered as our key elements for the topology of LCS network as well as cable complexity. Ring topology, one of the leading candidates in an industrial network, is able to achieve high availability and easily forms a redundant configuration.

But ring topology has several disadvantages such as cable complexity, vendor-dependent failover algorithm which covers switch to switch area and inconsistent performance when a changeover occurs [4], [21]. Consequently, LCS is configured with a dual tree topology providing overall redundancy as well as affording high availability as shown in Fig. 3. Other topologies such as bus or daisy chain were excluded from our consideration because they suffer a high impact when a connection is lost [4]. We divide the LCS network into two parts, i.e. a control domain and a data domain for stabilization of the control domain regardless of traffic fluctuation in another domain. Engineering consoles which are connected to both domains are able to monitor the whole status of our network using an application software such as Network Management System (NMS).

The configuration also focuses to decentralize the load of data processing because the high concentration of traffic is inevitable with only one server and processing overload is expected as well [15], [17]. So, we divide the expected traffic into two groups, namely server A group and server B group, to distribute considerable processing load into two groups as well as offering redundancy service with hot-standby architecture in each server group. Each controller is assigned to corresponding SCADA servers in A or B group depending on the number of its I/O tags to be processed on a server and its operational characteristics.

B. Logical Configuration for Controllers and Servers

The dual Ethernet cards in each controller which we chose are able to send the same data simultaneously to two independent nodes even though they are assigned to different subnets [22]. This is the critical feature to decide a redundancy scheme because it enables each primary and secondary server to build the same database at the same time. The redundant databases through two servers influence the additional reduction of processing load as well in that the dual databases are able to distribute clients, i.e. view nodes, to a primary or a secondary server in a group.

Two NICs in every SCADA server are also very helpful to improve the availability. The individual setting of an active path in every server is able to minimize the traffic loss in case of a failure as well as provide redundant architecture because the active paths for each primary and secondary server can be set differently in the LCS as shown in Fig. 5. For example, when subnet A fails (square symbol in Fig 5), two servers, SA-2.B and SB-2.B, are able to keep their connections with their controllers whereas others, SA-1.A and SB-1.A, try to change their connections to subnet-B. That is to say that at least one server in each server group is able to build the database without any data loss while failovers for other two server are in progress. If this configuration is not applied in the LCS, all four servers have to change their paths with lots of data loss when a default subnet fails.

C. Failover Mechanism in I/O Driver

An effective failover in LCS network needs to adequately consider combining a SCADA system with an IP network as described before. Fig. 6 shows the simplified functional modules of software in a SCADA server. Firstly, an I/O driver reads data from its controllers and writes them in an internal

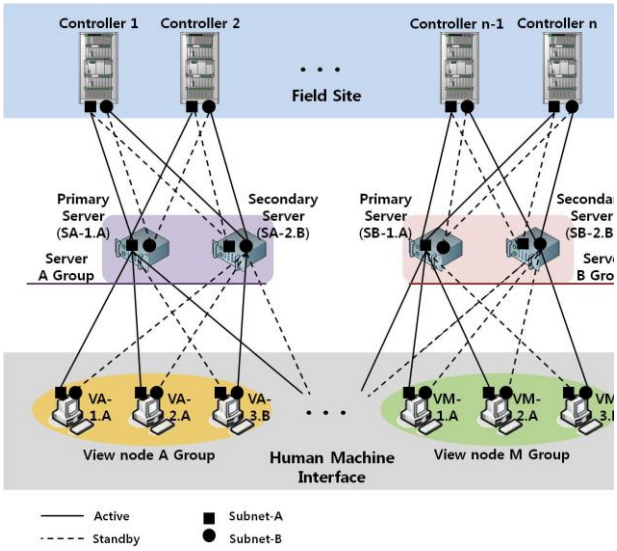

Fig. 5. Logical Configuration in LCS Network

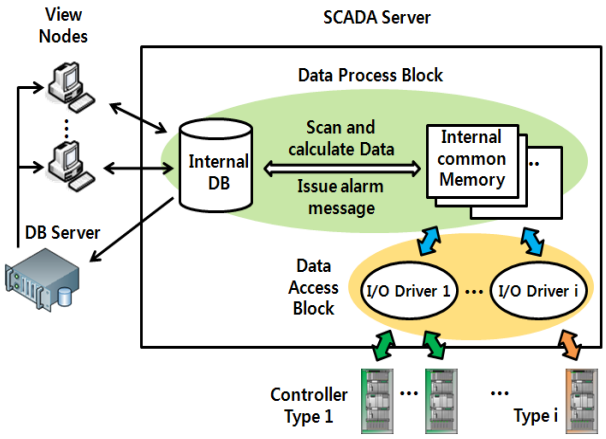

Fig. 6. Functional Architecture of a SCADA Server

common memory. The data processing module in the software scans the data from internal memory and processes them to write to an internal database. Finally, view nodes access the internal database in a SCADA server according to their network configurations and display the corresponding data on the screen. In addition to data processing, the I/O drivers of today are able to provide powerful mechanisms through reserved routes to guarantee end-to-end failover as well as support different types of open communication protocols from controllers to be mix-and-match [21].

The I/O drivers request the data from controllers with very short scan time. For the reason, the I/O drivers are able to examine the corresponding area of our network very closely, i.e. from SCADA servers to controllers regarded as the most critical part. An I/O driver tries several retransmissions and then selects another path via a secondary interface based on internal failover settings unless the I/O driver receives the response packet from a corresponding controller within the specific waiting time [23].

One of the most important considerations to use the I/O driver as failover mechanism is that unnecessary routes should be removed from failover setting to avoid considerable adverse effects because the I/O driver has the possibility to spend much time in finding unavailable paths when a fail occurs. The failover mechanism by I/O drivers is very analogous to the multihoming algorithms [24] such as AllRtxAlt, AllR tx Same or FrSame RtoAlt operating in the transport layer because they provide end-to-end fault tolerance and the parameters of timeout, retransmission and delay play an important role in failover performance. Thus, optimizing the parameters depending on fault types and traffic characteristics is the most influential activity in improving the failover performance in the LCS network.

D. Logical Configuration for Servers and View Nodes

Two Ethernet ports in every view node allow dual physical connections between a SCADA server and a view node. The client software in a view node is responsible for collecting the processed data from the corresponding SCADA server after searching the target server based on its server's name [23]. Thus, a "hostfile" mapping node names to IP addresses is able to play a leading role in deciding a primary path among two interfaces of a view node when it searches the target server. A primary and a secondary path in each view node can be easily set by not inserting or inserting a dash and the letter R following a node name in a "hostfile". For example, VA-1.A and VA-2.A are set to collect the data from the primary SCADA server (SA-1.A) through subnet-A by inserting -R at the tail of corresponding hostnames with subnet-B whereas VA-3.B gathers the data from the node of SA-2.B through subnet-B by inserting -R at the tail of corresponding hostnames with subnet-A as shown in Fig. 5. Ultimately, the suggested changes on hostfiles will lead the traffic to be distributed into two subnets.

V. EXPERIMENTAL AND OPERATIONAL RESULT

Our operational results for more than 6 years show that congestion or considerable fluctuation of traffic doesn't occur due to strict restrictions on traffic types and the number of access nodes in the LCS network. Hardware faults, on the other hand, such as damage to Ethernet connectors, faults of NICs, and even malfunction in an industrial switch device due to its firmware bug were experienced with very low frequency. The faults are sure to happen in an unknown future and it can be the time just before lift-off. And traffic concentration to a default path is commonly observed and it causes misallocation of network resources. For the reasons, the following experiments mainly focus to show the impact of failover parameters in failover performance and the results of the proposed configuration to redistribute the traffic.

A. Failover Performance

The server scans the data from a corresponding controller depending on the scan time in an I/O driver. The data itself practice good works as probe packets which monitor the network status without additional overload because a server periodically requests the data to a controller with very high frequencies, i.e. a period of 0.01 ~ 0.025 second in our case. Reply timeout, one of the key failover parameters which

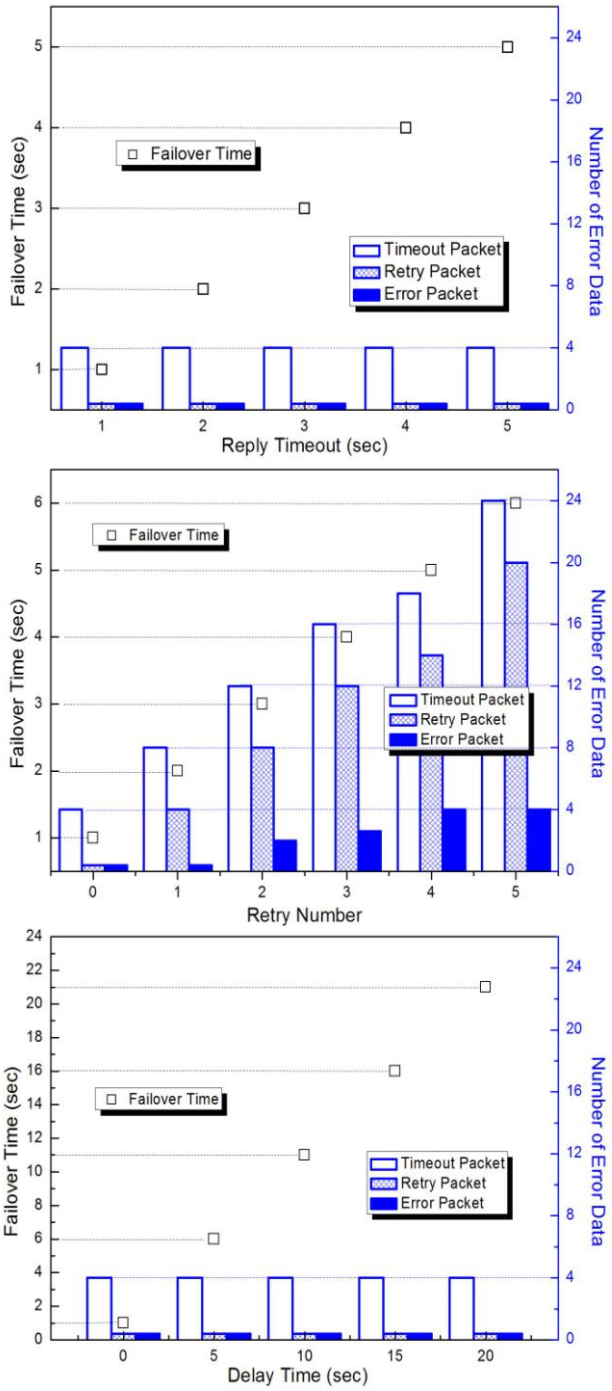

Fig. 7. Number of error data as failover parameters increase

represents waiting time for a response from a controller, should be set properly in an I/O driver after carefully considering sending, processing and receiving time for the data. If the value of reply timeout is too short, the I/O driver is very sensitive on response time and may cause unnecessary failovers. If too long, an operator would face long inoperable time for a problem. In the same approach, Retry number, the number of times I/O driver re-send a request to the same interface after reply timeout, and delay time, waiting time before using another physical interface after all retries fail, also need to be optimized depending on its own network characteristics [24], [25].

Fig. 7 shows how failover time and the number of error data change according to the values of key failover parameters, i.e. reply timeout, retry number and delay time, when a hardware fault occurs. The first graph in Fig.7 represents that the more time the intended failover needs as the value of reply timeout increases whereas the parameter doesn't influence the number

Of error data. In other words, the minimum value in the parameter causes the fastest failover. In the previous works, the process of tunning the values of reply timeout affects the failover performance significantly under the condition of temporary traffic congestion [24], [25]. But the event of reply timeout which is caused by a hardware fault means that the existing path is not available any more. And the second graph in Fig. 7 shows the number of retries proportionally increase the number of error data and the failover time. For example, twice retries cause 12 timeouted packets and 8 retried packets because twice retries mean that 4 packets, the unit which the I/O driver sends at a time, are retransmitted twice to the same interface after a timeout event occurs. When all retries are finished, the I/O driver regards the corresponding packets as error packets according to its internal processes. The third graph also shows that delay time doesn't influence the performance of failover. So, the above results show that the driver should retransmit the data to a reserved interface as soon as possible because traffic congestion doesn't occur in the LCS and a timeouted packet means the practical impossibility of transmitting data to the first interface containing a physical fault. In conclusion, the smaller value the driver has for the above parameters, the better performance the LCS network has in failover contrary to previous works. Our failover time which covers end to end nodes takes 1 second due to minimum timeout values recommended in RFC 2960 [23], [24], [25]. Additionally, another tests show that I/O driver setting with unnecessary path(s) spend much more time for recovery, about 2~120 seconds, which comes from spending time to find unnecessary paths.

B. Traffic Redistribution

Traffic redistribution mainly aims to deliver the data to corresponding devices through multiple routes. The traffic redistribution is able to reduce an additional processing load as well as increasing network efficiency because the redistribution has close correlation with resource allocation and network switchover. If the LCS traffic is fully concentrated in a specific network, all data should be moved to another network when physical failure occurs. And the data sessions should be reestablished with controllers which results in additional overload in a server. So, section IV describes the results of our attempts to balance the traffic through "hosts" files, I/O drivers and dual NICs.

Table II shows the traffic volume of each subnet in unbalanced networks, where our logical configuration is not applied. Most of LCS traffic resides in the Subnet-A at the initial stage and 32.4% of the total traffic is moved to the Subnet-B in case a failure occurs in the field. When the LCC network is down, 87.5% of the traffic is moved. Because the traffic amount from LCC is much larger than the field, different amounts of traffic are moved in case of each failure.

TABLE II
TRAFFIC VOLUMES (MBPS) IN THE UNBALANCED NETWORK

Network	Initial Stage	Subnet-A Down in Field	Subnet-A Down in LCC
Subnet-A	18.9	11.9	0
Subnet-B	2.7	9.7	21.1

TABLE III
TRAFFIC VOLUMES (MBPS) IN THE BALANCED NETWORK WHEN A FAILURE OCCURS IN THE FIELD

Network	Initial Stage	Subnet-A Down in Field	Subnet-B Down in Field
Subnet-A	13.4	10	16.4
Subnet-B	8.3	11	4.4

TABLE IV
TRAFFIC VOLUMES (MBPS) IN THE BALANCED NETWORK WHEN A FAILURE OCCURS IN THE LCC

Network	Initial Stage	Subnet-A Down in LCC	Subnet-B Down in LCC
Subnet-A	13.3	0	20
Subnet-B	8.2	21	0

TABLE V
THE NUMBER OF ERROR DATA IN A CONTROLLER WHEN THE UNBALANCED OR THE BALANCED NETWORK IS DOWN

Error Type	Unbalanced Network Down	Balanced Network Down
Timeout Packet	16	8
Retry Packet	8	4
Error Packet	0	0

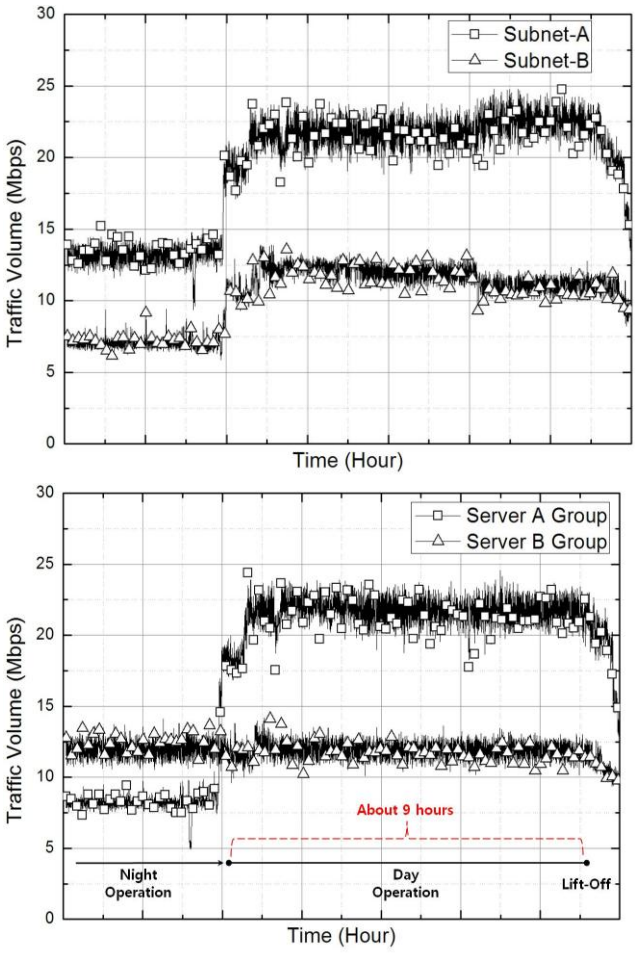

Fig. 8. Practical traffic shape in the LCS network during launch day

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

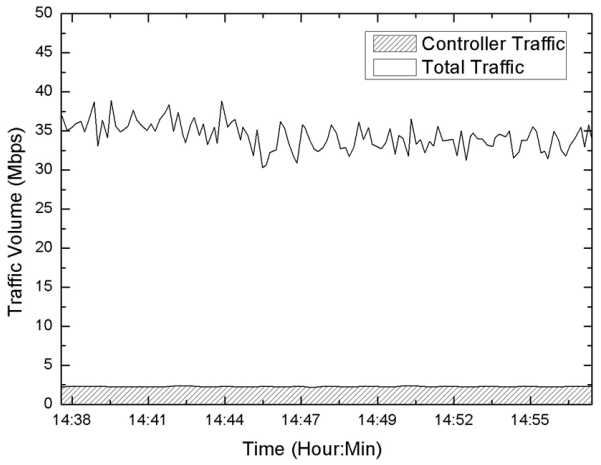

Fig. 9. Practical traffic volume of controllers during launch day

The total amount of LCS traffic is about 21Mbps varying a little from time to time according to the number of end nodes requesting the recorded data from the DB servers.

Tables III and IV show the results in a balanced network, where its default path in every node is distributed into two groups, i.e. Subnet-A and Subnet-B, according to the suggested configuration. At the initial stage in Table III, traffic share in network-A is reduced significantly from 87.5% to 61.75% whereas traffic share in network-B is increased from 12.5% to 38.25%. The Subnet-A still has higher share than the Subnet-B because two of three in each view group are connected to the Subnet-A as shown in Fig. 5. Table III shows that 15.7~18% in initial traffic is moved to its reserved network when failures occur in the field. In case of failures in the LCC network, more traffic, 38.1~61.9%, is moved as shown in Table IV . When a failure occurs in the field, the traffic volume doesn't drop to zero because the majority of view nodes occupying considerable traffic volume are still alive in the LCC. And the number of error data in a controller is described in Table V under the condition that the timeout value is set as 1 second and the retry number is set as 1. The test result definitely shows that the number of error

data in the balanced network is much smaller than the number in the unbalanced network when a failure occurs. That is to say that the balanced network with the proposed configuration is able to increase the efficiency of resources in a normal case and also able to reduce the number of error data in a failure case.

Fig. 8 shows the trend of LCS traffic at the day KSLV-1 was launched where we can confirm the results for traffic redistribution again. The first graph in Fig.8 shows that the Subnet-B also has considerable volume. As mentioned before, the reason why the Subnet-A has higher traffic volume than the Subnet-B is that two thirds of view nodes in LCC are connected to the Subnet-A based on our traffic policies. The second graph in Fig. 8 represents that the total processing load in the LCS is devided by two server groups. Server B group is responsible of controllers working days and nights continuously whereas A- group handling controllers mainly working days. In other words, Server A group has higher amount of traffic during the daytime than night whereas Server B group has constant traffic pattern. Fig. 8 also shows that LCS traffic has predictable patterns with little fluctuation in its volume unlike other networks because it's not connected to the outside Internet, and access nodes and data types are controlled by our planned traffic policies. Fig. 9 shows that controllers cover about 7% in the LCS' total traffic, i.e. about 35Mbps. And the share means that each view node handles much more traffic volume than a controller on average. Therefore, the number of view nodes displaying graphical information should be carefully planned and restricted based on expected traffic volume at its design stage.

VI. CONCLUSION

There are distinct differences between the LCS network and other common networks in that the LCS network has specific requirements, operational environment, traffic pattern and types of faults and it also requires compatibility with SCADA servers. Thus, common solutions are hard to be applied in the LCS network and instead based on the differences, specific network configuration and traffic handing schemes should be discussed to provide sufficient reliability for the network and lead the mission to a successful result.

The LCS network we propose is physically configured with dual tree topology with industrial switches, STP cables, two separated domains and two groups of SCADA servers in consideration of shock, EMI from rotary engines, the isolation of the most critical packets and high concentration of processing load. The I/O driver in the configuration is responsible for the fault detection and switchover of the LCS traffic because it closely monitors traffic status with very shot period in our case and doesn't need additional overload and provides end to end failover services for the most critical area as well. And the proposed configuration also focuses to redistribute the traffic from a default path to a reserved path using the I/O drivers, host files and dual NICs.

The experimental results show that the I/O driver has the best failover performance under the condition that the failover parameters, i.e. reply timeout, retry number and delay time, have the smallest values because a hardware fault means the practical impossibility of transmitting the data to a intended path. And the suggested configuration significantly increases the traffic share of a reserved network from 14.1% to 39% at initial stage and also reduces the error packets which move to a reserved network in case of a failure. The traffic shapes which are measured in launch day confirm that the efforts for redistributing both traffic volume and processing load works appropriately. And the last result represents that the number of view nodes should be carefully planned because the traffic volume in view nodes is much larger than the volume in controllers.

REFERENCES

1. H. Jung, D. K Hwang, K. R. Moon, D. R. Kim and S. H. Ra, "Control of Mechanical ground Support Equipment for Korean Launch Complex," in 3rd Asia-Pacific International Symposium on Aerospace Technology, Melbourne, Session2A, 2011

2. L. S. Klivans and S. B. Yochelson, "Computer Controlled Launch Control and Checkout of Operation Satellite Systems," IEEE Trans, Aerospace, vol. 1, pp.1249-1261, 1963
3. J. R. Moyne and D.M. Tilbury, "The Emergence of Industrial Control Network for Manufacturing Control, Diagnostics, and Safety Data," in Proc. IEEE, vol. 95, no. 1, pp. 29-47, 2007
4. Industrial Ethernet: A Control Engineer's Guide, [Online]. Available: http://www.cisco.com
5. H. Eto, H. Matsuo and F. Kurokawa "Network of Plant Remote Monitoring System Using UDP/IP for Wind-Farms," IEICE Trans, Communications, vol. E87-B, no. 12, pp. 3457-3464, 2004
6. KH. Mak and B.L. Holland, "Migrating electrical power network SCADA systems to TCP/IP and Ethernet networking," Power Engineering Journal, vol. 16, pp. 305-311, 2002
7. C. Kleedorfer, "Switch Based Industrial Ethernet Network," Computing & Control Engineering Journal, vol. 14, pp. 12-13, 2003
8. Ethernet Routing Switch 5000 Series, Competitive Performance Evaluation versus Cisco Catalyst 3750G and HP ProCurve 3400cl, No. 206106 [Online]. Available: http://www.tolly.com,
9. Cisco Hot Standby Router Protocol, IETF RFC 2281 [Online], Available: http://www.ietf.org/rfc/rfc2281.txt
10. J.T. Yu, "Applying IEEE802.1w to Improve Service Availability," IEEE International Conference on Dependable systems and Network, pp. B10-11, 2003
11. Link Aggregation Control Protocol, IEEE 802.1ad [Online], Available: http://standards.ieee.org
12. Spanning Tree Protocol, IEEE 802.1D [Online], Available: http://standards.ieee.org
13. Rapid Spanning Tree Protocol, IEEE 802.1w [Online], Available: http://standards.ieee.org
14. Product analysis: HiPER Ring vs. RSTP, [Online], Available: http://www.belden.com
15. R. H. McClanaban, "SCADA and IP: is Network Convergence Really Here?," IEEE Industry Applications Magazine, vol. 9, pp. 29-36, 2003
16. CW. Ten, CC. Liu and G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems," IEEE Trans, Power Systems, vol 23, pp.1836-1846, 2008
17. M.S. Thomas , P. Kumar, and V.K. Chandna, "Design, Development, and Commissioning of a Supervisory Control and Data Acquisition (SCADA) Laboratory for Research and Training," IEEE Trans, Power Systems, vol. 19, no. 3, pp. 1582-1588, 2004
18. B. Furht and R. Luken, "The Space Shuttle Launch Computer Control System at NASA Kennedy Space Center," in Proc. Euromicro '91 Workshop. IEEE Real Time Systems, pp.184-192, 1991
19. K. C. Lee, and S. Lee, "Performance evaluation of switched Ethernet for real-time industrial communications" Computer Standards & Interfaces, vol. 24, pp.411-423, 2002
20. S. Kjesbu, "Industrial Environment Proximity Switches," Communications Engineer, vol. 1, pp. 40-43, 2003
21. S. Rüping, E. Vonnahme,. and J. Jasperneite, "Analysis of Switched Ethernet networks with different Topologies used in Automation Systems" in Proc. Fieldbus Technology Conference (FeT '99), Megdeburg, pp351-358, 1999
22. Communication Interface P8151B, [Online]. Available: http://www.rockwellautomation.com/
23. MBE Driver, [Online]. Available: http://support.ge-ip.com/
24. Caro, "End-to-End Fault Tolerance Using Transport Layer Multihoming" Ph.D Dissertation, CISC Dept, University of Delaware, 2005
25. Stream Control Transmission Protocol, IETF RFC 2960 [Online], Available: http://www.ietf.org/rfc/rfc2960.txt

AUTHORS PROFILE

Il Hyung Jung received the B.S. degree in Electronic Engineering from Chosun University, Gwangju, Rep. of Korea, in 2000 and the M.S. degree in group of network engineering from ICU (currently KAIST), Daejon, Rep. of Korea in 2003. From 2004 to 2005 he worked for Ubiquoss Corporation as a network S/W researcher. He is currently working as a senior researcher at Launch Complex Department, Korea Aerospace Research Institute (KARI) and also working toward a PhD degree at information and communications engineering at Chungnam National University, Rep. of Korea. His research interests include network protocol, traffic engineering, automated control and sensor measurement.

Jae Chel Ahn received the B.S. degree in Computer Science from Howon University, Kunsan, Rep. of Korea, in 1999 and the M.S. degree in group of computer vision from Chonbuk University, Jeonju, Rep. of Korea in 2002. From 2002 to 2003 he worked for Point-I Corporation as a LBS (Location Based Service) S/W engineer. He is currently working as a senior researcher at Launch Complex Department, KARI, Rep. of Korea.

Kyung Rok Moon received his B.S., M.S. and Ph.D. degrees in Control and Instrumentation Engineering from Hanyang University, Rep. of Korea, in 1998 and 2000 respectively. He worked for Hyundai Motor Group as a control system engineer from 1999 to 2006. He is currently working as a principle researcher at Launch Complex Department, KARI, Rep. of Korea. His research interests include automated system, signal processing, and sensor measurement.

Jae-Yong Lee received his BS degree in electronics engineering from Seoul National University, Rep. of Korea and his MS and PhD degrees in electronic engineering from the Korea Advanced Institute of Science and Technology Daejeon, Rep. of Korea, in 1988, 1990, and 1995, respectively. From 1990 to 1995, he worked as a research engineer at the Digicom Institute of Information and Communications, Seoul, Rep. of Korea. Since 1995, he has been a professor at the Department of Information and Communication Engineering, Chungnam National University, Daejeon, Rep. of Korea. His research interests include computer networks, wireless Internet, sensor networks, and mobile communications.

Byung-Chul Kim received his BS degree in electronic engineering from Seoul National University, Rep. of Korea and his MS and PhD degrees in electronic engineering from the Korea Advanced Institute of Science and Technology, Daejeon, Rep. of Korea, in 1988, 1990, and 1996, respectively. From 1993 to 1999, he worked as a research engineer at Samsung Electronics, Suwon, Rep. of Korea. Since 1999, he has been a professor at the Department of Information and Communications Engineering, Chungnam National University, Daejeon, Rep. of Korea. His research interests include computer networks, wireless Internet, sensor networks, and mobile communications.