Journal of the Korean Society of Marine Engineering, Vol. 40, No.10, pp. 906~915, 2016
J. Korean Soc. of Marine Engineering (JKOSME)
https://doi.org/10.5916/jkosme.2016.40.10.906

ISSN 2234-7925 (Print)
ISSN 2234-8352 (Online)
Original Paper

The development of a ship's network monitoring system using SNMP based on standard IEC 61162-460

Zu-Xin Wu[1] · Sobia Rind[2] · Yung-Ho Yu† · Seok-Je Cho[3]

(Received September 20, 2016； Revised November 29, 2016；Accepted December 23, 2016)

Abstract: In this study, a network monitoring system, including a secure 460-Network and a 460-Gateway, is designed and developed according with the requirements of the IEC (International Electro-Technical Commission) 61162-460 network standard for the safety and security of networks on board ships. At present, internal or external unauthorized access to or malicious attack on a ship's on board systems are possible threats to the safe operation of a ship's network. To secure the ship's network, a 460-Network was designed and implemented by using a 460-Switch, 460-Nodes, and a 460-Gateway that contains firewalls and a DMZ (Demilitarized Zone) with various application servers. In addition, a 460-firewall was used to block all traffic from unauthorized networks. 460-NMS (Network Monitoring System) is a network-monitoring software application that was developed by using an simple network management protocol (SNMP) SharpNet library with the .Net 4.5 framework and a backhand SQLite database management system, which is used to manage network information. 460-NMS receives network information from a 460-Switch by utilizing SNMP, SNMP Trap, and Syslog. 460-NMS monitors the 460-Network load, traffic flow, current network status, network failure, and unknown devices connected to the network. It notifies the network administrator via alarms, notifications, or warnings in case any network problem occurs. Once developed, 460-NMS was tested both in a laboratory environment and for a real ship network that had been installed by the manufacturer and was confirmed to comply with the IEC 61162-460 requirements. Network safety and security issues onboard ships could be solved by designing a secure 460-Network along with a 460-Gateway and by constantly monitoring the 460-Network according to the requirements of the IEC 61162-460 network standard.

Keywords: IEC 61162-460, 460-Nework, 460-NMS, SNMP

1. Introduction

Increasingly the many interconnections of marine electronic devices, such as GPS, wind sensors, autopilot, depth sounders, and navigational instruments on board ships create a complex communication network of electronic devices. Therefore, modern ship environments may carry larger risks of unauthorized access or malicious attacks on ship network systems. Risks may also occur from personnel having access to the on board systems and, for example, introducing malware via removable devices **[1]**. Thus, data networks **[2]** should be considered a critical part of ship safety systems.

Networks on board ships may be threatened internally by network nodes or other networks and externally by unauthorized, uncontrolled networks, including both ship-borne networks and off-ship networks. Currently, ship systems **[3]** are highly integrated and can even be accessed from the shore, which may create a security risk to the ship's onboard network. Thus, there is a need for a ship network standard that addresses the safety and security of ships' onboard networks as well as a system for network management and configuration, fault detection, and network performance monitoring. IEC 61162 is a collection of IEC standards for "digital interfaces for navigational equipment within a ship" **[4]**. IEC 61162-450 is the part of IEC 61162 that specifies a method in which

† Corresponding Author (ORCID: http://orcid.org/0000-0001-8305-268X): Division of Information Technology Engineering, Korea Maritime and Ocean University, 727, Taejong-ro, Yeongdo-gu, Busan 49112, Korea, E-mail: yungyu@kmou.ac.kr, Tel: 051-410-4345

1 Navigation Collage, Dalian Maritime University, E-mail: wuzuxin@kmou.ac.kr, Tel: 051-410-4923, supported by "the Fundamental Research Funds for the Central Universities (3132015017)"

2 Division of Control Engineering, Graduate School of Korea Maritime and Ocean University, E-mail: sobia011@kmou.ac.kr, Tel: 051-410-4923

3 Division of Information Technology Engineering, Korea Maritime and Ocean University, E-mail: sjcho@kmou.ac.kr, Tel: 051-410-4344

navigational and radio communication equipment can interconnect in a single Ethernet network, called LWE (Light Weight Ethernet), and works for simple integrated bridge systems **[5]**. However, many ships require more complex bridge systems to support new e-navigation services and need higher safety and security standards. The IEC 61162-460 standard was developed by IEC technical committee 80 (maritime navigation and radiocommunication equipment and systems) as an extension to IEC 61162-450 to allow safe and secure implementation of more complex bridge systems. IEC 61162-460 standard defines safe and secure interconnection to external data sources, including other ship networks, off-ship data sources, and removable external sources by providing more extensive requirements to the components and operation of the system. It also defines the requirements of the monitoring system to aid in early detection and diagnosis of developing problems related to errors or overload of the 460-Network **[6]**.

The purposes of this study are to design and implement a secure 460-Network and 460-Gateway and to develop a network monitoring system by using the IEC 61162-460 ship network standard requirements. The network monitoring system monitors the 460-Network loads, traffic flows, status, network failure, and unknown device connections. It notifies the network administrators, system administrators, or IT managers in cases of problem detection via notifications, warnings, and alarms.

2. IEC 61162-460 Network

2.1 IEC 61162-460 Network Requirements

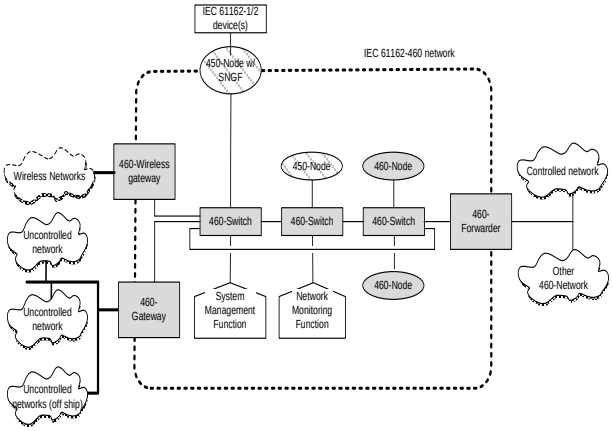

Figure 1: IEC 61162-460 network

Figure 1 shows an example IEC 61162-460 network which is composed of physical and logical network components. The physical components include a 450-Node, a 460-Node, a 460-Switch, a 460-Forwarder, and a 460-Gateway. The 460-Switch is the network infrastructure device used to connect nodes on the 460-Network. The 460-Forwarder safely exchanges data streams between the 460-Network and other controlled networks, including other 460-Networks. Moreover, the 460-Gateway connects 460-Networks and uncontrolled networks. Logical network components consist of network monitoring and system management functions. All 460-Network devices should satisfy the safety and security requirements as specified in the IEC 61162-460 standard.

2.2 Uncontrolled Network Security Requirements

All traffic from uncontrolled networks is passed or processed through the 460-Gateway.

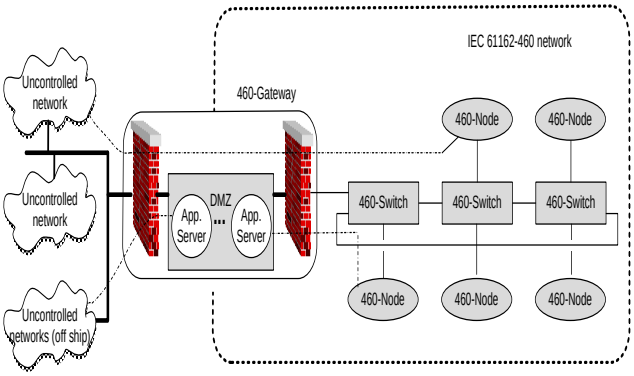

Figure 2: Uncontrolled network security

To protect the 460-Network from uncontrolled networks, the 460-Gateway contains firewalls and a DMZ (Demilitarized Zone) with various application servers as shown in **Figure 2**. An application server is a security device that can access common data from uncontrolled networks and 460-Networks, but only uncontrolled networks have permission to access data through firewalls. A DMZ is the physical manifestation of a logical subnetwork that contains and exposes an organization's external-facing services to larger and uncontrolled networks, usually including the internet; it is located inside the firewall. Two firewalls are implemented: one for the uncontrolled network and other for the 460-Network. The firewall is used to permit or deny traffic to and from uncontrolled networks, including off-ship network systems and other ship-borne systems, according to the preconfigured combination of source/destination IP (Internet Protocol) address, protocol, and port number **[7]**. All incoming and outgoing traffic must register in advance for the firewall. In this paper, a network-monitoring

function, shown in **Figure 1**, is designed and placed in the DMZ as one application server.

2.3 460-Gateway Requirements

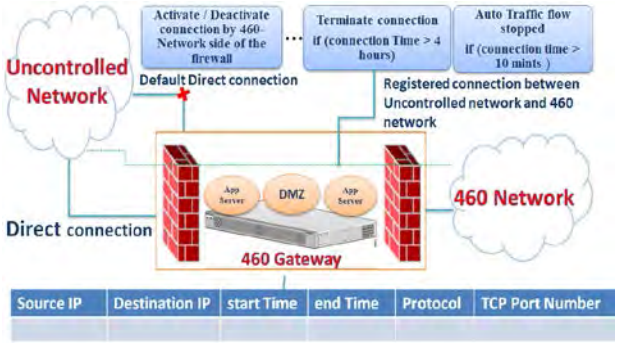

Figure 3: IEC 611612 460-gateway

Figure 3 shows the standard IEC 61162-460 requirements for a 460-Gateway. By default, the direct connection of the 460-Network to an uncontrolled network is prohibited. Internal and external firewalls configure and implement the source/ destination IP address, protocol, and port number. All connections between the 460-Network and uncontrolled networks need to be registered, and the 460-Gateway maintains a list of all activated connections. A direct connection between the 460-network and an uncontrolled network can only be activated or deactivated by an operation on the installation site (460-Network side of the firewall). Any direct connection will terminate automatically if its time exceeds 4 hours. Automatic forward traffic of the connection will stop if there is no traffic flow after time period pre-defined by manufacturer following 10 minutes.

2.4 IEC 61162 460-NMS (Network Monitoring System) Requirements

Given below are the Network Monitoring System requirements according to the IEC 61162-460 standard. The information that it is required to monitor includes the following:

(1) Network loads

(2) Traffic flow

(3) Network Status

(4) Network failure

(5) Device connection

The following information is the required traffic flow information:

(1)Input link utilization% (average over 5 minutes)

(2)Output link utilization% (exceeding 5 minutes)

(3)Number of input bytes (average over 5 minutes)

(4) Number of output bytes (average over 5 minutes)

(5) Input packets per second (average over 5 minutes)

(6) Output packets per second (average over 5 minutes)

(7) Input rate per interface (exceeding 5 minutes)

(8) Output rate per interface (average over 5 minutes)

2.4.1 Network Load-Monitoring Requirements

Network safety maintenance requires network load monitoring as well as alerts based on detected violations in the maximum network load. The network load-monitoring function shall generate the following alerts:

a) “Caution: Network traffic capacity exceeded” when the observed network load has exceeded the 80% limit for 30 s more than three times within a period of 10 min.

b) “Warning: Network traffic capacity exceeded” when the observed network load has exceeded the 80% limit for 30 s more than ten times within a period of 10 min.

2.4.2 SNMP Requirements

a) The network configuration and status information shall be reported by the 460-Switch each time it receives the periodic SNMP request.

b) The network monitoring function shall request the network status of all using request message every 30 s.

3. IEC 61162 460-Gateway Design and Configuration

3.1 IEC 61162-460 Gateway Design

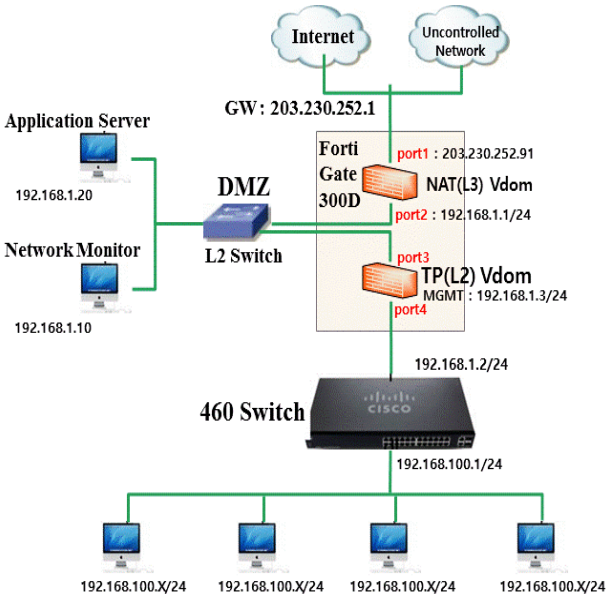

Figure 4: IEC 61162-460 gateway design

In designing the 460-Gateway, shown in **Figure 4**, the following network components are used:

a) CISCO L3 Catalyst 3560 X series **[8]** 460-Switch
b) Fort iGATE 300D **[9]** (460-Firewall)
c) DMZ (Demilitarized Zone) L2 Switch
d) 460-NMS (Network Monitoring System)
e) 460-Nodes

Figure 4 shows, the FortiGate 300D 460-Firewall and the CISCO L3 Catalyst 3560-X Series 460-Switch used to build a secure 460-Gateway. The FortiGate 300D 460-Firewall constructs two firewalls using VDOMs: a NAT L3 VDOM and a TP-Link L2 VDOM. Each VDOM operates as a single FortiGate security firewall, and all traffic enters or leaves the VDOM completely separate from other VDOM traffic. The NAT L3 VDOM controls the traffic to and from uncontrolled external networks, and the TP-LINK L2 controls traffic to and from the internal 460-Network. The CISCO 460-Switch is configured to create an uplink by setting up a VLAN1 with an IP address of 192.168.1.2/24. The SNMP server is enabled with the VLAN1 and assigned with this IP address. After that, the IP address 192.168.1.10 is assigned to the 460-NMS, which is a network monitoring system used to monitor the 460-Network. The SNMP Trap and Syslog Trap are enabled and assigned the 192.168.1.10 IP address of the 460-NMS host server. Finally, the FortiGate 300D 460-Firewall is configured to allow the 460-NMS to access the 460-Switch. 192.168.100.x/24-series network devices under the 460-Switch cannot communicate with outside networks.

3.2 460-Network Configuration

In a monitoring system, the SNMP server and the Syslog Server should use static IP addresses so that monitoring system can receive information from a fixed IP.

The following commands are used to configure a 460-Switch:

a) Set up Gateway IP for 460-Switch
#interface *vlan1*
#IP address *192.168.1.2 255.255.255.0*
b) Enable SNMP
snmp-server host *192.168.1.*2 v3 auth *authuser*
c) Enable SNMP Trap
#snmp-server host *192.168.1.10* traps v3 auth *authuser*
#snmp-server enable traps
d) Enable Syslog
#logging host *192.168.1.10*
#logging trap *7*
#logging on

4. 460-NMS (Network Monitoring System)

Network monitoring systems and network testing technologies have changed significantly over time. As with the technological advances in the field of networking, networks are continuously becoming more complex. Networks require monitoring systems to check the performance or failure of the network constantly **[10]**.

The 460-NMS is a software application that is used to maintain network safety and security according to the IEC 61162-460 standard by monitoring the network load and traffic flow and generating alerts or alarms in case of network overloads, device failure, or detection of unknown devices. A 460-NMS helps the 460-Network to run safely, securely, and smoothly. It is important to monitor the traffic flow at network nodes as well as the current network status in order to increase the performance and efficiency of the 460-Network.

The 460-NMS monitors the 460-network to alert it to the following network issues:

a) Any unknown device plugged into the 460-network
b) Insertion or removal of any fixed device within the network
c) Network device failure
d) Network overload
e) Network failure due to any known or unknown issue
f) Network connection failure

4.1 460-NMS Architecture

Figure 5 shows the conceptual model view of a 460-NMS that defines the structure, behavior, and specifics of the system.

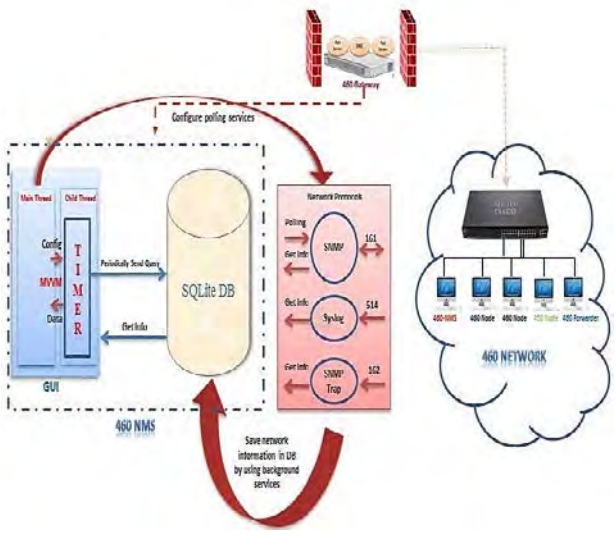

Figure 5: 460-NMS architecture

The 460-NMS collects and presents polling data from the 460-Switch MIB (Management Information Base) file using SNMP, Syslog, and SNMP Trap protocols. The C# SNMP SharpNet library **[12]** is used to query the network information of the 460-Switch using SNMP protocol over UDP on port 161. Enabling the SNMP Trap in the 460-Switch allows it to send notifications over UDP on port 162 in case any device is inserted or removed or if any unknown device detected in the network. Enabling Syslog in the 460-Switch allows it to send event notification messages to the Syslog server (460-NMS). Syslog uses the UDP port 514 for communication **[11]**. The SQLite database management tool is used to store and manage network information received from the 460-Switch.

The GUI is used for monitoring and visualizing the network information. The system backhand service collects network information periodically and saves it into the database. The main thread of the GUI configures the polling services and controls the child thread timers. The child thread contains timers that periodically send a query to retrieve network information from the database and send the data to the main thread.

4.2 460-NMS Design and Tools

a) Application Interface

The GUI of the 460-NMS was designed using WPF (Windows Presentation Foundation) technology. This provided clarity and flexibility to make changes. The MVVM (Model - View – View Model) software architectural design was used for the design and development of the 460-NMS, as shown in **Figure 6 [12]**.

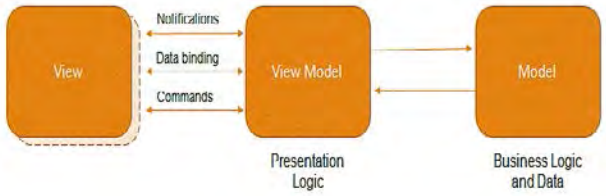

Figure 6: Model-view-view model

b) Database

To manage the 460-Network information, the database was designed using the SQLite database management tool. SQLite is a fast, well-organized, and embedded relational database **[13]**.

c) Backhand developing

Backhand developing was done with the Microsoft C# Programming language in the Microsoft.Net framework 4.5 **[14]**.

4.3 Entity—Relationship Diagram (ERD) Model of 460-NMS

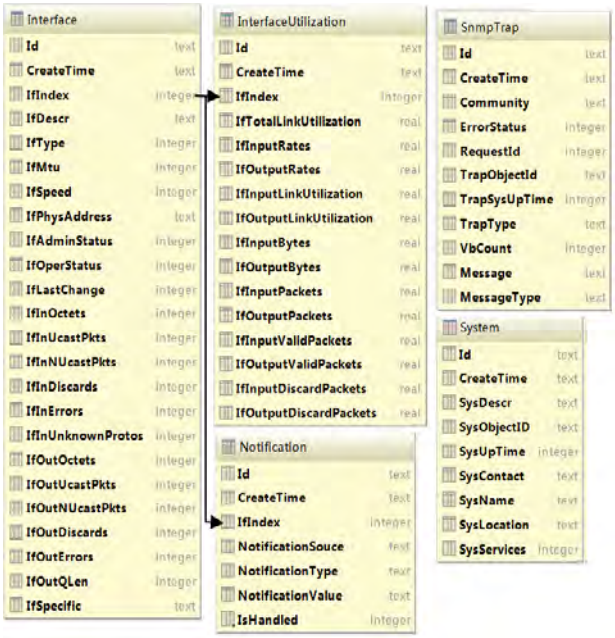

Figure 7: 460-NMS ER model

The Entity-Relationship diagram (ERD) model identifies the entities and the relationships between those entities. Figure 7 shows the ERD of the 460-NMS. It consists of the following system information entities:

(1) Interface: Manages the details of the 460-Switch interfaces.

(2) Interface Utilization: Manages the traffic flow information of each 460-Network device interface connected to a 460-Switch.

(3) System: manages the information of the system that is to be monitored

(4) SNMP Trap: Manages SNMP Trap information received from the 460-Switch.

(5) Notification: Manages all kinds of notifications.

4.4 Traffic Flow Information lists of 460-NMS

To calculate the traffic flow information of each 460-Switch interface, the following formulas are used (as shown in **Table 1**):

Table 1: Interface traffic flow information

Name	Formula
Total Link Utilization	(IfInputLinkUtilization+ IfOutputLinkUtilization)/2
Input Rates	(currIfInOctets - prevIfInOctets)/(1024*TI)
Output Rates	(currIfOutOctets - prevIfOutOctets)/(1024*TI)
Input Link Utilization	(currIfInOctets - prevIfInOctets)*8/(IfSpeed*TI)
Output Link Utilization	(currIfOutOctets - prevIfOutOctets)*8/(IfSpeed*TI)
Input Bytes	(currIfInOctets - prevIfInOctets)/1024
Output Bytes	(currIfOutOctets - prevIfOutOctets)/1024
Input Packets	(currIfInUcastPkts - prevIfInUcastPkts)/1024
Output Packets	(currIfOutUcastPkts - prevIfOutUcastPkts)/1024
Input Valid Packets	IfInputPackets - IfInputDiscardPackets
Output Valid Packets	IfOutputPackets - IfOutputDiscardPackets
Input Discard Packets	(currIfInDiscards - prevIfInDiscards)/1024
Output Discard Packets	(currIfOutDiscards - prevIfOutDiscards)/1024

*TI = Time Interval between two polling operations in a second

Below **Table 2** shows the interface table (ifTable), which is the description of interface traffic flow abbreviations used in **Table 1 [15]**.

Table 2: ifTable (Interface table)

IfInputLink Utilization	The use of bandwidth for an input link based on the sampling period
IfOutputLinkUtilization	The use of bandwidth for an output link based on the sampling period
ifInOctets	The total number of octets received by the interface
ifOutOctets	The total number of octets transmitted by the interface
ifSpeed	An estimate of the interface's current bandwidth (in bits per second)
ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer
ifOutUcastPkts	The total number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent
ifOutDiscards	The number of outbound packets that were chosen to be discarded, even though no errors had been detected, to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifInDiscards	The number of inbound packets that were chosen to be discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol

An example of how to calculate the Input Rate of a 460-Switch interface is given below, which is taken from **Table 1**. The same process applies for remaining traffic flow information mentioned in **Table 1**:

a) Receiving and parsing the interface's input octet value using the SNMP SharpNet library.

b) Using the method given below to calculate the Input Rate of the interface:

If currIfInOctets < prevIfInOctets then currIfInOctets = currIfInOctets + 2^{32}-1

*Input rate = (currIfInOctets- prevIfInOctets) / (1024 * (time2 - time1))*

Because the *ifInOctets* type in the SNMP MIB file is "Counter," it is reset to 0 when its value reaches at maximum value (2^{32}-1).

where CurrIfInOctets is the interface's input octet's value at time2 and PrevIfInOctets is the interface's input octet's value at time1.

4.5 Example to show SNMP MIB data parsing

SNMP SharpNet Library commands are used to fetch the network information from the CISCO 460-Switch MIB file. MIB is a tree-structured database. Each node of an MIB consists of the object identifier (OID), data type, and value, which is related to the network **[16]**. For example, to access the "sysDescr" node in the MIB file, the MIB tree structure, which is shown in **Figure 8** by green nodes, must be followed.

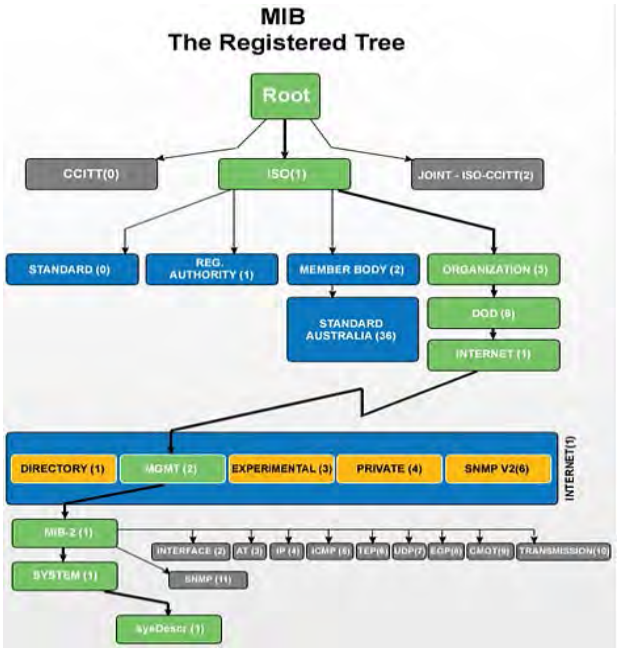

Figure 8: MIB tree structure

The process to access the “sysDescr” tree structure format is described below:

a) In string format: iso.org.dod.internet.mgmt.mib.system.sysDescr,

b) In number format: 1.3.6.1.2.1.1.1

The parsed information of the “sysDescr” node entities of the CISCO 460-Switch is as follows:

a) OID: 1.3.6.1.2.1.1.1

b) Data type: Octet String (as defined in MIB file)

c) Value: Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 15.0)

4.5.1 SNMP Message Parsing

The 460-NMS’s background services will periodically send a request (containing an OID) to the SNMP agent, and then the agent will reply with the specified object’s information to the SNMP manager **[17]**. **Figure 9** shows SNMP manager requests with an OID of 1.3.6.1.2.1.1.1.0 using the GET command. In response to the request, the SNMP agent checks the requested OID in the MIB database and sends the object’s information, which contains its value and data type, to the SNMP Manager.

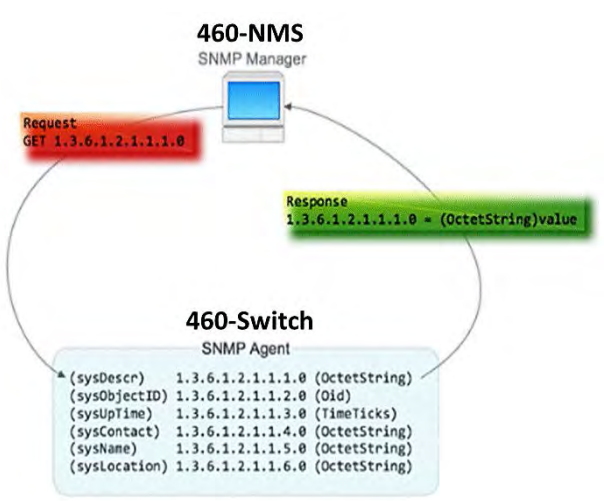

Figure 9: SNMP message parsing

4.5.2 SNMP Trap

If the SNMP Trap is enabled, when some changes take place in the SNMP agent device (460-Switch), then the agent will send a notification to the SNMP manager (460-NMS). For example, when the 460-Switch configuration or Border Gateway Protocol (BGP) state changes, it will trigger a notification **[17]**.

5. 460-NMS Implementation

As mentioned above, 460-NMS is a software application developed for monitoring 460-Network devices to ensure safe operation.

The GUI of 460-NMS is user-friendly and contains the following information wizards **[18]**:

5.1 Login wizard

The login wizard was designed to allow access to the 460-NMS to only trusted users. The user needs an Admin ID and a password to log in, as shown in **Figure 10**.

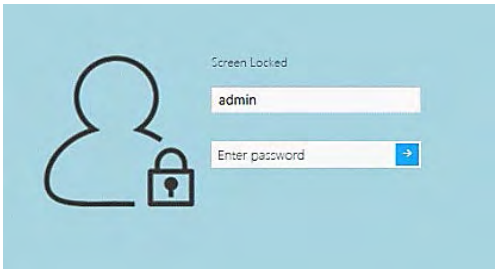

Figure 10: 460-NMS login interface

5.2 Main Form

Figure 11 shows the main system view, in which the 460-Switch represents the main root and its interfaces represent child nodes. Users can double-click on each node to view its detailed information.

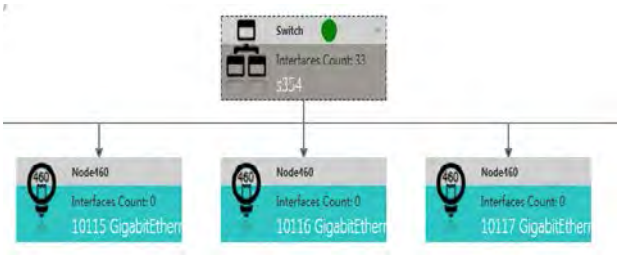

Figure 11: 460-NMS main form

5.3 460-NMS Testing

5.3.1 Lab Test

The lab environment testing process of the 460-NMS for monitoring the 460-Switch and its nodes according to the requirements of the IEC 61162-460 standard is described as follows:

a) First the community name, agent IP, port, and other system configuration settings were set as shown in **Figure 12** to connect the 460-NMS to the 460-Switch.

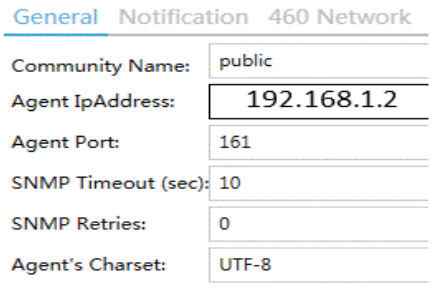

Figure 12: System setting general tab

b) Set the warning and critical threshold values for network overload according to the requirements by inputting data as illustrated in **Figure 13** (on the notification tab).

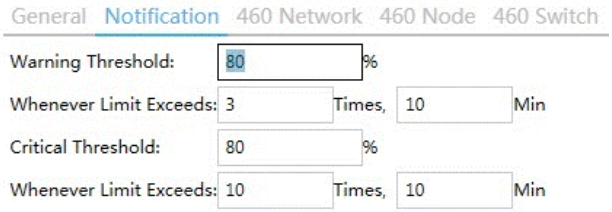

Figure 13: Notification tab

c) **Figure 14** shows the detailed information of the CISCO L3 Catalyst 3560 X series 460-Switch with its descriptive interfaces after successful connection. It contains four tabs: interfaces, notifications, SNMP Trap, and Syslog.

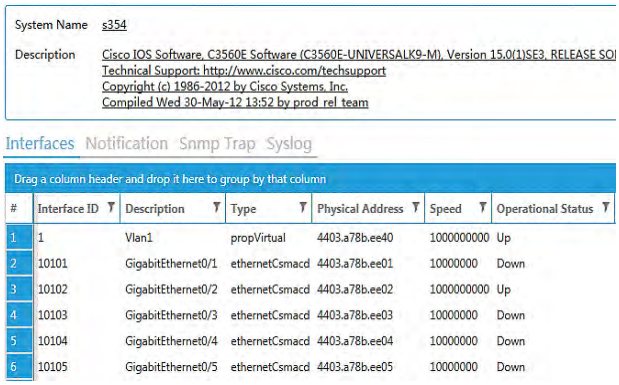

Figure 14: 460-Switch information wizard

d) The Information Wizard manages the core information of each interface, including interface type, speed, physical address, last updated time, and description. It contains two tabs, the traffic flow (Utilization), and charts that manage information about I/O rates, I/O link utilization, I/O Bytes, I/O packets, valid I/O packets, and discarded I/O packets, as shown in **Figure 15**.

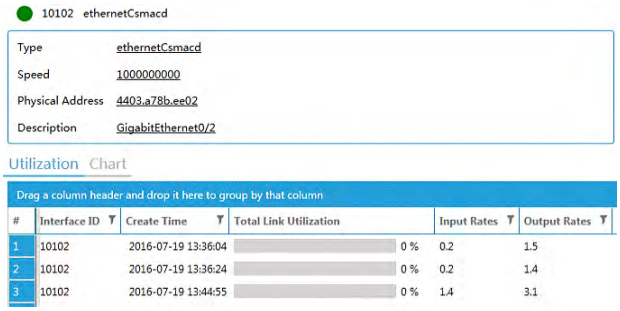

Figure 15: Interface information wizard

e) After that, the maximum bandwidth of interface number 10102 was set to 1 MB in order to check the network traffic overload notification when the network load was over 1 MB, as shown in **Figure 16** (Interface Bandwidth Setting).

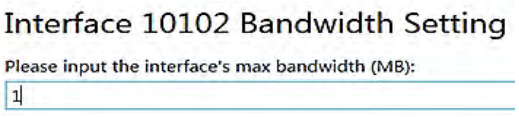

Figure 16: Interface max bandwidth setting

f) The I/O traffic flow rates of interface ID 10102 were tested. Since the bandwidth exceeded 80% of the predefined maximum value of 1 MB, the traffic overload notification "input/output rates overload" was received, as shown in **Figure 17**.

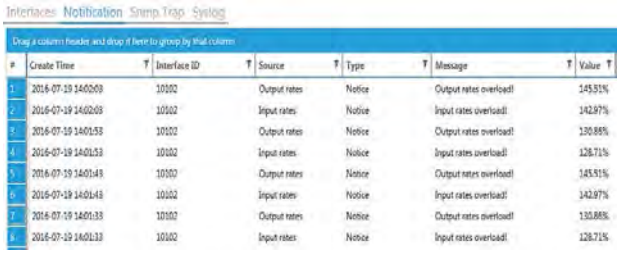

Figure 17: Input / Output traffic rates

g) During the device connection test, when the device connected to the GigabitEthernet0/15 interface was removed, the SNMP agent generated the SNMP Trap "changed state to down" as shown in **Figure 18** (SNMP Trap).

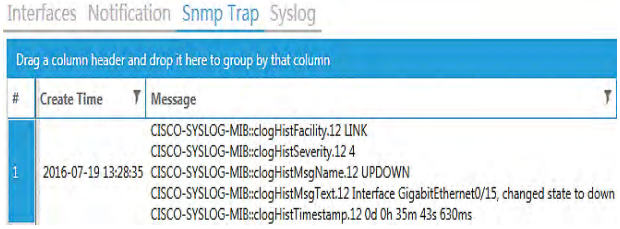

Figure 18: SNMP trap Tab

h) **Figure 19** shows the I/O rate chart view for interface 10102. The spine lines represent input and output rates.

Figure 19: Input / Output rates chart view

5.3.2 Real Network Test

The 460-NMS was tested in a real network environment to analyze and monitor a manufacturer-designed ship network. This network consisted of different ship data networks, including IEC 61162-450, IEC 61162-3 (NMEA 2000), IEC 61162-1, -2 (NMEA 0183) with various gateways, and uncontrolled networks, such as the Internet, as shown in **Figure 20**.

Figure 20: Manufacturer-designed ship network

In order to configure the 460-NMS to analyze and monitor the manufacturer-designed network, after configuring the 460-Switch, the following tests were performed:

a) The maximum bandwidth of each interface was set to 0.1 MB to check the traffic load. Because bandwidth exceeded 80% of the predefined maximum value of 0.1 MB, the “Input rates overload!” notification was received, as shown in **Figure 21**.

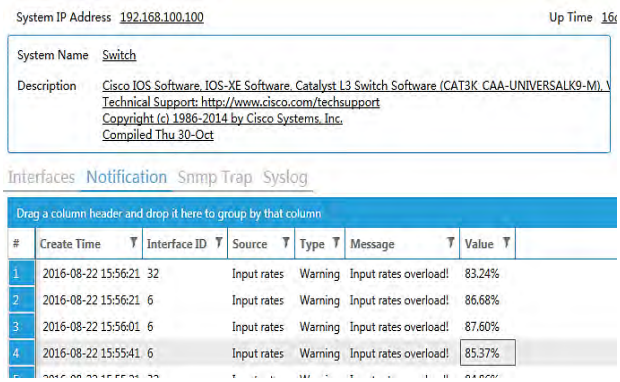

Figure 21: Input rates overload

b) **Figure 22** shows the I/O rates chart view of the interface named “GigabitEthernet1/0/16.” The green spine lines represent input rates, with a maximum value of 1037.5 kb/s, and the blue spine lines represent output rates, with a maximum value of 8045.2 kb/s.

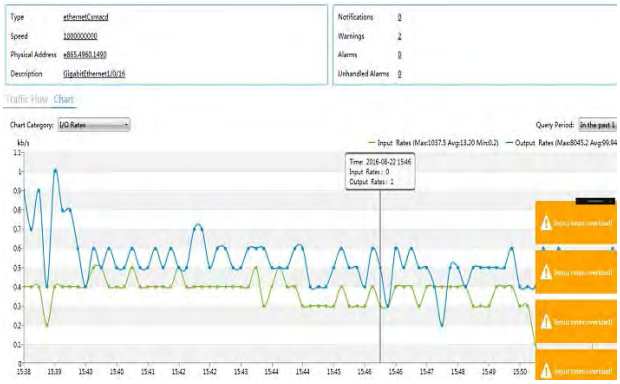

Figure 22: Input / Output rates flow chart

6. Conclusions

A secure 460-Network, a 460-Gateway, and a 460-NMS were developed and implemented based on the IEC 61162-460 network standard and then tested in lab and real network environments to satisfy the needs of onboard security for ships’ data networks. The network instruments used to design the 460-Network consisted of a CISCO 460-Switch, a 460-Gateway, a Fortinet 300D 460-Firewall, and 460-Nodes. Finally, the 460-Network load, traffic flow, and device connections were analyzed by the 460-NMS. The 460-NMS notifies the system administrator in case any problem occurs via alarms, warnings, and notifications. The test results confirmed that the performance of 460-NMS complies with the requirements of the IEC 61162-460 standard.

Acknowledgements

This paper is extended and updated from the short version that appeared in the Proceedings of the International Symposium on Marine Engineering and Technology (ISMT 2016), held at Korea Maritime and Ocean University, Busan, Korea, November 3–4, 2016.

References

[1] BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO, "The Guidelines on Cyber Security onboard Ships," BIMCO Bagsvaerdvej 161 Denmark, 2880 Bagsvaerd, Version 1.1., 2016, https://www.marad.dot.gov/wp-content/uploads/pdf/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016.pdf, Accessed August 10, 2016.

[2] O. J. Rodseth, "Design challenges and decisions for a new ship data network," ISIS 2011, Hamburg, September 15~16, 2011.

[3] ISO 16425-CD: Ships and marine technology Installation guideline for ship communication network of improving communication for shipboard equipment and systems (Committee Draft), 2012. ISO/TC 8/SC 6, Feb, 2013, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56739, Accessed July 15, 2016.

[4] IEC TECHNICAL COMMITTEE 80: MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS, International Electro technical Commission. IEC, http://www.iec.ch/index.htm, Accessed August 15, 2016.

[5] IEC 61162-450: Maritime navigation and radio communication equipment and systems - Digital interfaces - Part 450: Multiple talkers and multiple listeners - Ethernet interconnection, first edition, 2011. IEC, https://webstore.iec.ch/preview/info_iec61162-450/Bed1.0/Den.pdf, Accessed August 11, 2016.

[6] IEC 61162-460: Maritime navigation and radio communication equipment and systems - Digital interfaces - Part 460: Multiple talkers and multiple listeners – Ethernet interconnection - Safety and Security, 2015. IEC, https://webstore.iec.ch/preview/info_iec61162-460/Bed1.0/Den.pdf, Accessed July 11, 2016.

[7] ISOC RFC 791: Internet Protocol (IP), Standard STD0005 (and updates), https://tools.ietf.org/html/rfc791, Accessed July 21,2016.

[8] CISCO. CISCO CATALYST 3560 SERIES SWITCHES, http://www.cisco.com/c/en/us/index.html, Accessed October 21, 2016.

[9] A. Bristow, Bill Dickie, Bruce Davis., "the FortiGate Cookbook 5.2", FortiGate/FortiOS, FortiGate 5.2.0, 2015, http://docs.fortinet.com/d/fortigate-the-fortigate-cookbook-5.2, Accessed July 12, 2016.

[10] W. Barth, Nagios: System and Network Monitoring, William Pollock , 2nd Edition, 2008.

[11] ISOC RFC 5424: The Syslog Protocol, https://tools.ietf.org/html/rfc5424, Accessed July 21,2016.

[12] A. Ghoda, Windows 8 MVVM Patterns are Revealed: covers both C# and JavaScript, Apress, 2013.

[13] S. Haldar, SQLite Database System Design and Implementation, Second Edition, Version 1, Self-publisher 2015.

[14] M. Michaelis, E. Lippert, Essentials C# 6.0, 1st edition, Addison-Wesley Professional, 2015.

[15] .NET-SNMP, current release: 5.7.3, http://net-snmp.sourceforge.net/docs/mibs/interfaces.html, Accessed June 21,2016.

[16] ISOC RFC 3418: Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), https://tools.ietf.org/html/rfc3418, Accessed 19 August, 2016.

[17] ISOC RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, https://tools.ietf.org/html/rfc3411, Accessed 19 August, 2016.

[18] Z. X. Wu, S. Rind, Y. H. Yu, and S. J. Cho, "Ship's network security and monitoring system using SNMP," Proceedings of the ISMT 2016, p. 74, 2016.