Development of a Network Monitoring System for Ship's Network Security Using SNMP

A THESIS

Submitted to the Graduate School of
Korea Maritime and Ocean University, in partial fulfillment of the
requirements for the degree of Master of Science in Engineering

BY

Sobia Rind Baloch

December 2016

Advisor:

Professor Yung Ho Yu

Development of a Network Monitoring System for Ship's Network Security Using SNMP

By

Sobia Rind Baloch

Submitted in partial fulfillment of the requirements for the degree of Master of Science in Engineering

Approved by:

Professor Gang Gyoo Jin ………………

Professor Keel Soo Rhyu ………………

Professor Yung Ho Yu ………………

December 2016

Department of Control and Instrumentation Engineering

Graduate School, Korea Maritime and Ocean University

ACKNOWLEDGEMENTS

With deep and profound gratitude thanks to "Almighty Allah" for his so kindly conferring me the opportunity of undertaking and completing this thesis with a right approach and success.

I am especially very thankful to my thesis advisor Professor Yung Ho Yu, for his full time support, assistance and understanding. Who was always ready to help me throughout my thesis and showed me the right direction. I would also like to thank professor Gang Gyoo Jin and professor Keel Soo Rhyu for their assistance and suggestions to write this thesis.

I am very grateful to my lab mates and friends in Korea Maritime and Ocean University, especially to Dr. Soo-Jong Mo, Zu-Xin Wu, Sajad Rahmdel, Muhammadamin Beiramin, Eunhye Kim, Hong Ryul Lee, and Hwang Dumi for their support and making my stay in Korea loving and memorable. I would like to especially thanks to my sister Sadia Rind and some friends, Farooque Hassan, Imon and Saeed for providing me with unfailing support and continuous encouragement throughout my studies and stay in Korea.

Finally, heartily thanks to my most loving, caring and supportive parents for their sincere prayers and encouragement throughout my life and years of studies. This accomplishment would not have been possible without them.

Table of Contents

List of Figures

List of Tables

Ship's Network Security and Monitoring System using SNMP

Sobia Rind Baloch

Department of Control and Instrumentation Engineering
Graduate School of Korea Maritime and Ocean University

Abstract

Nowadays, the risk of unauthorized access or malicious attacks on ship's systems onboard internally or externally is possible to be a threat to the safe operation of ship's network. According to the requirements of IEC (International Electro-Technical Commission) 61162-460 network standard, a secure 460-Network is designed for safety and security of networks on board ships and developed a network monitoring software application for monitoring the 460-Network.

Therefore, in this thesis to secure the ship's network, ship's security network is designed and implemented by using 460-Switch, 460-Nodes, 460-gateway that contains firewalls and DMZ (Demilitarized Zone) with various security application servers in compliance with IEC 61162-460. Also, 460-firewall is used to permit/deny traffic to/from unauthorized networks. 460-NMS (Network Monitoring System) is a network monitoring software application, developed by using SNMP (Simple Network Management

Protocol) SharpNet library with.Net 4.5 frameworks and backhand SQLite database management which are used to manage the network information. 460-NMS configures 460-Switch and communicates by SNMP, SNMP Trap, and Syslog to gather the network information and status of each 460-Switch interface. 460-NMS analyze and monitors the 460-Network load, traffic flow, current system status, network failure, or detect unknown device connection. It notifies the system administrator via alarms, notifications or warnings in case if any network problem occurs. To confirm the performance of the designed 460-Network according to the requirements of IEC 61162-460 standard: First, the laboratory is composed of the dedicated network with CISCO 460-Switch, 460-Gateway, Fortigate 460-Firewall, and lab computers. These network devices exclude from external networks such as the internet. The 460-NMS is connected with configured laboratory network to analyze and monitor the network traffic flow, load and device connections by using SNMP.

Second, the test of 460-NMS is carried out in a company's network. That is very complex network environment which includes IEC 61162-460, IEC 61162-450, IEC 61162-3 (NMEA 2000), IEC 61162-1, -2 (NMEA 0183) data networks with 450-Gateway, Gateway 450 to 0183, Gateway N2K to 0183, and Gateway 0183 to N2K and excludes from unauthorized networks.

Finally after testing, it is confirmed that the 460-NMS analyzes, monitors the whole 460-network and notifies and warns abnormal status of 460-network as the requirements of IEC 61162-460 international standards.

1 . Introduction

1.1 Motivation

Increasingly, the interconnections between marine electronic devices such as GPS, wind sensor, autopilot, depth sounders, ECDIS which update ENC data from shore through the internet and or navigational instruments on ship's board, create a complex network of electronics devices to integrate navigational data. Therefore, nowadays ship's environment may cause the larger threats of unauthorized access or malicious attacks on ship's network systems. A risk may also occur from personnel having access to the systems onboard, for example, by introducing malware via removable devices [1]. Thus, those kinds of threats may affect safe navigation of ships.

Networks onboard ships might be threatened internally by network nodes or other networks and externally by open networks that are unauthorized networks including shipborne networks and off-ship networks. Currently, the ship systems are highly integrated and even can be accessed from shore [3], which may create a security risk to onboard ship's network. Thus, there is a need for ship network standard that must address the safety and protection of onboard ship's network and 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 one part of IEC 61162 standard that specifies a method which the navigational and radio communication equipment can safely interconnect in a single Ethernet network so called LWE that is, for simple, integrated bridge systems [5]. However, many ships require more complex bridge systems to support e-navigation services and need higher safety and security standard. IEC 61162-460 standard has been 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 internal and external data sources that include other ship networks on board, off-ship data sources, and removable external sources by providing more extensive requirements to the components and operation of the system. The primary purpose of IEC 61162-460 standard is to prevent the 460-Network from unauthorized networks and to make the 460-Network work efficiently and safely. It also defines, the requirements of the monitoring system to aid in early detection and diagnosis of problems related to errors or overload of the 460-Network [6]. The unauthorized and uncontrolled network can interface to IEC 61162-460 network through a 460-Gateway.

The purpose of this study is to design and implement a secure 460-network and develop a network monitoring system by using IEC 61162-460 ship network standard. The network monitoring system monitors the 460-network loads, traffic flows, status, network failure, and connection of any unknown devices. Also, it can notify the network administrators, system admins or IT managers in case of any problem detected via notifications, warnings or alarms [24].

1.2 Study Idea

E-navigation requires shipboard integrated information system in real-time to achieve the safety of navigation and protection of ocean environment. Data networks which are implemented onboard ship consist of IEC 61162-450, IEC 61162-3 (NMEA 2000), and IEC 61162-1, -2 (NMEA 0183) network standards, to satisfy data update rate and characteristics of the network. The information should be integrated from all kinds of equipment onboard through the ship's network to achieve the aim of e-navigation. While the data exchange is being carried out, threats of unauthorized access or malicious attacks from unauthorized and uncontrolled networks including attacks through Internet access can harm normal data exchange and integration. For this reason, the security network which can access safely from the unauthorized and uncontrolled network is necessary to achieve the purpose of e-navigation.

2 International Standards of Ship Network

2.1 Overview

Ships are complex entities: in a sense, a ship can be considered an autonomous moveable village with systems for power generation and distribution, propulsion, navigation, life support, cargo control, and monitoring [19]. Onboard ships the implemented data networks are IEC 61162-450, IEC 61162-3 (NMEA 2000), and IEC 61162-1, -2 (NMEA 0183) which are used to satisfy the data rate, network characteristics and to integrate the information from all kinds of on board equipment. An example of a layered ship network architecture shows in *Figure* ***2.1***, with a schematic representation of the network types on each layer and some sample applications. The structure can be divided into the following segments:

1. The first layer consists of the dedicated connections that use the IEC 61162-1, -2 (NMEA 0183) to interconnect various actuators, sensors, compass and so on to higher level components.

2. The second layer composes the instrument networks that interconnect components associated with a particular control function and display on the ship. For example, GPS, navigation, control of the engine, cargo and various kinds of equipment.

3. The third layer consists of the shipboard control networks that are mainly Ethernet-based LWE, is an interconnection system between the process segments. Control and monitoring systems based on IEC 61162-450 belong to this layer.

4. Ships contain other networks on the ship. Normally there is an administrative networks and ICS which control and interconnect various kinds of radio equipment and GMDSS and intercommunication system such as system.

5. Off ship is networked on shore, usually connected to the ship via a satellite. It often includes the owner or operator with secure data links to the ship, such as, through a VPN.

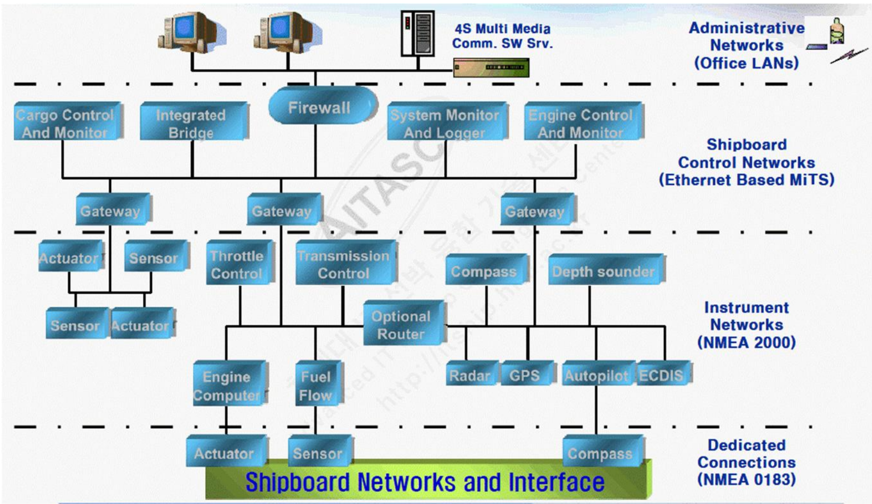

Figure 2.1 Schematic ship network architecture

Most of the network systems are interconnected, but only through dedicated applications that act as gateways or, in some cases, generic firewall or gateway components (FW/GW).

2.2 Ship's Data Network

IEC technical committee 80 initiates the standards for ship's data networks to have satisfactory data communication between electronic marine instruments via an appropriate interface. IEC 61162 is a collection of IEC standards for "Digital interfaces for navigational equipment within a ship," which describes below:

2.3 IEC 61162-1, IEC 61162-2, NMEA 0183

National Marine Electronic Association developed NMEA 0183 standard in 1989 for ship's data network communication that supports serial data transmission using RS-422 interface from single talker to multiple receivers. This standard defines the electrical signal requirements, data transfer protocol, data transmission timings, and specific message formats for a 4800-baud serial data interface. Devices are recognized as a talker or listener or sometimes both. A talker is any device that sends data to other NMEA 0183 device, and a listener is any device that receives data from other NMEA 0183 device, as shown in *Figure 2.2* [18].

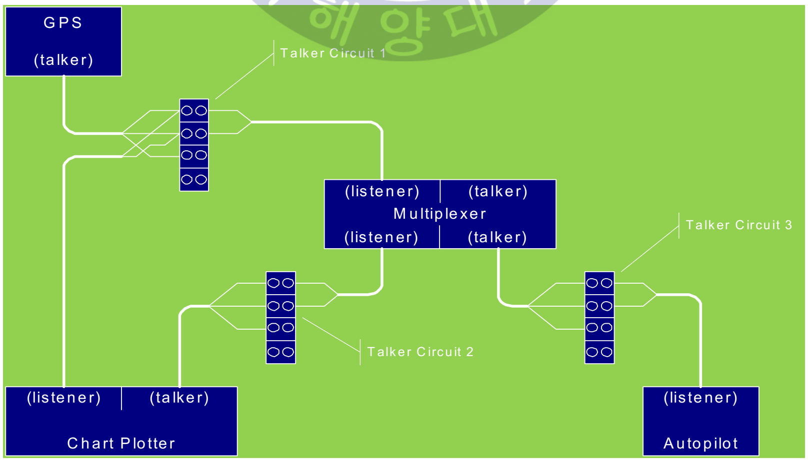

Figure 2.2 NMEA 0183- single talker multiple listener

Message Format:

The data format is ASCII characters and sent as text messages, as shown below:

$GPGSA,3,10,07,05,02,29,04,08,13,,,,,1.72,1.03,*hh [CR][LF]

All NMEA 0183 messages start with a "$" and transmit by a [Carriage Return] [Line Feed]. The five characters immediately after $ are the address field. The address field is interpreted based on the type of sentence (talker, query or proprietary). Multiple data fields follow the address field which is separated by commas.

Example: $HCHDM, 238, M, *hh [CR] [LF]

Where "HC" specifies magnetic compass as a talker, the "HDM" specifies magnetic heading message that follows the HC. The "238" is the heading value, "M" represents heading value as magnetic, and *hh as checksum.

The speed is limited to 4.8 kbps. NMEA 0183 publish as IEC 61162-1 standard in 1995. IEC 61162-2 is an extension of IEC 61162-1 with a high transmission rate of 38.4 kbps to support fast transmitting devices [18].

2.4 IEC 61162-3, NMEA 2000

NMEA 2000 was standardized as IEC 61162-3. It is a "plug and plays" communication which is used to interconnect electronic instruments (sensors and displays) within a ship, and exchange data between different manufacturer devices simultaneously. It supports up to 50 physical node connections and 250 kbps data rate at bus lengths of up to 200m [21].

The general topology of NMEA 2000 is known as "Trunk and Drop" or "Backbone and Drop," as shown in *Figure 2.3*. The NMEA 2000 backbone is connected in a linear form with each device connected to it via separate taps and drop cables. Two termination resistors are used to reduce line reflections or network disturbance, one at each end of network cable. The NMEA 2000 device is connected to the backbone network using a 3-port "T" connector and a drop cable. NMEA 2000 devices require a voltage range between DC 9 to 16 volts.

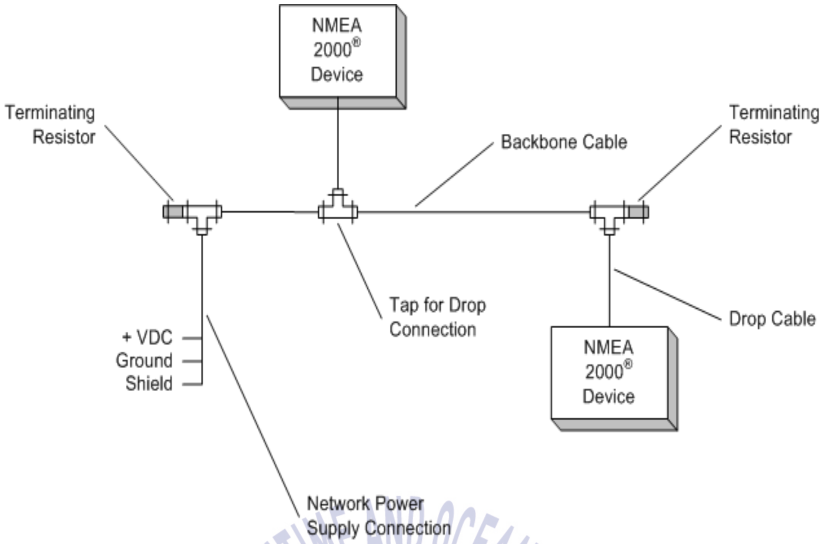

Figure 2.3 NMEA 2000 topology

2.4.1 CAN

CAN is a microprocessor peripheral developed jointly by Intel and Bosch. This device generates serial bit-stream that is to be transmitted on the network and gain access to the network when the equipment has to send data. The serial data frame used by CAN has a 32-bit arbitration field, 6-bit control field and from zero to 64-bit data field. Also, the structure contains the start of frame, end of frame bits, reserved bits, frame control bits, a 15-bit CRC error detection field, and 2-bit acknowledgment bits, as shown in below *Figure* ***2.4*** [21].

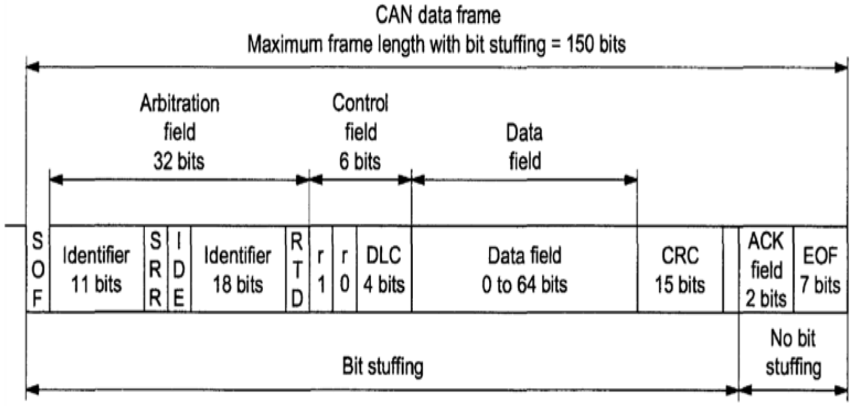

Figure 2.4 NMEA 2000 CAN frame

2.4.2 NMEA 2000 Messages

NMEA 2000 messages have three kinds which are single CAN Frame (8 bytes), multi-packet message (9-1785 bytes) and N2K fast packet (9-233 bytes). The messages transmitted on the NMEA 2000 network organized into parameter group numbers. *Figure **2.5*** shows the relationship between PGN and ID of CAN Frame [23].

PDU Format	29 bit Identifier						PGN 개수
	Priority 3bit	EDP 1bit	DP 1bit	PF 8bit	PS 8bit	SA 8bit	
		PGN					
PDU1	0-7	0	0	0-239	DA 0-255	SA 0-255	240
			1	0-239	DA 0-255	SA 0-255	240
PDU2	0-7	0	0	240-255	GE 0-255	SA 0-255	16x256 =4096
			1	240-255	GE 0-255	SA 0-255	16x256 =4096

Figure 2.5 (a) PDU1 format (b)PDU2 format (c) Relation between PGN and 29-bit ID

PGN is composed of EDP, DP, PF, and PS of total 29-bits. The method of composing PGN is divided into PDU1 and PDU2. There are two data pages (DP) in each PDU. PDU1 and PDU2 are distinguished with the value of PF. In PDU1 the PS is DA which means PGN is addressable, while in PDU2 the PS is GE which means PGN is broadcasting. So, the total number of PGN which can be expressed becomes 8672.

The PGNs have their own data format with the data fields containing information stored in a database. *Figure 2.6* shows a PGN 059392 with name "ISO Acknowledgment" which includes 4 data fields. Each data field defines in the data dictionary with defined data format. Every defined data format represents by standard data types, such as character, integer, unsigned integer, float, or a bit field. In the *Figure 2.6* shows that the PGN 059392 is a single Frame, the default priority of 6; data size is 8 bytes, and its destination is addressable.

ISO Acknowledgment **PGN: 059392**

This message is provided by ISO 11783 for a handshake mechanism between transmitting and receiving devices. This message is the possible response to acknowledge the reception of a "normal broadcast" message or the response to a specific command to indicate compliance or failure. The application layer is responsible for determining when this message is desired, outside of network management requirements specified by this standard (e.g. response to ISO Request message). This message will always be sent with a destination address of 255.

Single Frame: Yes *Priority Default:* 6 *Default Update Rate:* NA milliseconds *Frequency:* NA cycles per second

Destination: Address *Query Support:* *ACK Rqmnts:*

Field #	Field Name				Original Reference ID # 64
1	Control Byte 0x00 = Positive Acknowledgment; 0x01 = Negative Acknowledgment; 0x02 = PGN supported but access denied; 0x03 to 0xFF = Reserved	*Byte Field Size:*	*Bit Field Size:* 8	*Request Parameter*	No
2	Group Function Value Group Function of PGN being acknowledged. This field identifies for a device the specific group function of a PGN being acknowledged or declined. This field is not used if the PGN being acknowledged or declined is not a group function PGN.	*Byte Field Size:*	*Bit Field Size:* 8	*Request Parameter*	No
3	Reserved Bits Variable number of reserved bits, all set to logic "1"	*Byte Field Size:*	*Bit Field Size:* resv 24	*Request Parameter*	No

Figure 2.6 NMEA 2000 PGN

Currently, NMEA is working on a new standard called "OneNet" which is a method of transmitting NMEA 2000 messages over Ethernet. It supports up to 65000 devices and base on IPv6.

2.5 IEC 61162-450

IEC has published the IEC 61162-450 standard on ship data networks. It is an Ethernet-based network specification with a relatively small level of protocol complexity and is known as LWE. LWE is a trade-off between technology complexity and specific requirements from the ship equipment industry [2] [5].

2.5.1 Function Blocks

Below is the given description of specified functionality implemented by IEC 61162-450 equipment:

1. NF: Function block responsible for physical connectivity to the network and connectivity to the transport layer
2. ONF: Function block that interfaces to the network (for example real time streaming of Radar and CCTV image transfer, VDT sound transfer, etc.)
3. SF: Function block, identified by a unique system function ID (SFI), that is the only function block that can send information in a datagram format
4. SNGF: function block that enables transfer of sentences between the network and devices that are compliant with the IEC 61162-1 and IEC 61162-2 serial line interface.

Figure 2.7 shows the topology of IEC 61162-450 network with the function blocks.

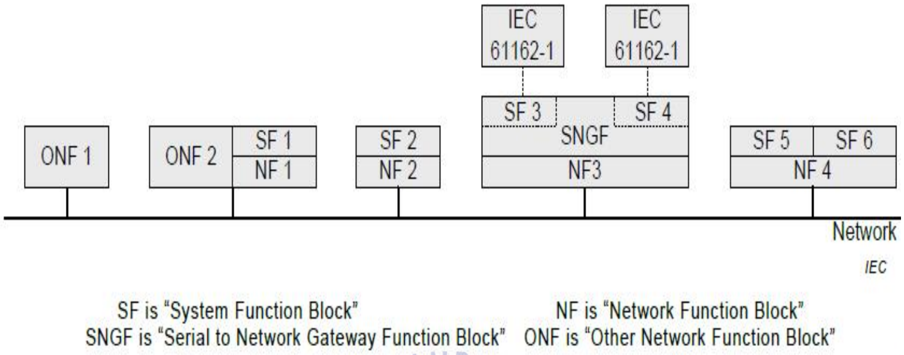

Figure 2.7 IEC 61162-450 network

2.5.2 IEC 61162-450 Message

An example of the structure of an Ethernet frame with an IEC 61162-450 sentence is given in Figure 2.8. The uppermost block shows the full Ethernet frame with the UDP user available data block shown in the white block. The IP and UDP headers are included in the gray blocks. The lower block shows the UDP user available data block with an IEC 61162-450 formatted sentence included. The numbers above the Ethernet frame gives the size of each block. The numbers in front of the UDP user data block gives the offset from the start of the block (0 – zero).

6	6	2	20	8	0-1472	4
dmac	smac	type	ip	udp	61162-450 message	crc32

0	U	d	P	b	61162-450 header
4	C	’0’			
6	\	s	:	T	61162-450 payload
10	I	0	0	0	
14	1	,	n	:	
18	3	3	4	*	
22	1	9	\	$	
26	T	I	R	O	
30	T	,	1	2	
34	3	.	4	5	
38	*	6	7	<CR>	
42	<LF>				

\s:TI0001,n:334*19\$TIROT,123.45*67<CR><LF>

Figure 2.8 Ethernet frame

2.5.3 IEC 61162-1 sentence

IEC 61162-450 protocol provides a mechanism by which IEC 61162-1 sentences can be sent to one or more receivers on the network. This protocol shall be used for SBM, MSM type messages and also CRP message exchanges.

2.6 IEC61162-460

IEC 61162-460 standard has been 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 [6].

2.6.1 Objectives

The major objectives of IEC 61162-460 network standard are to:

1. Define equipment and system requirements to improve network availability even when some network components or equipment fail to work as specified. These requirements will address safe behavior of failing devices as well as recovery mechanisms in the network, including redundancy;

2. Define new requirements and monitoring functions to allow safe design and operation of networks with high network loads regarding overall bandwidth or message frequency;
3. Allow safe and secure interconnection to external data sources, including other ship networks, off-ship data sources, and removable external data sources by providing more extensive requirements to the components and operation of the system;
4. Define system monitoring functions to aid in early detection and diagnosis of developing problems related to errors or overload of the system.

2.6.2 Scope

This standard is an add-on to the IEC 61162-450 standard for integrated navigation and radio communication systems where higher safety and security standards are needed, e.g. due to higher exposure to external threats or to improve network integrity. This standard provides requirements and test methods for equipment to be used in an IEC 61162-460 compliant network as well as requirements for the network itself and requirements for interconnection from the network to other networks. This standard also contains requirements for a redundant IEC 61162-460 compliant network [6].

3 . 460-Network Requirements

3.1 Overview

Figure 3.1 shows a 460-Network implementing IEC 61162-460 network standard on different parts and components of the 460-network. The gray block represents equipments and Pentagon signifies logical software functions stated in this specification [6].

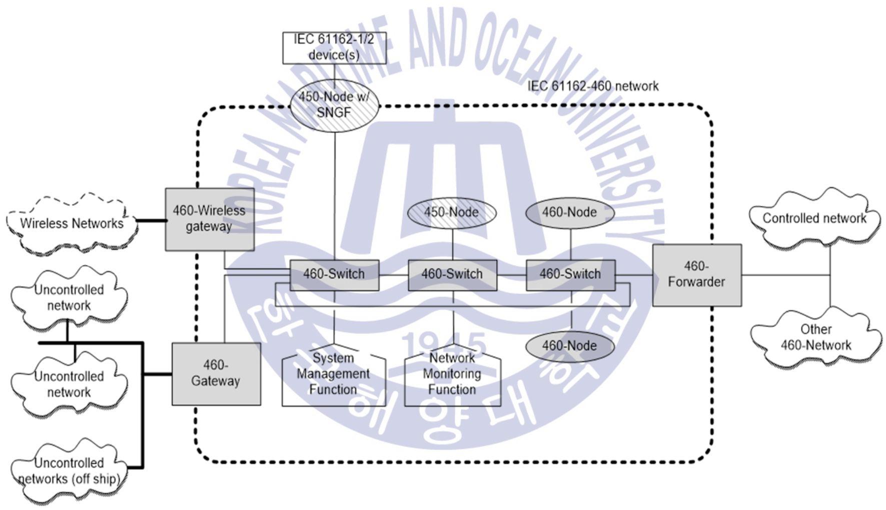

Figure 3.1 IEC 61162-460 network

3.1.1 Network Components

The IEC 61162-460 network composed of physical and logical network components, as described below:

1. Physical components

1. 450-Node: A device compliant with the IEC 61162-450 standard and which satisfies additional requirements specified in this standard.
2. 460-Node: Device compliant with the requirement of a 450-Node and meets the safety and security requirements as defined in IEC 61162-460 standard.
3. 460-Switch: Network infrastructure device used to interconnect nodes on a 460-Network and meets the safety and security requirements as defined in IEC 61162-460 standard.
4. 460-Forwarder: Network infrastructure device that can safely exchange data streams between a 460-Network and other controlled networks including other 460-Networks.
5. 460-Gateway: Network infrastructure device that connects 460-networks and uncontrolled networks. Also, satisfies the safety and security requirements as specified in this IEC 61162-460 standard.

2. Logical components

1. Network monitoring function

The network monitoring function shall perform the following tasks:

1. Network load
2. Network redundancy
3. Network topology

2. System management function

The system management function shall perform the following tasks:

1. Maintain configuration information of all network infrastructure and restore it when requested.
2. The management function shall maintain a history of at least the previous configuration.
3. Shall have the functionality to save or restore the configuration information automatically or manually from 460-Switches, 460-Forwarders or 460-Gateways.
4. Functionality to change the infrastructure configuration.

3.2 460-Network Traffic Management Requirements

3.2.1 460-Node Requirements

The 460-Node complies with the following to satisfy the network traffic management needs:

1. All traffic shall be specified as one of the IEC 61162-450 compliant data types for example IEC 61162-1 sentence transmission, binary image traffic or provided via as specified in IEC 61162-450 and as documented by the manufacturer.

2. The maximum operational data output for a device shall be declared by the manufacturer in bytes per second averaged over a specified period.

3. Devices shall continue normal operation with an input loss rate of packets up to 0.1%.

4. The manufacturer shall specify device behavior when its maximum input data rate exceeds.

5. The node shall process only data specified for the node

6. If VLAN provides, VLAN protocol version IEEE 802.1Q: the 460-Node shall support 2005. All VLAN traffic shall include in the maximum transmission rate.

3.2.2 460-Switch Requirements

The following are the traffic management requirements for a 460-Switch:

1. A means shall be provided to configure a stream or a network flow that identified by the combination of interface identifier, the MAC address or IP address, protocol number and TCP or UDP port number.
2. The total number of configurable traffic streams shall be at least 1024 streams.
3. A means shall be provided to allocate network bandwidth resource for each registered flow. The resource shall be increased or decreased by 1 Kb/s steps.
4. All incoming and outgoing traffic shall configure.
5. All traffic not configured shall be prohibited.

6. The amount of bandwidth allocated at a 460-Switch shall be more than or equal to the sum of all traffic volumes of each traffic class assigned to the network connected to the switch.
7. The total amount of traffic per each interface to a 450-Node and 460-Node shall be limited to the network design value of that interface using resource allocation. The network design value shall be selectable between 0 - 50%.
8. If VLAN provided, a means to configure VLAN per each interface shall provide.
9. If VLAN provided, VLAN protocol version IEEE 802.1Q:2005 shall support.

3.3 Security Requirements

3.3.1 Threat Scenarios

As shown in *Figure* ***2.1*** *Schematic ship network architecture*, 460-Networks can be threatened internally by 450-Nodes and externally from uncontrolled networks such as the internet, shipborne equipment or off-ship equipment. Therefore, 460-Networks need to be protected from internal and external threats.

1. Internal threats

A security threat may cause from inside a 460-Network. The following are scenarios that can occur in 460-Networks:

1. Malware replication from other equipment in 460-Network such as a notebook that is infected by the malware;
2. Infection from corrupted mass storage devices (e.g. USB flash drive) or removable media drives (CD/DVD) being used within the 460-Network, e.g. in connection with (authorized or unauthorized) maintenance and support;
3. Attacker installs a backdoor in one of the equipment and gets system privilege through it. Then he attacks other equipment;
4. User deletes system file or change configuration file by mistake;
5. Illicit access that prohibits the proper operation of equipment.
6. False data generation that prohibits the proper operation of equipment.
7. Security threats in controlled networks which easily propagate to 460-Networks;

8. Security threats in other 460-Networks which easily propagate to 460-Networks;
9. Interruption of network service due to the heavy volume of broadcasting traffics and of ICMP and IGMP packets

2. External threats

Equipment and systems from outside of a 460-Network, such as from one of a shipborne network or off-ship networks, may cause some security threats. The following are scenarios that are caused by external networks:

1. Threats from un-secure wireless networks;
2. Malware in other shipborne networks infects equipment in 460-Network;
3. User in a shipborne network logs in remotely to equipment in a 460-Network, and deletes an important file or changes the configuration by mistake;
4. Shipborne equipment has installed a backdoor that uses as an attack agent. Direct attack to equipment through the network infrastructure such as switch or router;

5. Scanning attack. Attacker finds a port for attack by scanning the ports first. If found, it scans the service with the port. For example, when port number 80 is open for the web service, attacker collects the information of web server type and version;
6. Indirect attack to the 460-Network via uncontrolled networks such as another shipborne network;
7. Data are sniffing and modification attack during the communication with external equipment and systems. When equipment in a 460-Network communicates with off-ship network systems, the attack extracts and modifies data by sniffing. For example, the navigational route information may be exposed to and be changed by pirates and terrorists;
8. Incoming excessive data traffic to 460-Networks and protocol features attack including SYN flooding attack.

3.3.2 Internal Network Security Requirements

The following are the internal security requirements to safe 460-Network from internal threats:

1. A 460-Node, 460-Switch, and 460-Forwarder shall not utilize a wireless LAN interface and WAP functions

2. The maximum input and output bandwidth of a 460-Node device shall be declared by manufacturer in bytes per second average over a specified period
3. The method used to protect 460-Switch, 460-Forwarder from DoS attacks is to limit the traffic maximum value, disabled unnecessary services and by using ICMP and IGMP protocols.
4. The number of connection points (USB ports, disc drives, etc.) shall be limited
5. Access to make changes in the configuration of any 460-Network components shall be subject to user authentication provided with valid log-in information.
6. All allowed data shall identify by the IP address and UDP/TCP port number.
7. For each physical port, the connected 450-Node or 460-Node device shall be identified by the MAC address

3.3.3 Uncontrolled Network security requirements

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

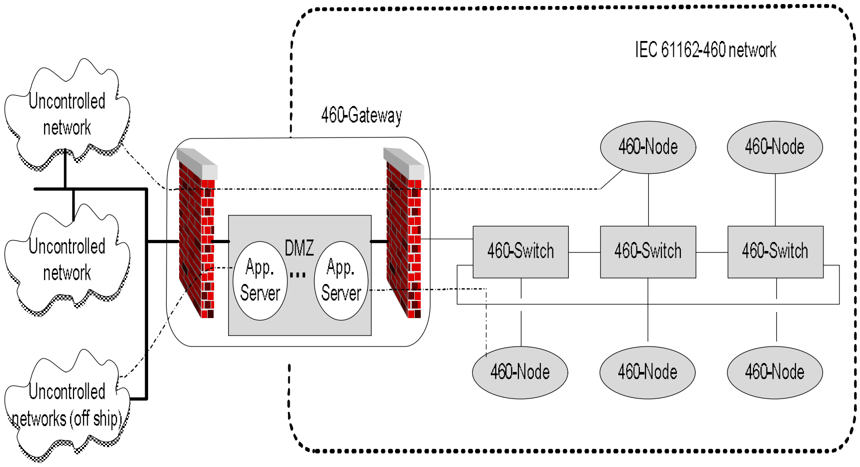

Figure 3.2 Uncontrolled network security

To protect the 460-Network from uncontrolled networks 460-Gateway contains firewalls and DMZ with various application servers as shown in *Figure 3.2*. An application server is the security device that can access common data from uncontrolled networks and 460-Network, but only uncontrolled networks have permission to access data from application servers. The DMZ is the physical of the logical subnetwork that contains and exposes an organization's external-facing services at larger and uncontrolled network, usually the internet. It locates inside the firewall. Two firewalls are implemented, one for the uncontrolled network and other for the 460-Network. The firewall is to permit or to deny traffic from/to an uncontrolled network including off-ship network systems or other ship-borne systems. The firewall shall configure with the combination of source/destination IP [7] address, protocol, and port number. All incoming/outgoing traffic shall register in advance for the firewall.

3.4 460-Gateway Requirements

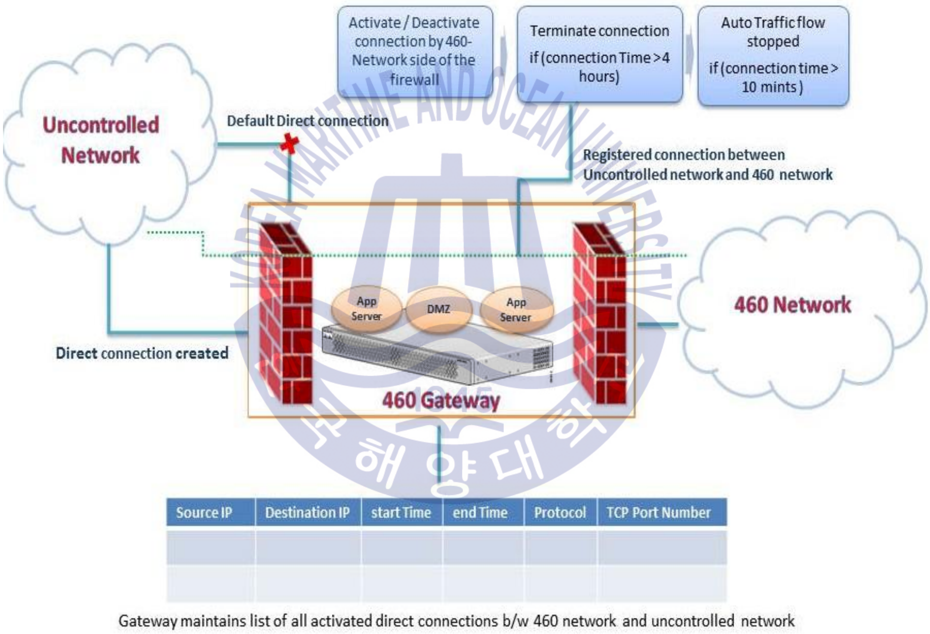

Figure 3.3 IEC 61162 460-gateway

Figure ***3.3*** shows IEC 61162-460 standard requirements for 460-Gateway which are described below in detail:

1. By default, direct connection of 460-Network to uncontrolled network is prohibited.
2. Internal and external firewalls implement and configure with the source/ destination IP address, protocol, and port number.
3. All connected connections between 460-Network and uncontrolled network need to be registered, and 460-gateway maintains the list of all activated connections that includes source/ destination IP, start time, end time, protocol and port number.
4. The direct connection between 460-network and uncontrolled can only be activated and deactivated by an operation on the installation site (460-network side of the firewall).
5. All direct connections will terminate automatically if the time exceeds greater than 4 hours.
6. Auto forward traffic of direct connections will stop; if there will be no traffic flow within 10 minutes added manufactured predefined time.

3.5 IEC 61162 460-NMS Requirements

Given below are the Network Monitoring System requirements by IEC 61162-460 standard.

3.5.1 460-Node

The following is the required configuration information for monitoring at a 460-Node:

1. The number of interfaces;
2. The list of traffic flows and its designed maximum traffic rate;
3. The change of the flows: add, delete or modify;
4. The list of flows assigned to each interface.

The following information is the required status information:

1. Interface link utilization per each interface (average over 5 min);
2. Interface input rates per each interface (average over 5 min);
3. Interface output rates per each interface (average over 5 min).

3.5.2 460-Switch

The following is the required configuration information for monitoring at a 460-Switch:

1. Interface information: interface type (Ethernet-CSMA/CD, FDDI), maximum speed, maximum transmission unit;
2. List of neighbor MAC address per interface;
3. The change of neighbor MAC address;

The following is the required status information for monitoring at a 460-Switch:

1. Interface input link utilization in % (average over 5 min);
2. Interface output link utilization in % (average over 5 min);
3. The number of interface input bytes (average over 5 min);
4. The number of interface output bytes (average over 5 min);
5. The number of interface input packets per second (average over 5 min);
6. The number of interface output packets per second (average over 5 min);

3.5.3 Network load-monitoring requirements

The maximum network load based on the manufacture's declarations of maximum traffic rates for all flows of the system. Maintaining the network safety requires network load monitoring and alerts based on detected violations in the maximum network load. The network monitoring function shall request network status from all 460-Switches using SNMP request messages periodically each 30s, get the traffic flow information and monitor network load by using (interface input link in % and interface output link utilization in %) from SNMP. The network load monitoring function shall generate the following alerts:

1. Caution: Network traffic capacity may exceed when the observed network load has exceeded the 80% limit for 30 sec more than three times within a period of 10 min;
2. Warning: Network traffic capacity exceeded when the observed network load has exceeded the 80% limit for 30 sec more than ten times within a period of 10 min.

3.5.4 Syslog recording function requirements

1. The network monitoring function shall provide a recording and view for the Syslog information, which 450-Nodes, 460-Nodes, 460-Gateways and 460-Wireless gateways have provided.

2. The minimum capacity of the recording shall be 100,000 messages. The recorded Syslog messages shall be available at least for last 30 days.

3.5.5 SNMP requirements

1. The network configuration and status information shall be responded by 460-Switch when it receives SNMP request message periodically.
2. Any event or report received from 460-Switch using SNMP.
3. The network monitoring function shall request network status from all 460-Switches using SNMP request messages periodically each 30 sec.
4. The network monitoring function shall request network configuration information from all 460-Switches using SNMP request messages periodically each 30 Minutes.

4 . 460-Gateway design and SNMP

4.1 SNMP

SNMP is an application layer protocol for collecting and organizing information of network devices such as routers, switches, servers and other network devices. SNMP is widely used to monitor and manage network devices [22].

4.1.1 SNMP Components

4.1.1.1 SNMP Manager

SNMP Manager is like management system that communicates and manages SNMP-enabled network devices. SNMP Manager queries and gets network information from SNMP agents by using some SNMP functions.

4.1.1.2 SNMP Agent

SNMP Agent is a program in network devices. It collects and stores management information defined in network device database and makes it available to SNMP Manger. *Figure **4.1*** shows the basic

SNMP communication where manager sends some queries to port 161 of agent device and get the response.

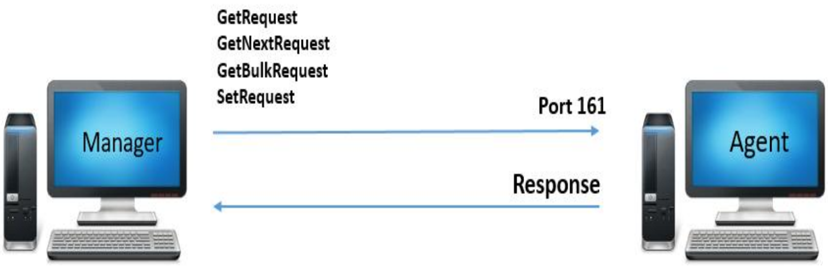

Figure 4.1 Basic SNMP communication

4.1.2 SNMP Versions

4.1.2.1 SNMP v1

It is the least secure version of SNMP due to its lack of encryption techniques, like sending passwords over plain text.

4.1.2.2 SNMP v2

It is the second version of SNMP that revises SNMP v1 and includes improvements in the area of performance, security, and communication.

4.1.2.3 SNMP v3

This version of SNMP implements "User-Based Security." That safety feature allows setting Authentication/ Encryption based on the user requirements.

Security has been the issue in SNMP protocol versions, such as clients authentication by using the "community string" as a password between a manager and agent. The clear text passwords provide no security to networks; anyone can retrieve, change or configure network information. The SNMP v3 addresses the security that is not given in SNMP v1 and v2 [20].

Following are the configuration information that SNMP v3 provides:

3. Username: Textual description of the person responsible for the SNMP entity that is to manage.
4. Security Level: Level of security includes values as noAuthNoPriv, authNoPriv, authPriv.
5. Authentication protocol: Used MD5, SHA1 for authentication, to prove that you are who you are.

6. Authentication Passphrase: Passphrase used with authentication protocol and must be eight characters long.
7. Privacy Protocol: Protocol used for privacy, to encrypt the SNMP data packet.
8. Privacy Passphrase: It is used with the privacy protocol.

4.1.3 MIB

MIB is a database which manages network information of managed objects that the agent tracks. It is organized hierarchically and can be accessed using SNMP protocol. Any status or statistical data that can be found by network information management system is defined in a MIB [17].

MIBs are a collection of defalcations which define the properties of the managed object within the device to be managed. MIB files are defined by the manufacturer of the network device. In this thesis, we have used CISCO 3650 SWITCH MIB files for accessing network information of each switch interface.

1. SNMP OID

OID Stands for Object Identifier. OID is unique name for an object in a MIB database.

Example: Below is simple structure of OID that is shown in *Figure* ***5.4****. MIB tree structure* and described in section 4.4.1.2 (SNMP MIB data parsing):

iso(1).org(3).dod(6).internet(1).mgmt(2).mib(1).system(1).sysDescr(1) or 1.3.6.1.2.1.1.1

2. SNMP Message Types

Every type of SNMP supports the following request types, send by the SNMP manager to fetch network information from managed device:

3.Get: It is performed to retrieve one or more values from managed device.

4.Get Next: It retrieves the value of next OID in the MIB tree.

5.Set: It is used to modify or assign the value of managed device.

6.Get Bulk: It sends multiple get request and returns result in the bulk of OIDs.

3. SNMP Trap

When some changes happen in SNMP agent device, the notifications sent by the agent over UDP port 162 to pre-configured receivers such as SNMP Manager, as shown in *Figure 4.2*.

Figure 4.2 SNMP trap notification

4. SNMP Message Format

The SNMP message format specifies which fields to include in the message and what order. The message is made up of several layers of nested fields, as shown in *Figure 4.3*.

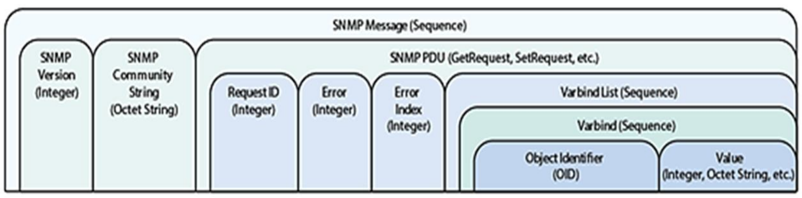

Figure 4.3 SNMP message format

The entire message is composed of three main fields, which are: SNMP Version (integer), the SNMP Community String (Octet String) and SNMP PDU. In Appendix **오류! 참조 원본을 찾을 수 없습니다.** shows the details of each SNMP message field.

4.1.4 Syslog

Syslog is a logging mechanism in network devices or SNMP agent. It is used to collect system logs which contain critical information about the status, errors, warning, and configuration logs of the devices. By monitoring Syslog messages, network security administrators can troubleshoot the network problems. Syslog uses the UDP, port 514 as default, for communication as shown in *Figure 4.4* [13].

Figure 4.4 Basic SYSLOG communication

1. Syslog Message Main Components

The information provided by the originator of a Syslog message includes the facility code and the severity level.

1. Facility

Syslog Facility is one information field associated with a Syslog message. The Syslog protocol defines it. In Appendix **오류! 참조 원본을 찾을 수 없습니다.** shows Facility code with information.

2. Severity Level

Messages are generated according to a severity level, specified by a number (0 through 7), mentioned in Appendix **오류! 참조 원본을 찾을 수 없습니다.**.

3. Priority Values

Each Syslog message includes a priority value at the beginning of the text. The priority value ranges from 0 to 191 and is made up of a Facility value and a Level value. The priority is enclosed in "<>" delimiters.

The priority value is calculated using the following formula:

Priority = Facility*8 + Severity

4. Message

The message component has these fields: TAG, which should be the name of the program or process that generated the message, and content which contains the details of the message.

2. Syslog Message Format

Sharing log data between different applications requires a standard definition and format of the log message, such that both parties can interpret and understand each other's information.

The Syslog protocol is originally defined in RFC 3164 "The BSD Syslog Protocol." RFC 3164 is now superseded by RFC 5424. RFC 5424 is considered better since it using structured data to makes events easier to parse on the receiving end, but for some reason, not all devices support it.

A. RFC 3164 Version

RFC 3164 defined each message have the following fields [13], shown in *Figure 4.5*:

1. Timestamp: The date and time from the firewall clock. The default is no time stamp.
2. Device ID: Added to uniquely identify the firewall is generating the message. It can be the firewall's host name, an interface IP address, or an arbitrary text string. The default is no device-id.
3. Message ID: Always begins with %PIX-, %ASA-, or %FWSM-, followed by the severity level and the six-digit message number.
4. Message Text: A description of the event or condition that triggered the message.

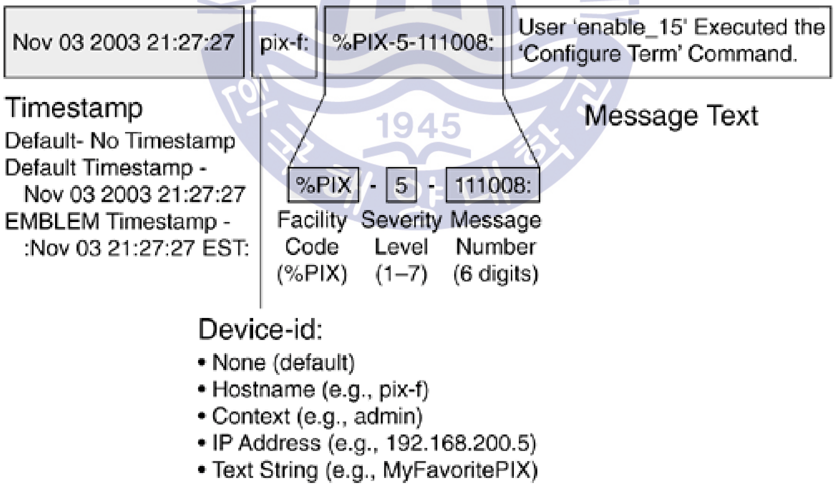

Figure 4.5 RFC 3164 message format

B. RFC 5424 Version

RFC 5424 defines the Syslog log message format and rules for each data element in each message. A Syslog message has the following format: A header, followed by structured data (SD), followed by a message, shown in *Figure **4.6*** [13].

The header of the Syslog message contains “priority,” “version,” “timestamp,” “hostname,” “application,” “process id,” and “message id.” It is followed by structured data, which contains data blocks in the “key=value” format enclosed in square brackets “[],” e.g. [SDID@0 utilization=“high” os=”Linux”] [SDPriority@0 class=” medium”]. In the example image below, the SD is simply represented as “-,“ which is a null value (nil value as specified by RFC 5424). After the SD value, BOM represents the UTF-8 and “su root failed on /dev/pts/7” shows the detailed log message, which should be encoded UTF-8.

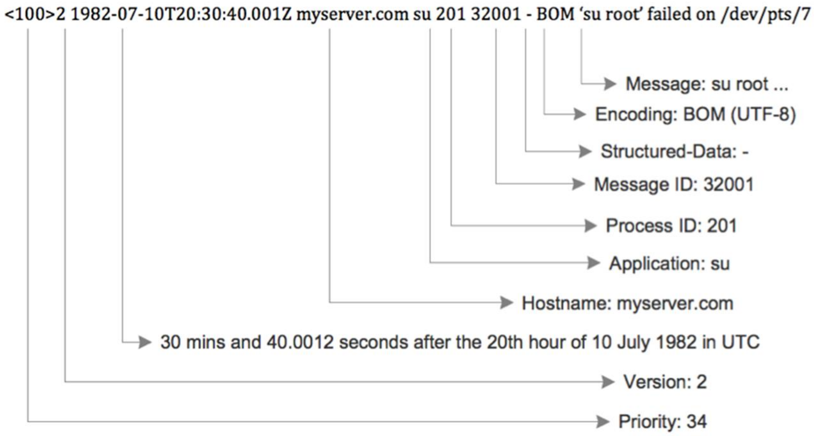

Figure 4.6 RFC 5424 message format

4.2 CISCO Switch

In this study, Cisco 460-Switch version C3560E Software (C3560E-UNIVERSALK9-M), Version 15.0(1) SE3, and RELEASE SOFTWARE (fc1) is used. The Cisco® Catalyst® 3560 Series is a line of fixed configuration, enterprise-class switches that include IEEE 802.3af and Cisco pre-standard PoE functionality in Fast Ethernet and Gigabit Ethernet configurations [8].

Performed the below-mentioned configurations to configure the CISCO 460-Switch for designing secure 460-Network:

4.2.1 Initial configuration for the Switch

Followed the below steps to initialize and configure the CISCO 460-Switch:

Step 1: Connecting to the Switch

The console port is used to perform initial configuration. Connect the Switch console port to a PC, used an RJ-45 to DB-9 adapter cable.

Step 2: Starting the Terminal-Emulation Software

Start the Terminal Emulation software before power on Switch, to see output display from the POST. The terminal software is a PC application such as HyperTerminal or ProComm Plus that makes communication between the Switch and PC. Configure the terminal emulation software as given below values:

•9600 baud; •8 data bits; •1 stop bit; •No parity; •None (flow control)

Step 3: Connecting to a Power Source

As the switch powers on, it begins the POST, a series of tests that runs automatically to ensure that the switch functions properly. POST lasts approximately 1 minute and after POST is complete, the system and status LEDs will remain green.

Step 4: Initial Configuration

Follows these steps to complete the initial configuration for the switch:

Step 1 *At the terminal prompt, enter the enable command to enter privileged exec mode.*

```
Switch> enable
Password: password
Switch#
```

Step 2 *Set the system time using the clock set command in privileged EXEC mode.*

```
Switch# clock set 14:30:09 10 Oct 2016
```

Step 3 *Verify the change by entering the show clock command.*

```
Switch# show clock
14:30:09.719 UTC Fri Oct 10 2016
```

Step 4 *Enter the configure terminal command to enter global configuration mode.*

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config)#
```

Step 5 *Configure a host name for the switch, and press* ***Return****.*

```
Switch (config)# hostname S354
```

4.2.2 IP Configuration

In a monitoring system, the SNMP server and Syslog Server should use static IP address, and then the 460-NMS can receive information from a fixed IP.

Step 1 *Configure the interface that connects to the management network. (The IP address and subnet mask shown are for example only. Use an address appropriate for your network.).*

S354 (config)# **ip routing**
S354 (config)# **interface** Vlan1
S354 (config-if)# **ip address** 192.168.1.2 255.255.255.0
S354 (config-if)# **no shutdown**
S354 (config-if)# **ip default-gateway** 192.168.1.1
S354 (config-if)# **exit**
S354#

Step 2 *View the configuration you just created and confirm that it is what you want.*

S354# **show run**
Building configuration...
Current configuration: 5957 bytes
!
! Last configuration change at 15:30:02 UTC Fri Oct 10 2016
!
Version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname s354

Step 3 *Verify the IP information by using the* ***show ip interface brief****.*

```
S354# show ip interface brief
Interface            IP-Address     OK?   Method    Status
Protocol
Vlan1                192.168.1.2  YES    NVRAM    up
down
FastEthernet0        unassigned     YES    NVRAM   down
  down
GigabitEthernet0/1   unassigned     YES   unset      down
down
GigabitEthernet0/2   unassigned     YES   unset      down
down
GigabitEthernet0/3   unassigned     YES   unset      down
down
```

4.2.3 SNMP Configuration

Step 1 *Set the community string.*

S354 (config) # **snmp-server community** public

Step 2 *Enable snmp v3 server and associate a user with a remote host using* ***auth*** *(authNoPriv) authentication.*

S354 (config)# **snmp-server group** *authgroup* **v3 auth**

S354 (config)# **snmp-server user** authuser authgroup **remote** 192.168.1.10 **v3 auth md5** authpassword

S354 (config)# **snmp-server user** authuser authgroup **v3 auth md5** authpassword

S354 (config)# **snmp-server host** 192.168.1.2 **v3 auth** authuser

Step 3 *Enable snmp v3 traps.*

S354 (config)# **snmp-server host** 192.168.1.10 **traps v3 auth** authuser

S354 (config)# **snmp-server enable traps**

4.2.4 Syslog Configuration

Syslog is a logging mechanism in network devices used to collect system logs which contain critical information about the status, errors, warning, configuration logs, etc., of the devices. Below show the syslog configuration settings:

Step 1 *Enable log time stamps..*

S354 (config)# **service timestamps log uptime**

Step 2 *Enable syslog server and set log level..*

S354 (config)# **logging host** 192.168.1.2

S354 (config)# **logging trap 7**

S354 (config)# **logging on**

S354 (config)# **exit**

Step 3 *Save configuration.*

S354 # **copy running-config startup-config**

4.3 IEC 61162-460-Gateway Design and 460-Network Configure

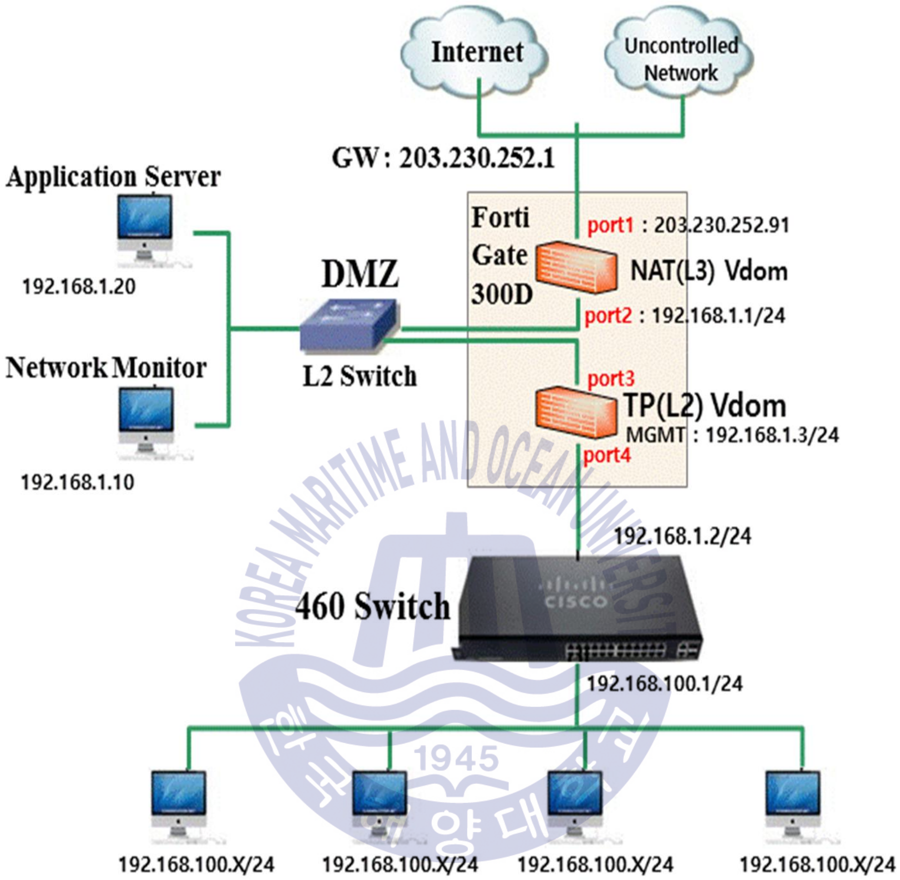

Figure 4.7 IEC 61162-460 network

The following network components use for designing the 460-Gateway and configuring 460-Netowrk as shown in *Figure 4.7*:

1. CISCO L3 Catalyst 3560 X series [8] 460-Switch
2. Fort iGATE 300D [9] (460-Firewall)
3. DMZ L2 Switch

4. 460-NMS
5. 460-Nodes

The 460-Gateway is designed and 460-Network configured by following the below procedure:

1. The Fortigate 300D 460-Firewall and CISCO L3 Catalyst 3560 X series 460-Switch are used to build a secure 460-Gateway.
2. The Fortigate 300D 460-Firewall constructs the two firewalls using VDOMs which is divided into NAT L3 VDOM and TP-Link L2 VDOM. Each VDOM operates as a single FortiGate security firewall and all traffic enters or leaves a VDOM is completely separated from other VDOM traffic.
3. NAT L3 VDOM will control the traffic to/from external uncontrolled networks and TP-LINK L2 will control traffic to/from internal 460-Network.
4. The CISCO 460-Switch configured to create Up Link by making VLAN1 with an IP 192.168.1.2/24.
5. SNMP server is enabled with the VLAN1 by assigning the IP 192.168.1.2/24.
6. Assigned IP 192.168.1.10 to 460-NMS, which is a network monitoring system used to monitor the 460-Network.
7. SNMP Trap and Syslog Trap are enabled with the assigned IP 192.168.1.10 of 460-NMS as the host server.

8. Allowed the 460-NMS to access 460-Switch by configuring Fortigate 300D 460-Firewall.
9. 192.168.100.x/24 series network device under the 460-Switch cannot communicate with the outside networks.

5 . Design of a 460-NMS

Network monitoring system and network testing technologies have changed significantly over time. As technological advances in network field, networks are becoming complex day by day. To check the performance or failure of any network constantly needs a network monitoring system [10]. To increase the performance and efficiency of the 460-Network, it is important to analyze and monitor the 460-Network traffic flow, current network status, and resource consumptions.

The 460-NMS is a software application which is developed to maintain the network safety and security by analyzing and monitoring the 460-Network load, traffic flow, and device connections. It generates alerts or alarms in case of network overloads, device failure or detection of any unknown device.

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

1. Any unknown device plugged in the 460-network
2. Plugged in or plugged out of any fixed device within the network
3. Network device failure
4. Network overloads
5. Network failure due to any unknown or known issue
6. Network connections failure

5.1 460-NMS Architecture

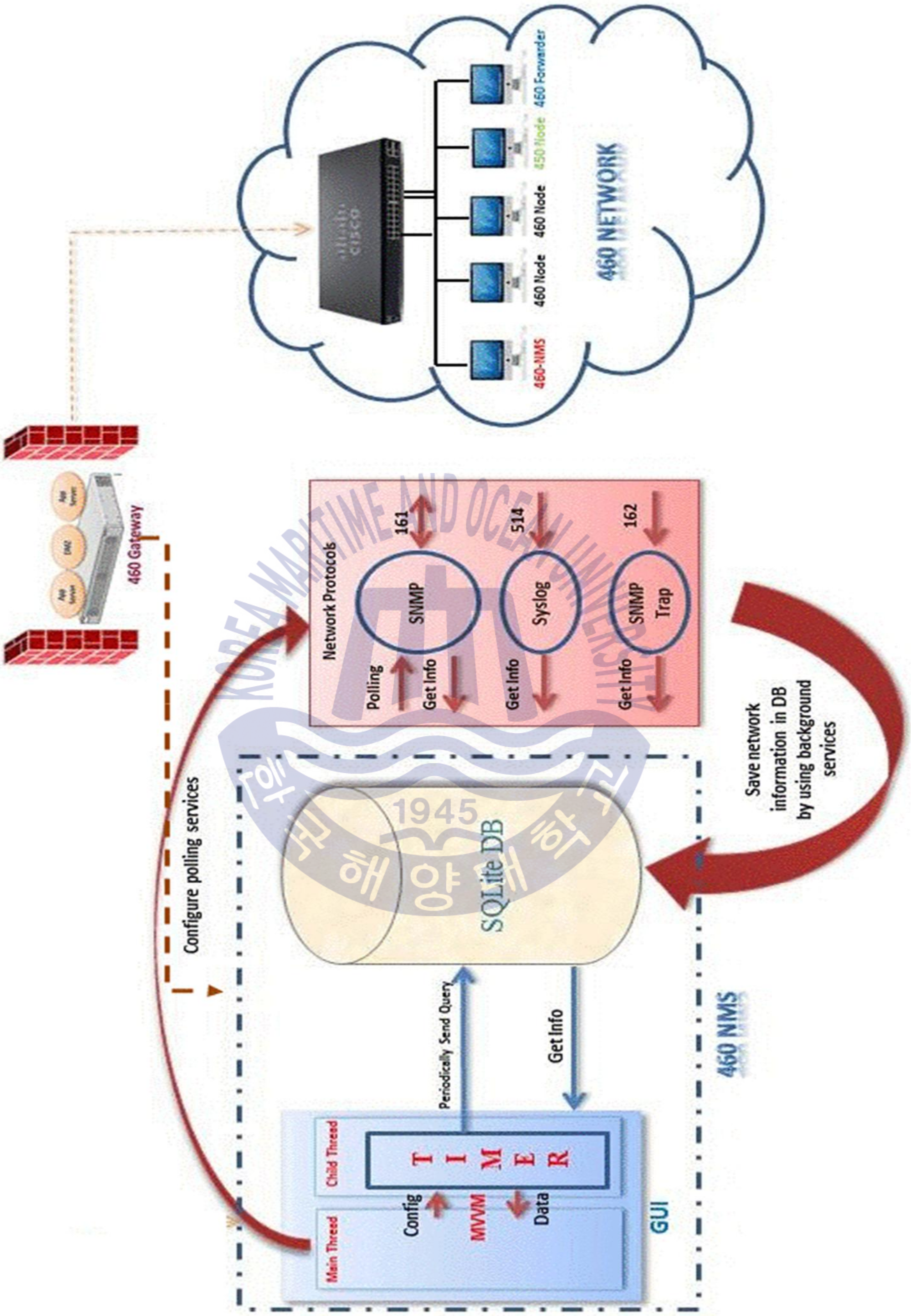

Figure 5.1. 460-NMS architecture

Figure 5.1 shows the conceptual model view of 460-NMS that defines the structure, behavior, and more detail view of the system.

1. In this study, 460-Network used CISCO 3560 series 460-Switch which contains 24 ports. So it can support up to 24 network devices includes 460-Nodes, 460-Forwarder, 450 Nodes and other 460-switch and through 460-Forwarder to controlled networks.
2. 460-NMS collects and presents the polling data from 460-Switch MIB file using SNMP, Syslog, and SNMP Trap protocols.
3. SNMP is an Internet standard protocol for collecting and organizing information of network devices that support SNMP protocol. It is widely used in network management systems to monitor network-attached devices for conditions that warrant administrative attention [11].

SNMP have the following basic components:

1. SNMP Manager: 460-NMS acts as an SNMP manager that communicates with the 460-Switch (SNMP Agent). It monitors 460-Network by sending queries and getting response to/ from 460-Switch.
2. SNMP Agent: 460-Swtich acts as an SNMP agent that manages network status information in a MIB file.
3. C# SNMP SharpNet library [12] is used to query the network information from 460-Swtich by SNMP protocol over UDP, port 161.

4. SNMP Trap is one type of notification in SNMP standard. By enabling SNMP Trap in 460-Swtich allows it to send notifications over UDP, port 162. It works in the case of any device plugged in or out, or any unknown device detected in the network.
5. Syslog is a logging mechanism in network devices used to collect system logs which contain critical information about the status, errors, warning, configuration logs, etc., of the devices. By enabling Syslog in 460-Switch allows it to send event notifications messages to Syslog server (460-NMS). It uses the UDP, port 514, for communication [13].
6. SQLite database management tool is used to store and manage the network information received from 460-Switch.
7. 460-NMS GUI is for monitoring and visualizing the network information. Backhand of GUI works by using threads and timers to get network information from the database periodically. Main thread to configure the polling services and child thread timers. Child thread contains timers that periodically send a query to retrieve network information from the database and send data to the main thread.

5.2 460-NMS Design and tools

5.2.1 Application Interface

The GUI of 460-NMS designed using the WPF technology. For great visual appearance and easy to change the GUI visualization, WPF technology is used. MVVM software architectural design used for design and development of 460-NMS.It is an architectural design pattern that separates an application into three layers that make up the pattern's title, as shown in *Figure 5.2*[14].

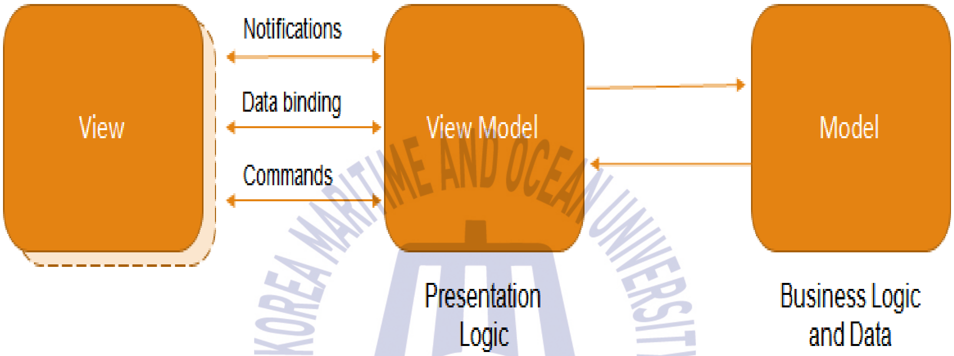

Figure 5.2. Model-view-model

5.2.2 Database

To manage the 460-Network information, a database is designed by using SQLite database management tool. SQLite is very fast, well-organized and embedded relational database [15].

5.2.3 Backhand developing

Backhand developing done by using Microsoft C# Programming language in the Microsoft.Net framework 4.5. The benefits of C# are its robustness, ease of programming, excellent database connectivity, and ability to run on the two most common operating system platforms (Windows and UNIX) [16].

5.3 Entity—Relationship Diagrams (ERD) Model of 460-NMS

The ERD model identifies the concepts or entities and the relationships between those entities, shown in *Figure 5.3*.

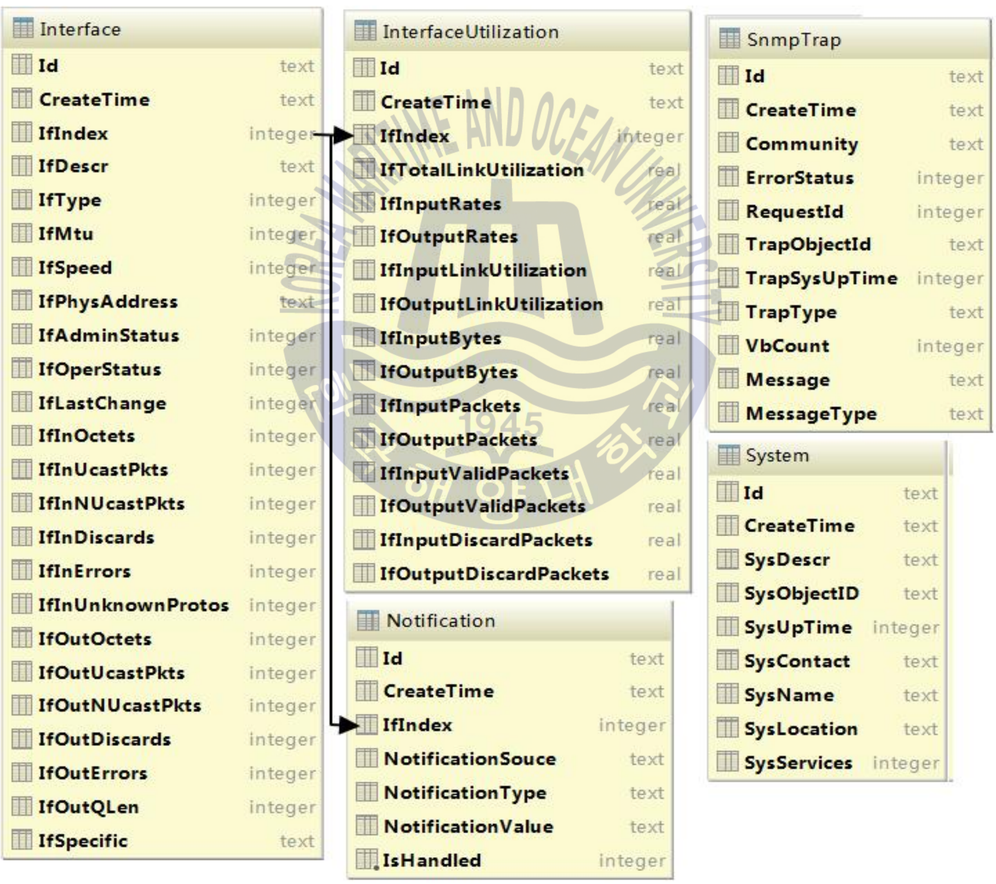

Figure 5.3 ER-model of 460-NMS

5.4 Traffic Flow Information Lists of 460-NMS

To calculate the traffic flow information of each 460-Switch interfaces, following formulas used as shown in *Table 1. Interface traffic flows information*:

Table 1. Interface traffic flows 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

Ps: TI = Time Interval between two polling in seconds

Give below is an example of Input / Output rates, to show how to calculate I/O rate of each 460-Switch interface, which is taken from **Table 1**; the same process applies for remaining traffic flow information:

a) Received and parsed the interface's input octet value by using SNMP SharpNet library.

b) Used the given below method to calculate Input rate of each interface:

Condition: If currIfInOctets < prevIfInOctets then currIfInOctets = currIfInOctets + 232-1

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

Note: As ifInOctets type in SNMP MIB file is Counter, when its value reaches at maximum value (232-1), it will be reset to 0.

Where,

CurrIfInOctets: interface's input octet's value at time2

PrevIfInOctes: interface's input octet's value at time1

5.5 SNMP MIB data parsing

For managing network information, tree-structured database MIB used in SNMP. Each node of MIB consists of the OID, data type, and value information entities [17]. Use SNMP SharpNet Library commands to fetch the network information of CISCO 460-Switch MIB File. For example to access "sysDesc" node in MIB tree structure, followed MIB tree structure green colored nodes as shown in *Figure* ***5.4***.

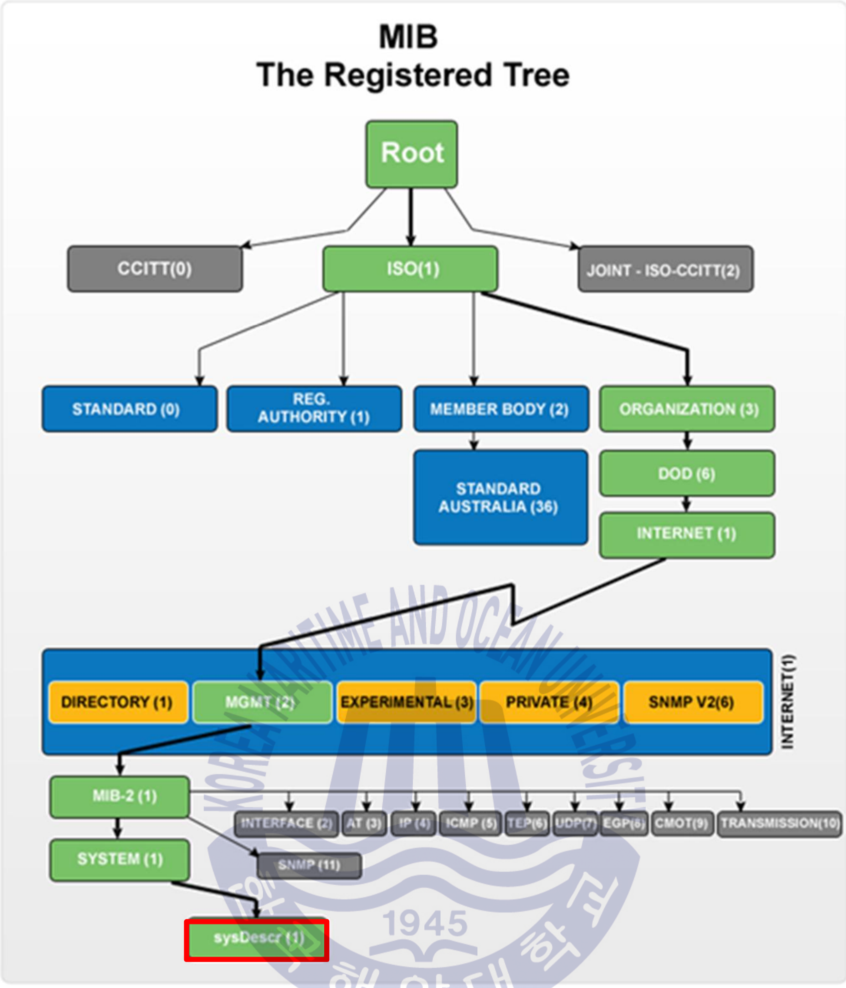

Figure 5.4. MIB tree structure

Access "sysDesc" tree structure format, mentioned below:

1. In string format: iso.org.dod.internet.mgmt.mib.system.sysDescr,
2. In number format: 1.3.6.1.2.1.1.1

The parsed information of "sysDesc" node entities of CISCO 460-Switch is mentioned below:

1. OID: 1.3.6.1.2.1.1.1

2. Data type: Octet String (as defined in MIB file)
3. Value: Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 15.0)

5.5.1 SNMP message parsing

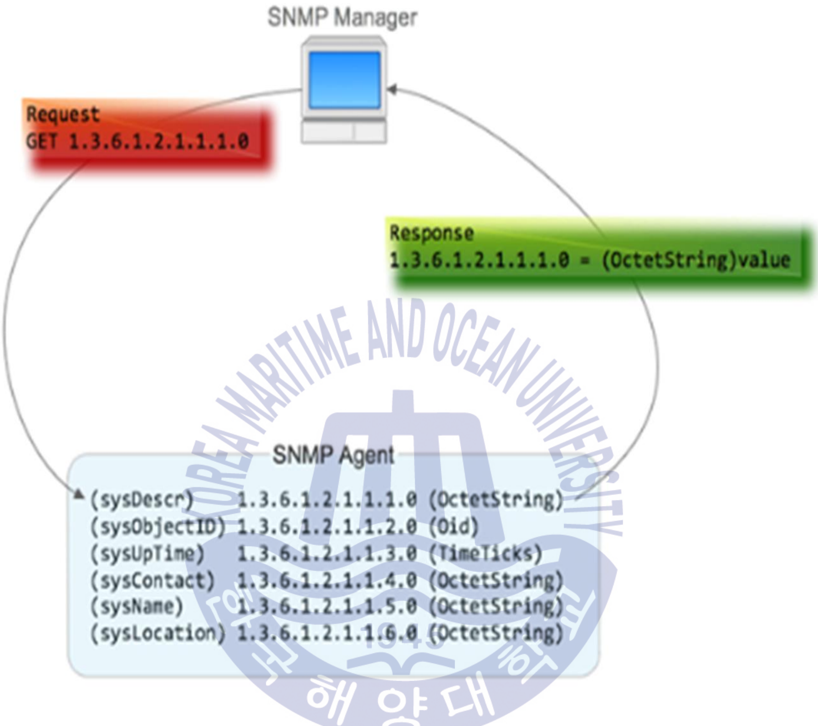

Figure 5.5. SNMP message parsing

460-NMS's background service will periodically send a request (containing OID) to SNMP agent, and then the agent will reply the specified object's information to SNMP manager. *Figure* **5**.**5**shows [11], SNMP Manager (460-NMS) requests OID: 1.3.6.1.2.1.1.1.0 through GET command using SNMP SharpNet library. In response, SNMP Agent (460-Switch) checks the requested

OID in MIB database and send the object's information contains value and data type to SNMP Manager (460-NMS).

5.5.2 SNMP Trap

If SNMP Trap enabled, when some changes happen in SNMP agent device (460-Switch), then the agent will send a notification to SNMP manager (460-NMS). For example, when 460-Switch configuration or BGP state changes, it will trigger a notification [11].

5.5.3 Syslog Parsing

If Syslog enabled, whenever 460-Switch adds a new log that will send to 460-NMS. Nowadays, the widely used Syslog format defined in RFC 5424, as shown in *Figure **4**.**6***

6 . Implementation and Testing of 460-NMS

As mentioned above, 460-NMS is a software application developed for monitoring the 460-Network devices to make sure a safe operation. The GUI of 460-NMS is user-friendly that consists of following information wizards.

6.1 460-NMS Interface

6.1.1 Login Wizard

The log in wizard designed to get access to 460-NMS by only trusted users, a user needs Admin ID and password to log in as shown in *Figure **6.1***.

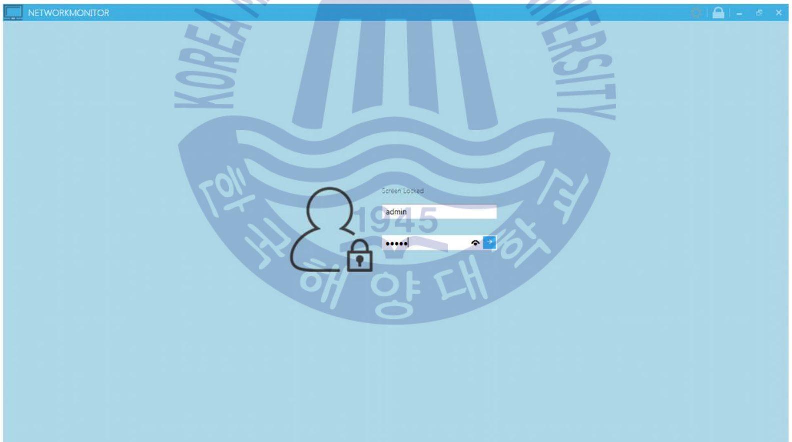

Figure 6.1. 460-NMS login interface

6.1.2 Main Form

The main form of the system consists of four parts as shown in *Figure **6.2***:

①. Toolbar: It has different chart layouts, export, screen refresh and print icons for main window network view.

②. Organization chart: The organization chart has three different views that are default, small and detail view. The root of the organizational structure represents 460-Switch, and it is child nodes that are 460-Switch interfaces. Double click on each node to see its detail information.

③. Search bar: It is the architecture view for searching the main system and its interfaces.

④. Navigation panel: For the types of network which has large number of nodes, navigation panel uses to view the particular node on the organization chart.

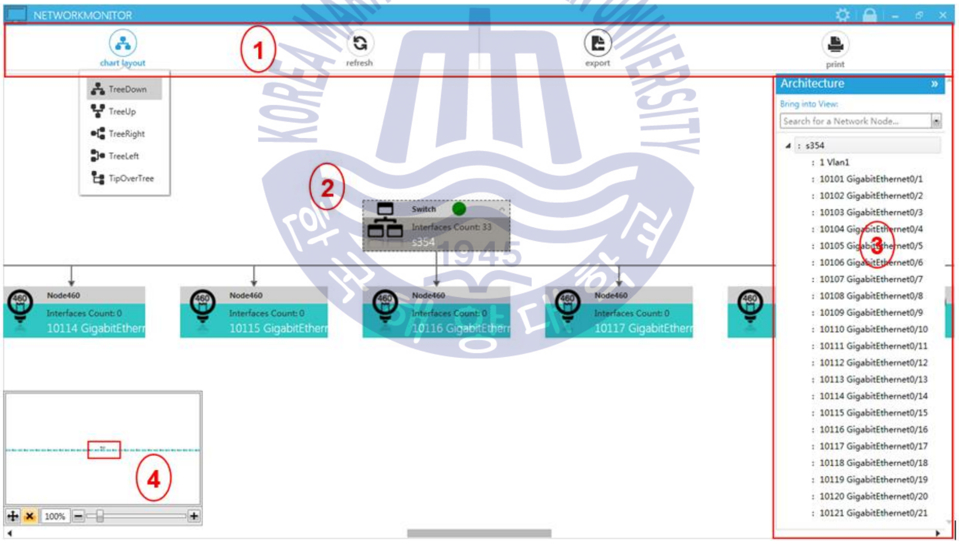

Figure 6.2. Main form of 460-NMS

6.2 460-NMS Testing

6.2.1 Lab Test

Figure 4.7 IEC 61162-460 shows in *Figure 4.7* the 460 Network designed in our lab. According to the testing requirements of IEC 61162-460 Network standard, 460-NMS monitors the lab designed 460-Network to analyze and check its performance. Below procedure shows, how 460-NMS analyze and monitors the 460-Switch and its nodes:

1. Set the community name, agent IP and other system configuration settings to connect 460-NMS to 460-Switch, as shown in *Figure **6.3***:

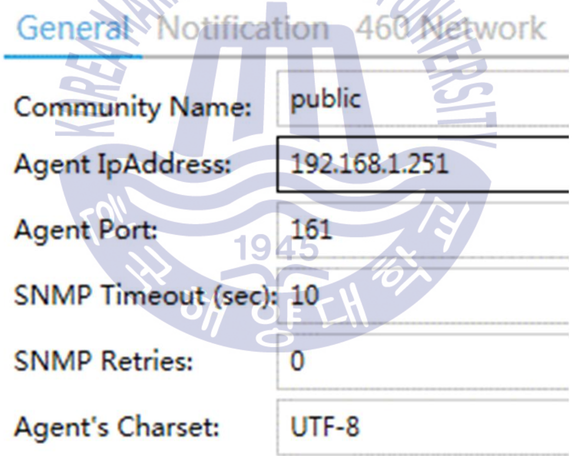

Figure 6.3. System setting general tab

2. According to the requirements, by inputting data as illustrated in *Figure **6.4***, set the warning and critical threshold values for the network overloads.

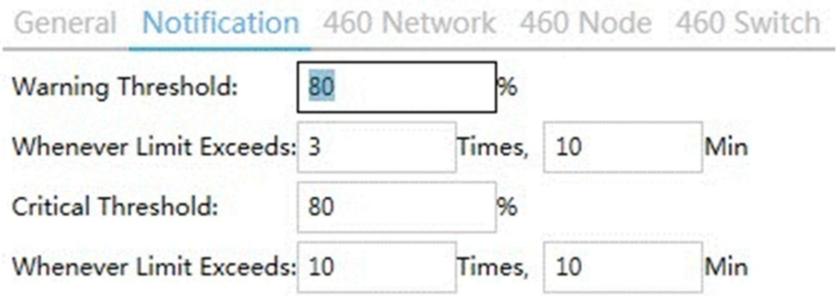

Figure 6.4. Notification tab

3. After successful connection, *Figure* ***6.5*** shows the detail information of CISCO L3 Catalyst 3560 X series 460-Switch with its descriptive interfaces which includes interface ID, name, type, physical address, speed, and status. It contains four tabs, namely, interfaces, notifications, SNMP Trap and Syslog.

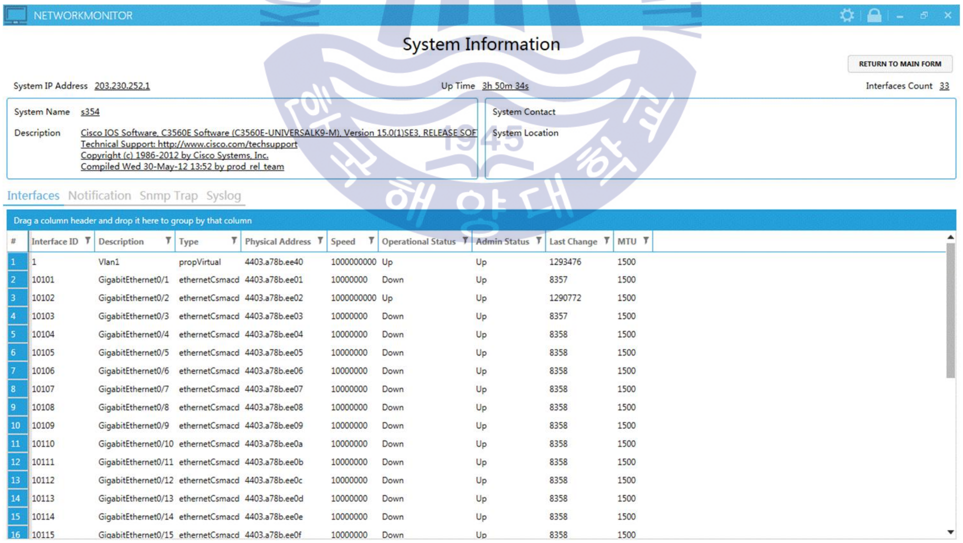

Figure 6.5. 460-Switch information wizard

4. Now set the maximum bandwidth to 1 MB, of interface ID “10102”, to check the network traffic overload shown in *Figure* ***6.6*** (Interface Max Bandwidth Setting).

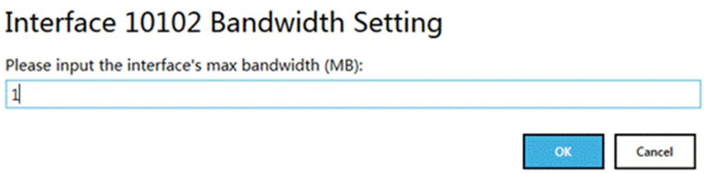

Figure 6.6. Interface max bandwidth setting

5. After testing the traffic flow rates of interface ID “10102”, as the bandwidth reached 80% of predefined value 1 MB, received the “traffic overload” notifications of input/output rates, shown in *Figure* ***6****.7.*

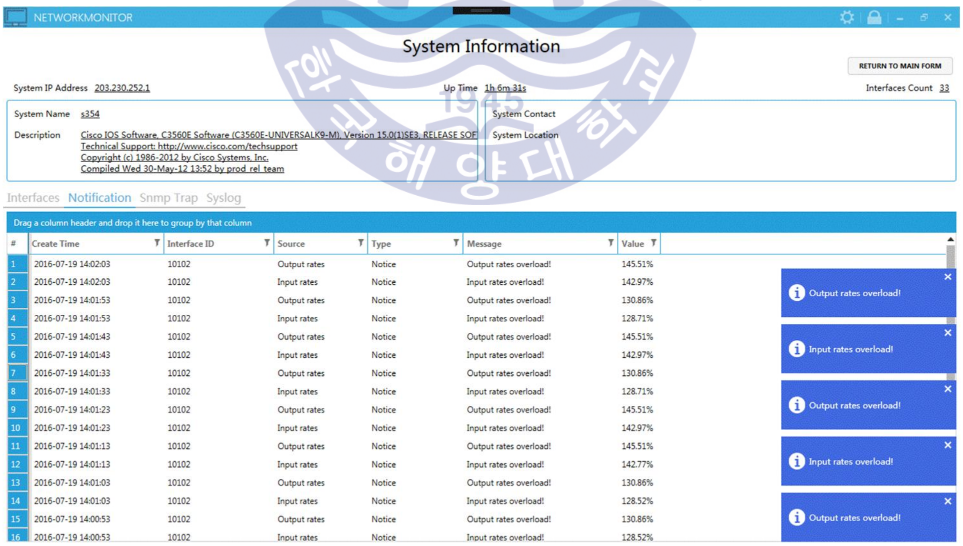

Figure 6.7. System information

6. During testing, when the connected device to the GigabitEthernet0/15 interface plugged out, the SNMP agent generated the SNMP Trap, "changed state to down," as shown in *Figure **6.8***.

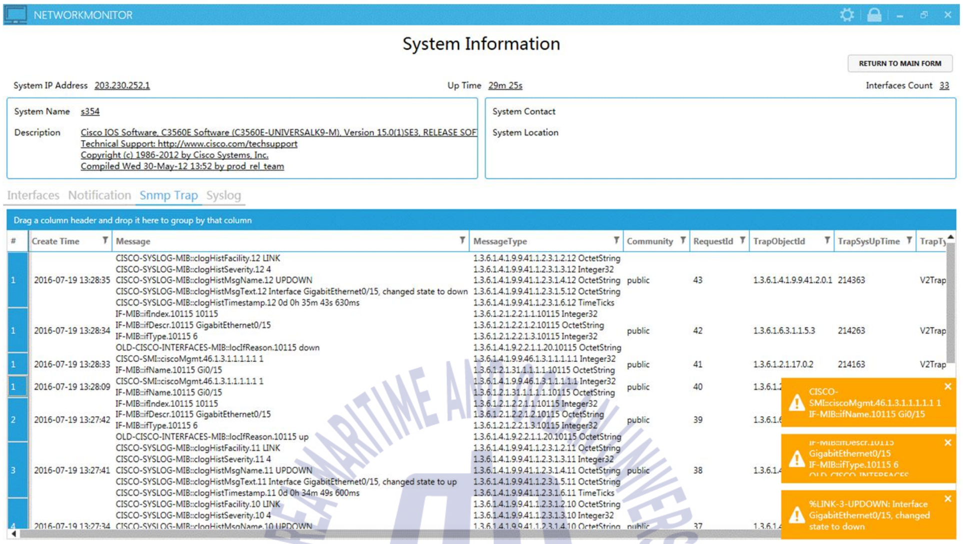

Figure 6.8. System traps information

7. To test the connection of a network device within the network, when the connected device to the GigabitEthernet0/15 interface plugged out, the Syslog error notification generated, "%LINK-3-UPDOWN: Interface GigabitEthernt0/15, changed state to down", as shown in *Figure **6.9***.

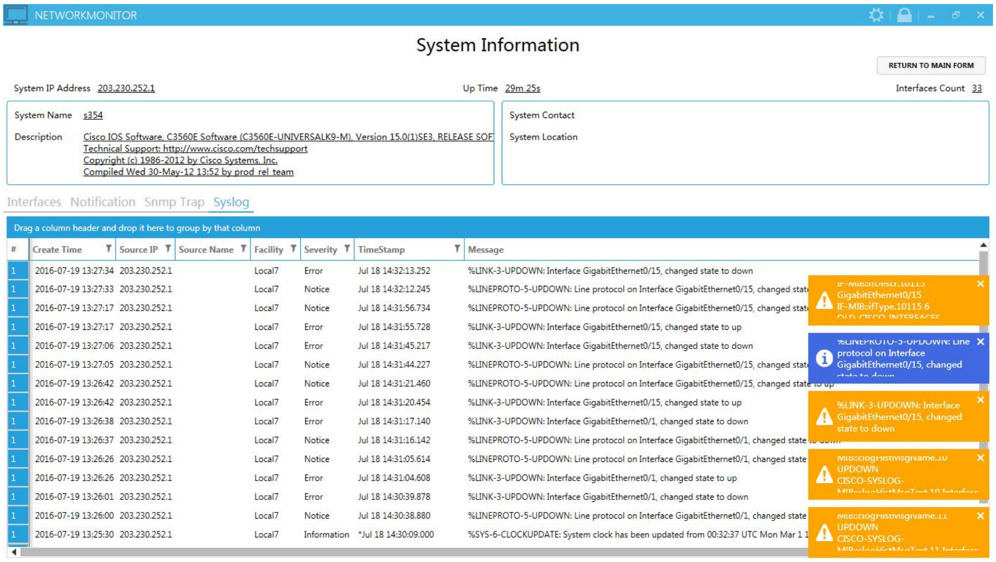

Figure 6.9. Syslog information

8. To view the detail information of each 460-Switch interface, click on the interface node shown in *Figure 6.2. Main form*. Interface Information Wizard manages the core information of each interface. It contains two tabs, Traffic flow and Charts that manages I/O Rates, I/O Link Utilization, I/O Bytes, I/O Packets, I/O Valid Packets, and I/O Discard Packets information. According to the network load requirements of IEC 61162-460, tested the network traffic capacity of interface ID “10102”. During testing when traffic load exceeds the 80% of the limit for 30 secs more

than ten times within a period of 10 min. The system generated the alarm “Output rates overload” shown in the Figure 6.10.

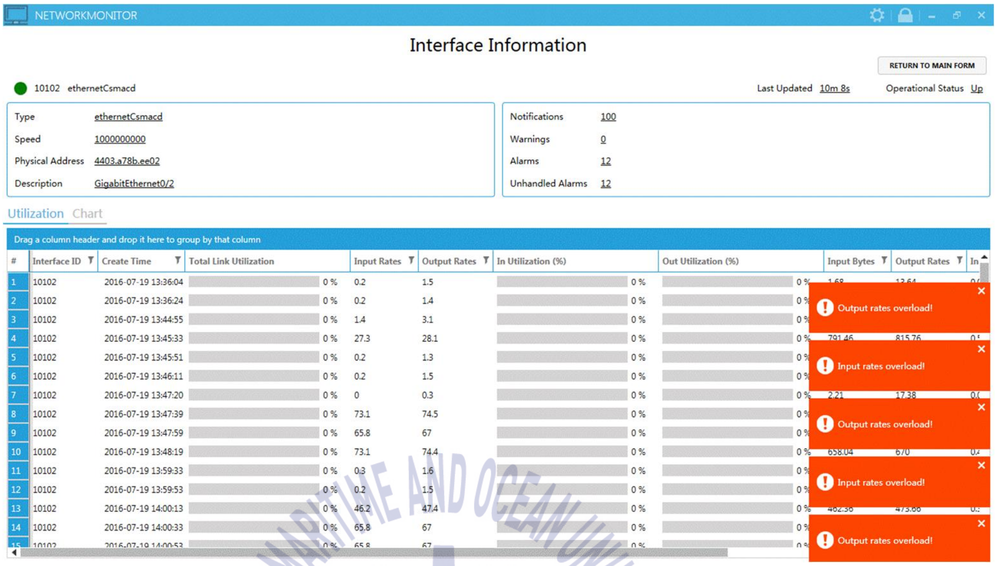

Figure 6.10. Interface information wizard

9. *Figure **6.11*** shows the Input/output rate Chart View of interface ID “10102”, the green spine lines represents Input rates with max 680.9 kb/s and blue represents Output rates with max 18.9 kb/s.

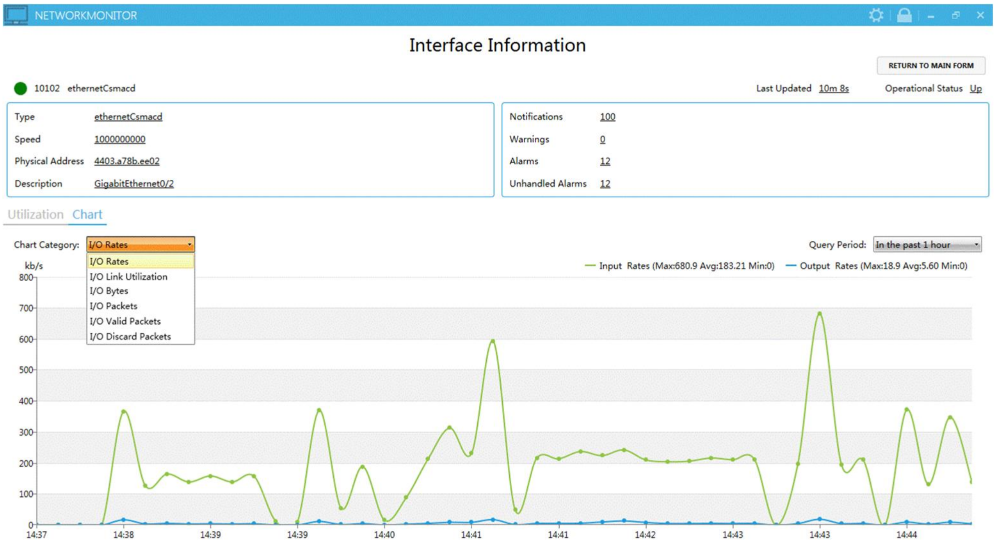

Figure 6.11. I/O rates chart view

10. There are three types of alerts in the proposed system: Notice (blue), Warning (Orange) and Alarm (red). Whenever the system gets the information as SNMP trap, Syslog, or network overloaded, it will give the alert to the network administrator. Meanwhile, the alert will be saved into the database.

6.3 Real Network Test

*Figure **6.12*** shows the very complex network environment which is designed in a marine electronic company. It consists of different ship data networks which are IEC 61162-460, IEC 61162-450, IEC 61162-2 (NMEA 2000), IEC 61162-1,-2 (NMEA 0183) with 460-Gateway, Gateway 450 to 0183, Gateway

N2K to 0183, Gateway 0183 to N2K and excludes from uncontrolled networks like the internet.

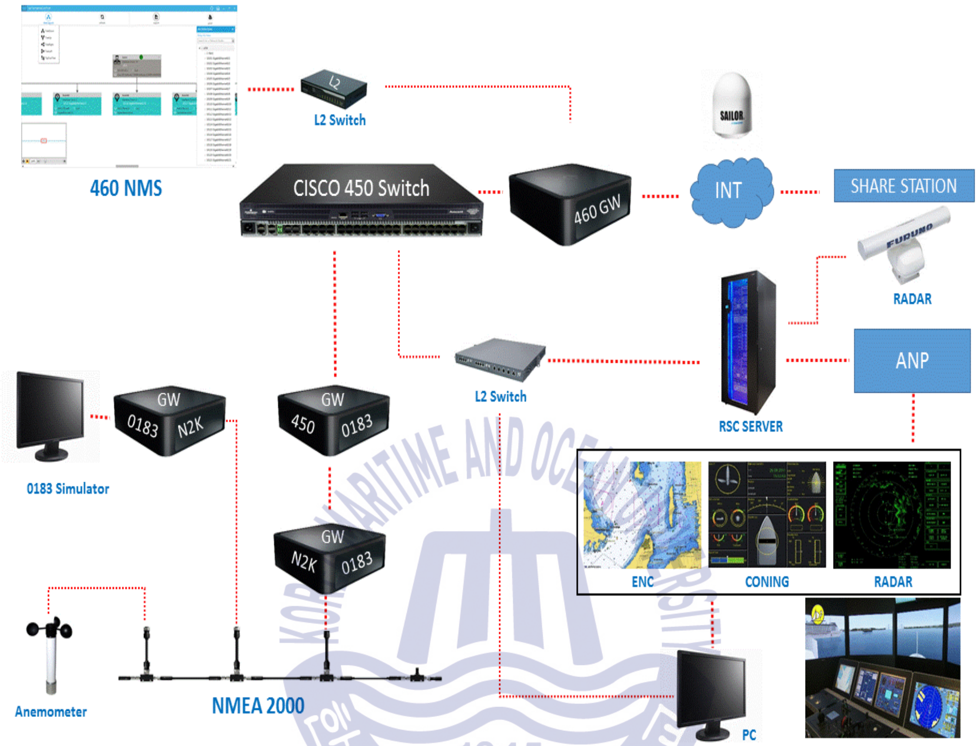

Figure 6.12 Complex 460-network design

To analyze and monitor the company's designed network by using 460-NMS, the following experiments were performed:

1. Configured the CISCO Catalyst L3 3650 460-Switch and enabled SNMP, SYSLOG and SNMP Trap for testing the complex 460-Network operation, as shown in *Figure **6.13***

```
System: Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 03.03.05SE RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 30-Oct  Switch 146144257
Total Number of Interfaces: 35
Interface [0]: GigabitEthernet0/0 ethernetCsmacd e865.4960.1480
Interface [0]: Null0 Other
Interface [0]: GigabitEthernet1/0/1 ethernetCsmacd e865.4960.1481
Interface [0]: GigabitEthernet1/0/2 ethernetCsmacd e865.4960.1482
Interface [0]: GigabitEthernet1/0/3 ethernetCsmacd e865.4960.1483
Interface [0]: GigabitEthernet1/0/4 ethernetCsmacd e865.4960.1484
Interface [0]: GigabitEthernet1/0/5 ethernetCsmacd e865.4960.1485
Interface [0]: GigabitEthernet1/0/6 ethernetCsmacd e865.4960.1486
Interface [0]: GigabitEthernet1/0/7 ethernetCsmacd e865.4960.1487
Interface [0]: GigabitEthernet1/0/8 ethernetCsmacd e865.4960.1488
Interface [0]: GigabitEthernet1/0/9 ethernetCsmacd e865.4960.1489
Interface [0]: GigabitEthernet1/0/10 ethernetCsmacd e865.4960.148a
Interface [0]: GigabitEthernet1/0/11 ethernetCsmacd e865.4960.148b
Interface [0]: GigabitEthernet1/0/12 ethernetCsmacd e865.4960.148c
Interface [0]: GigabitEthernet1/0/13 ethernetCsmacd e865.4960.148d
Interface [0]: GigabitEthernet1/0/14 ethernetCsmacd e865.4960.148e
Interface [0]: GigabitEthernet1/0/15 ethernetCsmacd e865.4960.148f
Interface [0]: GigabitEthernet1/0/16 ethernetCsmacd e865.4960.1490
Interface [0]: GigabitEthernet1/0/17 ethernetCsmacd e865.4960.1491
Interface [0]: GigabitEthernet1/0/18 ethernetCsmacd e865.4960.1492
Interface [0]: GigabitEthernet1/0/19 ethernetCsmacd e865.4960.1493
Interface [0]: GigabitEthernet1/0/20 ethernetCsmacd e865.4960.1494
Interface [0]: GigabitEthernet1/0/21 ethernetCsmacd e865.4960.1495
Interface [0]: GigabitEthernet1/0/22 ethernetCsmacd e865.4960.1496
Interface [0]: GigabitEthernet1/0/23 ethernetCsmacd e865.4960.1497
Interface [0]: GigabitEthernet1/0/24 ethernetCsmacd e865.4960.1498
Interface [0]: GigabitEthernet1/1/1 ethernetCsmacd e865.4960.1499
Interface [0]: GigabitEthernet1/1/2 ethernetCsmacd e865.4960.149a
Interface [0]: GigabitEthernet1/1/3 ethernetCsmacd e865.4960.149b
Interface [0]: GigabitEthernet1/1/4 ethernetCsmacd e865.4960.149c
Interface [0]: StackPort1 propVirtual
Interface [0]: StackSub-St1-1 propVirtual
Interface [0]: StackSub-St1-2 propVirtual
Interface [0]: Vlan1 propVirtual e865.4960.14c7
Interface [0]: Vlan100 propVirtual e865.4960.14d1
```

Figure 6.13 460-Switch interfaces

2. After successful 460-Switch configuration, connected the 460-NMS to 460-Switch and configured the system settings in 460-NMS which includes community name, IP address (192.168.100.100), etc. as can be seen in *Figure* ***6.14*** the tree view of 460-Switch as root, with its interfaces as child nodes.

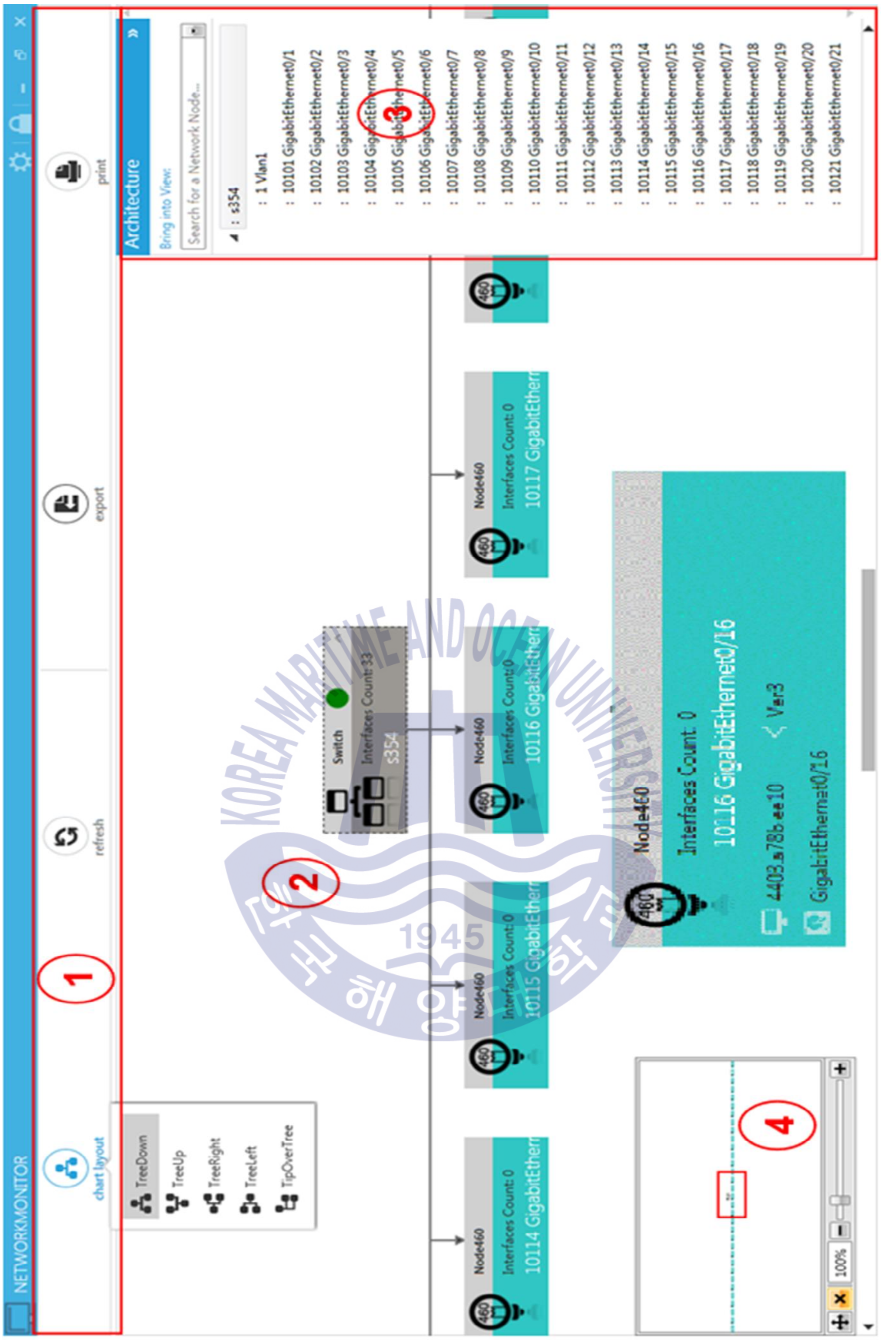

Figure 6.14 460-Switch with interfaces

3. *Figure* ***6.15***, shows the 460-Switch detailed information with its interfaces which includes system name, description, IP address, system up time. Also, each interface information that includes interface description, Physical address, type, speed, operation and admin status.

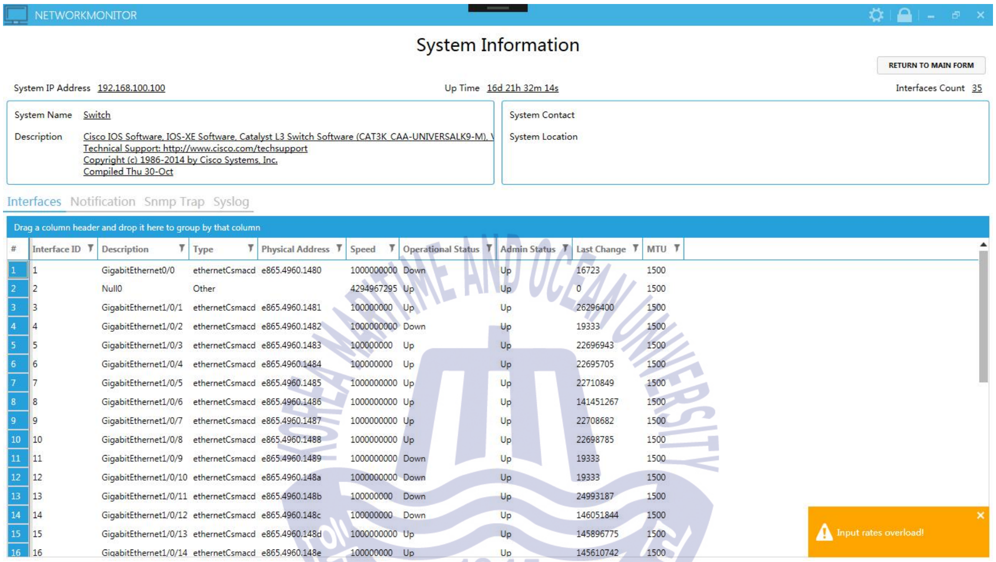

Figure 6.15 460-Switch information

4. To test the traffic load, set the maximum bandwidth to "0.1 MB" of each interface. Shown in *Figure* ***6.16*** the notifications received as "warning": "Input rates overload" as bandwidth reached above 80% of predefined value "0.1MB".

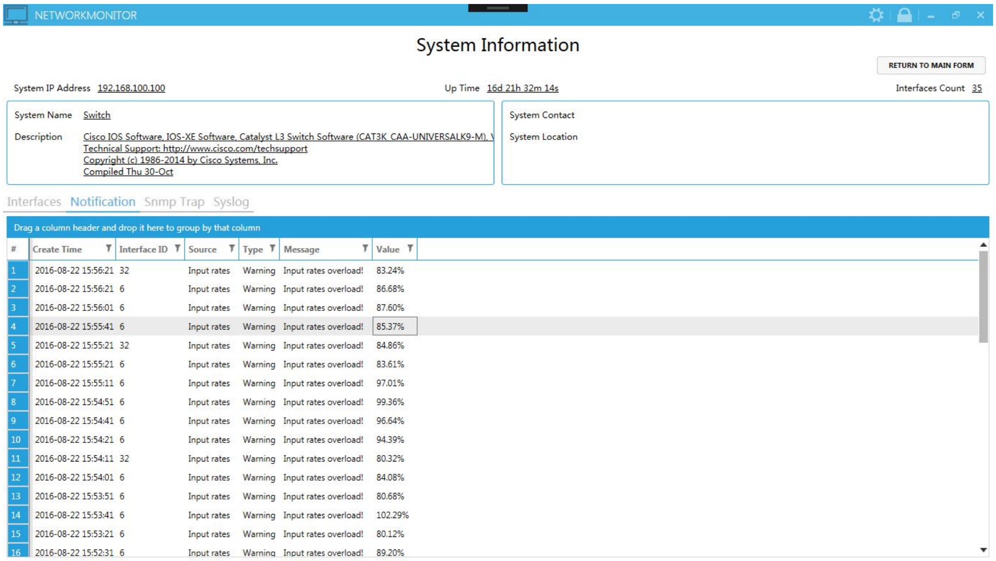

Figure 6.16 Input rates overload notifications

5. During device connections test, when the connected device to the GigabitEthernet1/0/12 interface plugged in, the Syslog notification generated as "%LINK-3-UPDOWN: Interface GigabitEthernt1/0/12, changed state to up" with Source IP "192.168.100.100" and creation time "2016-8-22 15:36:56" pm. As shown in *Figure **6**.**17***.

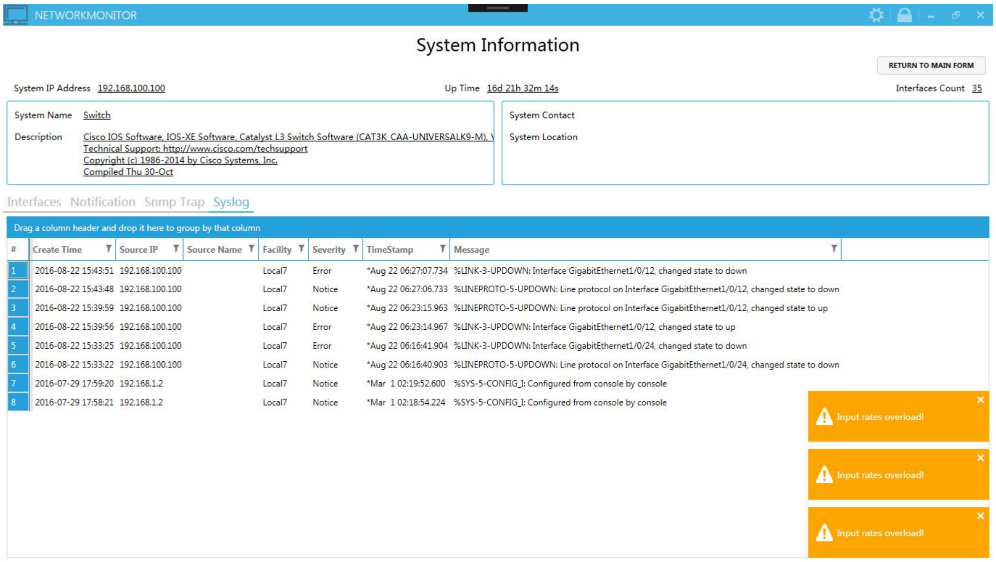

Figure 6.17 Syslog notifications

6. *Figure **6.18*** shows the traffic flow information of interface named "GigabitEthernet1/0/16" and ID "18" with Input rate values 0.4, 0.2, 0.5 MB, as input rates are greater than the predefined value of 0.1 MB, so received many warnings of input rate overload.

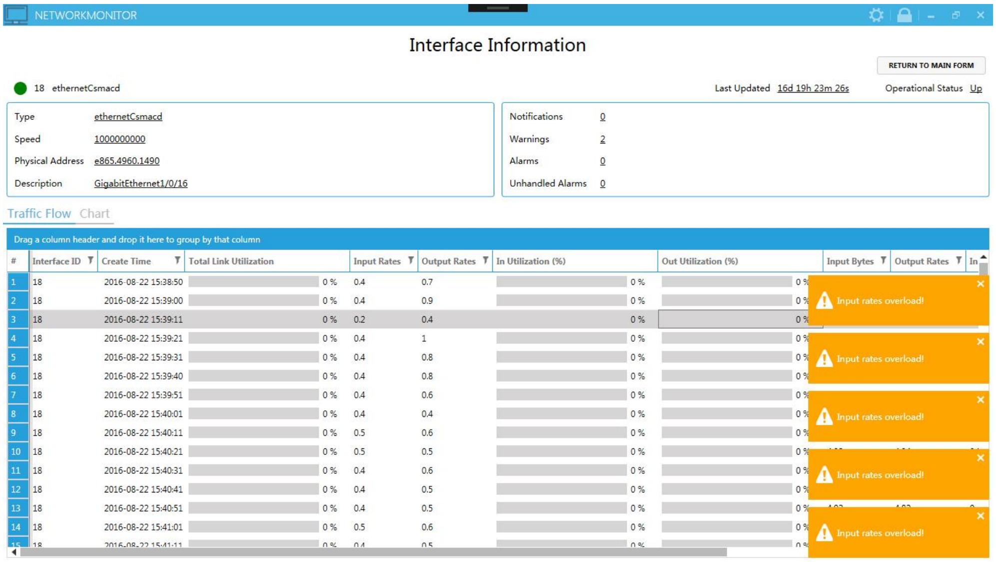

Figure 6.18 Traffic flow information

7. *Figure* ***6.19*** shows the Input / Output rates chart view of the interface named "GigabitEthernet1/0/16", the green spine lines represents Input rates with 1037.5 kb/s Max and the blue spine lines represent output rates with 8045.2 kb/s Max.

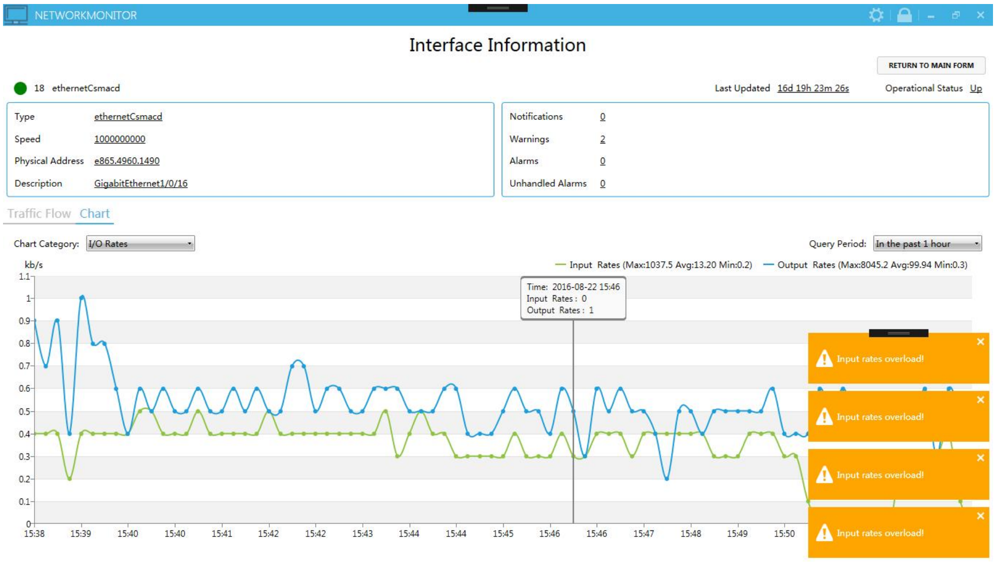

Figure 6.19 Input / output flow chart

After successful tests on the network of lab and company's designed 460-Network according to the requirements of IEC 61162-460 international standard, it is confirmed that 460-NMS is capable of analyzing and monitoring the performance of 460-network and keep the data networks safe from internal and external threats. Also notifications, warnings or alarms in case of any abnormal status are generated according to the standard.

7 . Conclusion

In this thesis, according to the requirements of IEC 61162-460 network standard, a secure 460-Gateway, a 460-Network, and a 460-NMS are designed, implemented and tested to satisfy the needs of onboard security for ship's data networks. The network instruments used to design the 460-Network comprises of CISCO 460-Switch, 460-Gateway, Fortinet 300D 460-Firewall and 460-Nodes. The 460-NMS is tested at both in the lab and real network environment composed by marine electronic company, for analyzing and monitoring the 460-Network load, traffic flow, and device connections. 460-NMS notifies the system administrator in case of any problem occurs via alarms, warnings or notifications. The test results are confirmed the performance of the proposed 460-NMS is compliance with the IEC 61162-460 standard.

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.

[2] O. J. Rodseth, "Design challenges and decisions for a new ship data network," ISIS 2011, Hamburg, 15th to 16th, 2011. [ONLINE] Available at http://www.mits-forum.org/resources/lwe-paper-isis-v9.pdf.

[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.

[4] IEC TECHNICAL COMMITTEE 80: MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS, International Electrotechnical Commission. [ONLINE] Available at http://www.iec.ch/index.htm. [Accessed 30 August 2016], 1906.

[5] IEC 61162-450: Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 450: Multiple talkers and multiple listeners - Ethernet interconnection, Ed. 1.0., 2011.

[6] IEC 61162-460: Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 460: Multiple talkers and multiple listeners – Ethernet interconnection - Safety and Security, 2013.

[7] ISOC RFC 791: Internet Protocol (IP), Standard STD0005 (and updates).

[8] CISCO. CISCO CATALYST 3560 SERIES SWITCHES. [ONLINE] Available at http://www.cisco.com/c/en/us/index.html.

[9] Adam Bristow, Bill Dickie, Bruce Davis., “the FortiGate Cookbook 5.2”, FortiGate/FortiOS, FortiGate 5.2.0, 2015.

[10] Wolfgang Barth, “System and Network Monitoring,” Nagios, 2nd Edition, 2008

[11] ISOC RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.

[12] SNMP SharpNet, SNMP Library for C#. [ONLINE] Available at http://www.snmpsharpnet.com/.

[13] ISOC RFC 5424: The Syslog Protocol.

[14] Ashish Ghoda., Windows 8 MVVM Patterns Revealed: covers both C# and JavaScript, Apress, 2013.

[15] Sibsankar Haldar., SQLite Database System Design and Implementation, Second Edition, Version 1, 2015.

[16] Mark Michaelis, Eric Lippert., “Essentials C# 6.0”, 1st edition, Addison-Wesley Professional, 2015.

[17] ISOC RFC 3418: Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

[18] NMEA 0183: Standard For Interfacing Marine Electronic Devices, Version 3.01, January 1, 2012. [ONLINE] Available at http://caxapa.ru/thumbs/214299/NMEA0183_.pdf

[19] Ø.J.Rødseth, Maritime Information Technology Standards, Computer networks on board and shore, Last Updated 2012, [ONLINE] Available at http://www.mits-forum.org/network.html

[20] SANS Institute InfoSec Reading Room, Security SNMP, SNMP Version 3, Version 1.4, [ONLINE] Available at https://www.sans.org/reading-room/whitepapers/networkdevs/securing-snfFmp-net-snmp-snmpv3-1051

[21] Frank Cassidy, Larry Anderson, Lee A. Luft, NMEA 2000 A Digital Interface for the 21st Century, Institute of Navigation's, 2002, California [ONLINE] Available at http://www.digitalmarine.kr/info/nmea/NMEA-2000-tech-information.pdf

[22] J.D.Case, M.Fedor, M.L. Schoffstall, J.Davin, RFC 1157, Simple Network Management Protocol (SNMP), May 1990

[23] Kyung-Yup Kim, Dong-Hyun Park, Jin-Bo Shim, Yung-Ho Yu, "A Study of Marine Network NMEA 2000 for e-navigation", JKOSME, 2010.

[24] Zu-Xin Wu, Sobia Rind, Yung-Ho Yu, "Ship's Network Security and Monitoring System using SNMP", International Symposium on Marine Engineering & Technology 2016 (ISMT 2016), September, 2016

APPENDIX

1. Information List of 460-NMS Database

Table 2 Data entity-system

Name	Type	Description
Id	Guid	Primary key
CreateTime	DateTime	Record created time
SysDescr	String	A textual description of the entity.
SysObjectID	String	The vendor's authoritative identification of the network management subsystem contained in the entity.
SysUpTime	UInteger	The time since the network management portion of the system was last re-initialized.
SysContact	String	The textual identification of the contact person for this managed node.
SysName	String	An administratively-assigned name for this managed node.
SysServices	Integer	The physical location of this node.
SysLocation	String	A value which indicates the set of services that this entity primarily offers.

Table 3 Data entity-interface

Name	Type	Description
Id	Guid	Primary Key
CreateTime	DateTime	Record Created Time
IfIndex	Integer	A unique value for each interface.
IfDescr	String	A textual string containing information about the interface.
IfType	Integer	The type of interface, distinguished according to the physical/link protocol(s) immediately `below' the network layer in the protocol stack.
IfMtu	Integer	The size of the largest datagram which can be sent/received on the interface specified in octets.
IfSpeed	UInteger	An estimate of the interface's current bandwidth in bits per second.

IfPhysAddress	String	The interface's address at the protocol layer immediately `below' the network layer in the protocol stack.
IfAdminStatus	Integer	The desired state of the interface.
IfOperStatus	Integer	The current operational state of the interface.
IfLastChange	UInteger	The value of SysUpTime at the time the interface entered its current operational state
IfInOctets	UInteger	The total number of octets received on the interface, including framing characters.
IfInUcastPkts	UInteger	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
IfInDiscards	UInteger	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
IfInErrors	UInteger	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
IfInUnknownProtos	UInteger	The number of packets received via the interface which was discarded because of an unknown or unsupported protocol.
IfOutOctets	UInteger	The total number of octets transmitted out of the interface, including framing characters.
IfOutUcastPkts	UInteger	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
IfOutDiscards	UInteger	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
IfOutErrors	UInteger	The number of outbound packets that could not be transmitted because of errors.

Table 4 Data entity-snmp trap

Name	Type	Description
Id	Guid	Primary Key
CreateTime	DateTime	Record Created Time
Community	Integer	SNMP server's community name.
TrapObjectId	String	Trap's object identifier
TrapSysUpTime	UInteger	Trap's SysUpTime

TrapType	String	The Type of Traps.
Message	String	Trap's textual information.

Table 5 Data entity-syslog

Name	Type	Description
Id	Guid	Primary Key
CreateTime	DateTime	Record Created Time
SourceName	Integer	Syslog server name
Facility	Integer	Syslog's current facility
Severity	Integer	Syslog's current severity level.
Message	Integer	Syslog's textual information.
TimeStamp	UInteger	Syslog server timestamp.

Table 6 Data entity-notification

Name	Type	Description
Id	Guid	Primary Key
CreateTime	DateTime	Record Created Time
IfIndex	Integer	A unique value for each interface.
NotificationSource	String	Notification Source
NotificationType	Integer	Notification type (Notice, Warning, Alarm)
NotificationValue	Integer	Notification value

Table 7 Data entity-interface traffic flow

Name	Type	Description/Formula
Id	Guid	Primary Key
CreateTime	DateTime	Record Created Time
IfIndex	Integer	A unique value for each interface.
IfTotalLinkUtilization	Decimal	(IfInputLinkUtilization+ IfOutputLinkUtilization)/2
IfInputRates	Decimal	(currIfInOctets - prevIfInOctets)/(1024*TI)
IfOutputRates	Decimal	(currIfOutOctets - prevIfOutOctets)/(1024*TI)

IfInputLinkUtilization	Decimal	(currIfInOctets - prevIfInOctets)*8/(IfSpeed*TI)
IfOutputLinkUtilization	Decimal	(currIfOutOctets - prevIfOutOctets)*8/(IfSpeed*TI)
IfInputBytes	Decimal	(currIfInOctets - prevIfInOctets)/1024
IfOutputBytes	Decimal	(currIfOutOctets - prevIfOutOctets)/1024
IfInputPackets	Decimal	(currIfInUcastPkts - prevIfInUcastPkts)/1024
IfOutputPackets	Decimal	(currIfOutUcastPkts - prevIfOutUcastPkts)/1024
IfInputValidPackets	Decimal	IfInputPackets - IfInputDiscardPackets
IfOutputValidPackets	Decimal	IfOutputPackets - IfOutputDiscardPackets
IfInputDiscardPackets	Decimal	(currIfInDiscards - prevIfInDiscards)/1024
IfOutputDiscardPackets	Decimal	(currIfOutDiscards - prevIfOutDiscards)/1024

Ps: TI = Time Interval between two polling in seconds

2. Syslog Message

Table 8 Syslog facility

Facility value	Description
0: kern	kernel messages
1: user	user-level messages
2: mail	mail system
3: daemon	system daemons
4: auth	security/authorization messages
5: syslog	messages generated internally by syslogd
6: lpr	line printer subsystem
7: news	network news subsystem
8: uucp	UUCP subsystem
9: clock	clock daemon
10: authpriv	security/authorization messages
11: ftp	FTP daemon
12: ntp	NTP subsystem
13: logaudit	log audit
14: logalert	log alert
15: cron	scheduling daemon
16: local0	local use 0 (local0)
17: local1	local use 1 (local1)

18: local2	local use 2 (local2)
19: local3	local use 3 (local3)
20: local4	local use 4 (local4)
21: local5	local use 5 (local5)
22: local6	local use 6 (local6)
23: local7	local use 7 (local7)

Table 9 Syslog-severity level

Severity Level	Description
0: emergencies	The system is unusable
1: alerts	Immediate action is required
2: critical	A critical condition exists
3: errors	Error message
4: warnings	Warning message
5: notifications	A normal but significant condition
6: informational	Information message
7: debugging	Debug output and very detailed logs

3. SNMP Versions

Table 10 SNMP versions

Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2C	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication.
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: DES 56-bit encryption 3DES 168-bit encryption AES 128-bit, 192-bit, or 256-bit encryption

4. SNMP Message

Table 11 SNMP message fields

Field	Description
SNMP message	A sequence representing the entire SNMP message consisting of the SNMP version, Community string, and SNMP PDU.
SNMP Version	An Integer that identifies the version of SNMP.
SNMP Community string	An Octet String that may contain a string used to add security to SNMP devices.
SNMP PDU	An SNMP PDU contains the body of the SNMP message. There are several types of PDUs. Three common PDUs are GetRequest, GetResponse, SetRequest.
Request ID	An Integer that identifies a particular SNMP request. This index is echoed back in the response from the SNMP agent, allowing the SNMP manager to match an incoming response to the appropriate request.
Error	An Integer set to 0x00 in the request sent by the SNMP manager. The SNMP agent would place an error code in this field in the response message if an error occurred processing the request. Some error codes include:
	0x00 -- No error occurred
	0x01 -- Response message too large to transport
	0x02 -- The name of the requested object was not found
	0x03 -- A data type in the request did not match the data type in the SNMP agent
	0x04 -- The SNMP manager attempted to set a read-only parameter
	0x05 -- General Error (some error other than the ones listed above)
Error Index	If an Error occurs, the Error Index holds a pointer to the Object that caused the error, otherwise, the Error Index is 0x00.
Varbind List	A Sequence of Varbinds.
Varbind	A Sequence of two fields, an Object ID and the value for/from that Object ID.
Object Identifier	An Object Identifier that points to a particular parameter in the SNMP agent.
Value	SetRequest PDU -- Value is applied to the specified OID of the SNMP agent.
	GetRequest PDU -- Value is a Null that acts as a placeholder for the return data.
	GetResponse PDU -- The returned Value from the specified OID of the SNMP agent.

5. Abbreviations

Table 12 Abbreviations

IEC	International Electro-Technical Commission
DMZ	Demilitarized Zone
NMS	Network Monitoring System
SNMP	Simple Network Management Protocol
NMEA	National Marine Electronic Association
LWE	Light Weight Ethernet
ICS	Integrated Communication System
GMDSS	Global Maritime Distress and Safety System
PAGA	Public and General Announcement
VPN	Virtual Private Network
FW/GW	Firewall / Gateway
CAN	Controller Area Network
PGN	Parameter Group Number
OSI	Open System Interconnect
TAG	Transport Annotate and Group
SFI	System Function Identifier
MSM	Multi-Sentence Message
CRP	Command Response Pair
SNGF	Serial to Network Gateway Function Block
ONF	Other Network Function Block
SF	System Function Block
NF	Network Function Block
VLAN	Virtual Local Area Network
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
WAP	Wireless Application Protocol
DoS	Denial of Service
IP	Internet Protocol
MIB	Management Information Base
SD	Structured Data
PoE	Power over Ethernet
POST	Power-On-Self-Test
VDOMs	Virtual Domains
NAT	Network Address Translation
WPF	Windows Presentation Foundation
MVVM	Model-View-View Model
ERD	Entity Relationship Diagram
OID	Object Identifier

BGP	Border Gateway Protocol
EDP	Extended Data Page
DP	Data Page
PS	PDU Specific
PF	PDU Format
DA	Destination Address
PDU	Protocol Data Unit
PGN	Parameter Group Number
MAC	Media Access Control
CSMA	Carrier Sense Multiple Access
CD	Collision Detection
FDDI	Fiber Distributed Data Interface
MVVM	Model-View-View Model
WPF	Windows Presentation Foundation
BGP	Border Gateway Protocol
GPS	Global Positioning System
ECDIS	Electronic Chart Display and Information System
ENC	Electronic Navigation Chart