TransNav
http://www.transnav.eu
the International Journal on Marine Navigation and Safety of Sea Transportation
Volume 16
Number 3
September 2022

DOI: 10.12716/1001.16.03.07

Software Solutions for GMDSS Network and Equipment

D.S. Ilcev
University of Johannesburg (UJ), Johannesburg, South Africa

ABSTRACT: This paper introduces software solutions for communication, equipment control, and management of oceangoing ships for enhanced Global Maritime Distress and Safety System (GMDSS) network and equipment. This software controls all maritime transmission systems and integrates communications software at level of server and workstations. Equipment control software is used to control and maintained locally or remotely transceivers, transmitters, receivers and other hardware. Special management software is included to process, analyze and exploit the various types of information generated by GMDSS networks and equipment. This papers are also includes the concept of software solutions on radio and satellite GMDSS ship terminals, on radio and satellite GMDSS coast terminals, and as well as in GMDSS Cospas-Sarsat ground terminals. In addition, the cybersecurity system in GMDSS security management is also described in this paper.

1 INTRODUCTION

The GMDSS solutions are designed to comply with International Maritime Organization (IMO), International Convention for the Safety of Life at Sea (SOLAS), International Telecommunication Union (ITU), and international maritime specifications. All types of oceangoing ships are increasingly using systems that rely on digitization, integration, software, and automation, which requires onboard cyber risk management and improved functionality. Modern GMDSS and digital oceangoing ships are increasingly using novel radio and satellite communication systems and technology that rely on digitization, integration, security and automation, which call for cyber risk management onboard and to enable the proper operation of radio or satellite systems.

At this point, as maritime software systems continue to develop, Information Technology (IT) and Operational Technology (OT) onboard ships are being networked together and more frequently connected to the Internet via ships radio and satellite communication systems. This brings the greater risk of unauthorized access or malicious attacks to ships' systems and networks. Risks may also occur from personnel accessing systems onboard ships, for example by introducing malware via removable media and connecting hardware with adequate software to the Internet.

2 SOFTWARE SOLUTIONS ON RADIO GMDSS SHIP TERMINALS

Given the key role of GMDSS in saving lives, ensuring its continued availability is crucial. While it could be possible to disrupt ships radio or satellite communications via jamming, the set of technologies used should mean other channels continue to work. A risk is its reliance on a single operator for satellite communications, but other providers are likely to be approved in the next few years. Due to its broadcast nature and simple analogue modulation the lack of confidentiality means that UHF (Ultra High Frequency), VHF (Very High) and MF/HF (Medium/High Frequency) radio communication networks should not be used to transmit sensitive data and information. In practice, these solutions can be used for general ship-to-ship and ship-to-shore communications.

The development of software-defined radio technology means that radio signals of the frequencies used by satellite communication systems can be received and analyzed cheaply. If sensitive information is being transmitted in plain text, then it may be possible to intercept it. Older satellite equipment may also be at risk of direct attacks over the Internet. The advances in radio and satellite technology have brought widespread benefits to society and industry, and the maritime sector is at a point where it can start to capitalize on these developments too. New hardware initiatives such as Radio-Automatic Identification System (R-AIS), NAVigational DATa (NAVDAT) and VHF Data Exchange System (VDES) solutions look set to increase the level of background communications between ships and ship to shore, and offer the potential for increases in efficiency and safety.

However, the integration of new connectivity with the support of modern software solutions into existing platforms is not without risks, and therefore a lot of care needs to be taken in order to ensure the continuous security of the entire system controlled by computers (PC).

For instance, since R-AIS network lacks any mechanism for validating messages are being broadcast correctly, it is possible to spoof messages to present as a different vessel, or “fake” a vessel location. This is often used to conceal illegal activity such as illegal fishing or evading international sanctions. Additionally, since R-AIS network is used to generate collision-avoidance warnings, spoofing ship locations could be used to “force” a vessel off course and “push” it into dangerous waters.

Maritime mobile radio and satellite networks are increasingly used for voice and data communications when a ship is either at dock, sailing inshore or in distress alert because of its lower cost and latency than satellite. Often, the same equipment is used to access both Internet and terrestrial services via suitable software. In fact, data and voice transmitted over Internet or cellular networks is encrypted, but information may then pass over the internet where no confidentiality can be guaranteed.

Although, the cellular standards have controls in place to ensure message integrity, communications could be disrupted through jamming, but authorities would be quick to react to mobile network outages. With the availability of cheaper, faster internet access, usage will increase and the risk of malicious documents or software being downloaded onto onboard devices will also increase.

The secure Web browser via Internet onboard ships via satellite communication equipment has to provide some advantages:

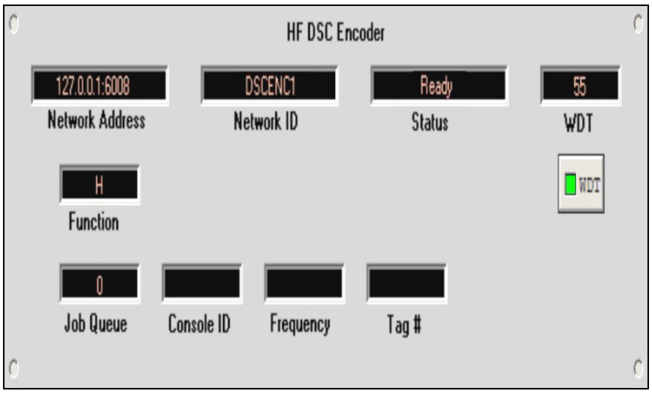
1. Secure Internet access for surfing, interacting and E-mails including attachments must use approved Windows 10 operational systems.
2. Onboard computers or laptops and network or GMDSS server must be protected against any malware such as Trojans, ransomware, Advanced Threat Protection (ATP) and zero-day exploits.
3. Dangerous scripts and the click on malicious links no longer pose a threat. Thus, if ransomware or an encryption Trojan gets onto any computer, it encrypts PC data or locks operating system.
4. High usability of a secure Internet Web browser means that onboard operator does not have to get used to the new browser system or environment.

The biggest problem while using browsers is active content such as Flash, Java, JavaScript, ActiveX or HTML 5, whereby foreign code is executed on the PC, on the own operating system and thus in the data infrastructure itself. If this program code contains malicious software, it is also executed. This includes e-mails with malicious links that operator opens in the browser. Consequently, a secure web browser is essential.

With the real browser in the box terminal server, operator can feel completely safe when surfing the Internet. The basic principle here is that Rohde & Schwarz (R&S) offers the completely separate operating system and browser, which keeps malware away from the computer (PC) or the corporate network. Very important: For users, there are no restrictions on surfing the Internet. They use the secure web browser as usual. For companies, this type of secure Internet access means a considerable relief. That possibility is because fewer hacked computers reduce IT system downtime and the associated loss of productivity.

The maritime complete solution has a special software package that includes all functions and management processes, various systems and operators from an intuitive user interface with a focus on easy operation and simple integrated management of space (radio and satellite) Communication, Navigation and Surveillance (CNS) systems.

The maritime complete solution has a special software package that includes all functions and Incorporating VHF and MF/HF Ship Radio Station (SRS) and ground based Coast Radio Station (CRS), including Ship Earth Stations (SES) and Coast Earth Station (CES) terminals, can be remotely controlled via touch screen computers and suitable Network Management System (NMS). Thus, in this way it can be configured the GMDSS communication systems and customized to suit all requirements. From a simple single GMDSS radio and radio equipment and systems setup to a complex onboard ships and national system with multiple operator and communication radio sites installed at various remote locations, to provide complete GMDSS solutions.



HF DSC Encoder

Network Address	Network ID	Status	WDT
127.0.0.1:6008	DSCENC1	Ready	55

Function
H

Job Queue	Console ID	Frequency	Tag #
0			

Figure 1. Radio DSC Encoder Software – Source: TransOceana

Communication and navigation operators onboard oceangoing ships must take great care not to use unauthorized software and to keep them away from shipboard systems. In this way, it is recommended to ensure that viruses and malware are scanned before connecting authorized USB storage devices to IT or OT and other shipborne network systems. In addition, all ppersonal computers, laptops, tablets, USB memory sticks or cellphones must not be connected to onboard operational systems. At the same time, it will be important to guard the ship's crew and all passengers and train them on what to do if important OT systems are not working. Everyone needs to know where to get IT and OT help, and report suspicious or unusual problems faced by IT and OT systems.

Many practical skills require ships operators to use new passwords from time to time and every time they log on to the ship. Choose complex passwords with numbers, symbols and some capital letters. Operators need to be careful, so the operators must be able to do that remember them and keep usernames and passwords for personal use only. Change the default user passwords and delete the user accounts of colleagues who have left the ship. Ship operators should only open emails or open attachments from senders they know and trust. They also need to know what to do with suspicious emails, and to think carefully before sharing information on social media or in person email about own shipping company, business, ship or crew.

Oceangoing ships use trusted Virtual Private Network (VPN) client and trusted storage disks. Trusted VPN Client is hardware-independent, allowing it to be deployed on a wide variety of advanced hardware platforms. Different end users in maritime industry can work as usual with the Microsoft Windows 10 platform without any business interruption. However, IT administrator manages a software package that can easily be installed on existing systems. Today’s hard disks have storage capacities that make it possible to store a large amount of sensitive data locally. Notebooks and portable storage devices, such as Universal Serial Bus (USB) flash drives and portable hard disks, can easily be stolen or left behind. In order to prevent sensitive data from falling into the wrong hands, storage devices have to be encrypted using a safe t method of comprehensive full-disk encryption.

2.1 *Radio DSC Encoder Software Solutions on GMDSS Ships*

The TransOceana Digital Selective Calling (DSC) encoder product is a special software application that runs on the new generation of Windows Operating System (OS), which hardware configuration is shown in Figure 1. The DSC encoder is used to convert the radio VHF and MF/HF DSC messages from an operator console into audio signals which are then sent to the ground radio stations via transmitter. The encoder can support two similar radios such as two radio VHF devices, or two different types of radio devices, such as a VHF and MF/HF radio transceiver. Otherwise, the configuration can be changed as required by user.

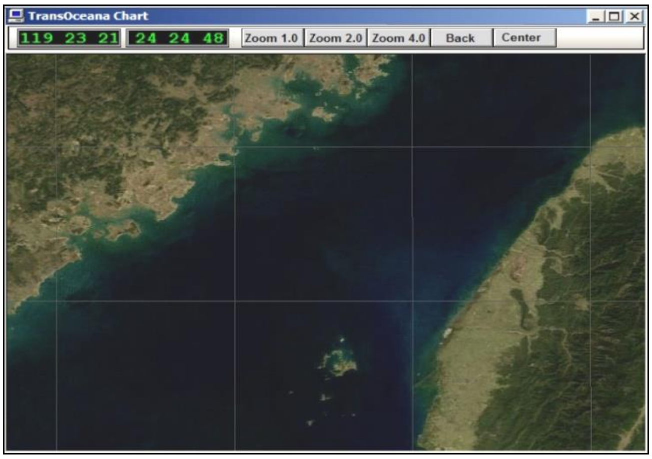


Figure 2. Radio DSC Encoder Software – Source: TransOceana

The GMDSS ships radio receiver and transmitted stations for VHF and MF/HF are installed in compliance with relevant IMO and ITU specifications for DSC, NAVigational TEleX (NAVTEX), NAVDAT, R-AIS, VDES, voice and data logging. Both hardware and software are developed for SRS terminals that serve GMDSS solutions. As technology continues to develop IT and OT systems, GMDSS terminals will be connected to the shore Internet.

The software script files are used to configure an encoder for any type of radio, which unit is shown in Figure 1. The script file is used to initialize the radio before a transmit and to reset the radio after a transmit. In fact, script files exist for many different radio models with new ones added as needed. This means a new transmitter can be added by simply adding a new encoder and script.

The encoder can be configured for radio VHF, MF and/or HF, which architecture can be changed to support different radio assignments. Encoders can be added or removed from the system at any time. An encoder can be used as shared assets by multiple consoles or limited to a specific console. The message queuing design is used to support multiple consoles. The encoder is also compatible and can be used with older generation of radio transmitters or with newer, modern radios. Thus, a wide range of interfacing methods can be used to support any type of transmitter. According to the regulatory compliance this encoder unit meets or exceeds DSC class A requirements such as ITU-R M.493.13, ITU-R M.541.9, ITU-R M.821.1 and ETS 300 338 regulations.

2.2 *Radio DSC Map Functions Software Solutions on GMDSS Ships*

The DSC TransOceana map function option runs on the operator console applications, which hardware configuration is illustrated in Figure 2. The map function provides an easy to use method for displaying ship locations on a regional map without having to purchase or interface to 3rd party map applications. Thus, if a DSC message is received with a position, then the map is automatically updated with the location the Maritime Mobile Service Identity (MMSI) of the certain vessel. This mapping feature is integrated with the virtual receivers within the operator console to selectively filter what is added to the map. The map display always centers on the last position added making it easy to locate the vessel.

Landmarks and positions of other special interest can be added to the map and saved to the ship's database. Layers can be defined by the operator to add or remove location types. In that manner, by integrating the DSC map function with a virtual receiver, an alert can be sounded when the map is updated. For example, if a distress call within a geographic area is received, the map will be updated and an alert sounded.

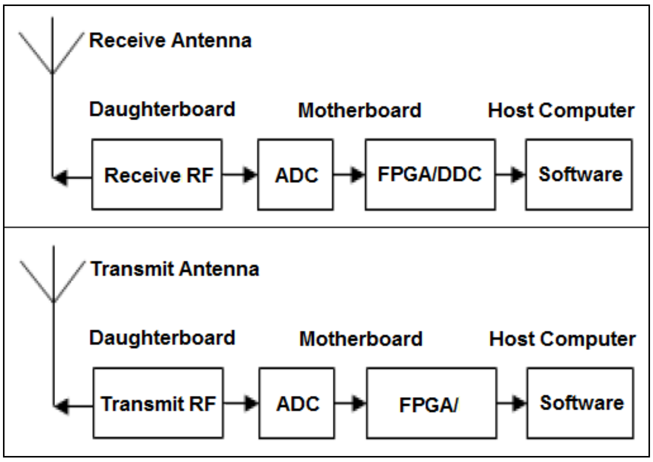


Figure 3. DSC Receiver/Transmitter – Source: Gannapathy

The mapping program indicates flexibility in providing the relative position of vessels reporting positions system in a radio DSC transmission. Onboard mapping screen can be centered on distress or at operator's discretion mapping screen can display chart or map available to operator in a JPG format. One click access to map from regular console display or can be displayed on split screen operating system. If there is a distress call, the position of the vessel in distress flashes to alert operator t vessels in the area that could respond. Mapping system is compatible and integrated into the operator console and is an option available with purchase of console. No separate interface needed to install mapping in the device.

2.3 *Shipborne Software Defined Radio (SDR) on GMDSS Ships*

In 1992, Joseph Mitola proposed the basic concept of Software Defined Radio (SDR) system and equipment. Namely, SDR equipment is a special radio communication system that uses software to process various signals in lieu of the traditional hardware components that are generally made for those dedicated tasks. It is mostly used in all mobile communications, including for maritime applications, research and development, and military projects. In fact, a typical SDR setup involves an Radio Frequency (RF) front-end connected to a computer that will perform the conversions from analog to digital, and the inverse for receiving or sending signals, respectively. Because of rapidly developing digital electronics, the capabilities of SDR system and equipment continue to increase.

The new SDR system is an instantaneous radio communication implemented from previous radio components, such as filters, modulation, demodulation, decoding, detectors, amplifiers and mixers in software. The motherboard is placed between the daughter board (RF front-end) and host computer at both transmitter and receiver. The Analog-to-Digital Converter (ADC) and Digital-to-Analog Converter (DAC) changes the data format from analogue to digital and vice versa.

The system uses Field Programmable Gate Array (FPGA) to execute high bandwidth mathematical calculations such as decimation, modulation/demodulation, and digital down conversion, digital up conversion and interpolation signal processing process. Besides FPGA, programmable hardware SDR has additionalm approaches, such as Digital Signal Processors (DSP) and General-Purpose Processor (GPP). The wired is used to transmit and receive data between motherboard and host computer. The architecture of SDR at the receiver and transmitter are shown in Figure 3.

The specialized processor in SDR is called DSP, which is needed to extract the information from the signal and it represents the signals digital as a sequence of numbers or symbols. The basic operations of the processor include some processes such as filtering, transformations, modulation, correlation and convolution. The FPGA compoents are semiconductor devices which consist of logic components and interconnect that are both programmable. The element can be combined to perform simple gate level logic operations such as AND, XOR, etc. The advantages of the architecture of an FPGA allow the designs to perform multiple computational operations in parallel. Parallelism enable substantial data throughput at relatively low lock rates.

The GPP elements are designed for computers which is personal computer /workstation. It is easier to program the platform and makes it flexible. However, high energy consumption is needed to achieve the performance of objective. Currently SDR can be used for all mobile CNS and lso to implement simple radio modem technologies such as Global System for Mobile Communications (GSM), Wide band Code Division Multiple Access (WCDMA), WiMAX , Wi-Fi and others.

Once SDR system transfers the data from one source to a digital format, software-driven automated features are used to conduct secondary tasks involving radio communications. A radio program can also transmit and receive a range of frequencies.

The risk of hardware replacement or adaptation according to customer needs is also removed.

The current and future SDR market in the RF range will offer users UHF, VHF, MF, HF and satellite frequency bands supporting CNS solutions, by component will offer software, receivers, transmitters, auxiliary and other hardware system), by platform will provide service to commercial maritime, land (road and rail) and aeronautical applications, including military, police and space applications,

With the rapidly evolving modern digital electronics, SDR capabilities continue to increase in maritime space (radio and sagtellite) CNS systems such as: communications that support Voice, Data and Video (VDV), navigation that supports all GNSS networks, AIS, Directopn Finder (DF), DSC, NAVTEX, radars, and other devices, including new surveillance systems.

3 SOFTWARE SOLUTIONS ON SATELLITE GMDSS SHIP TERMINALS

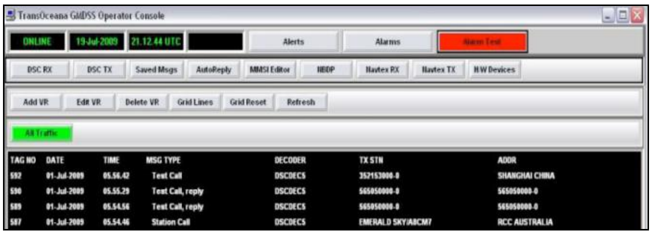
When the SES terminal receives a signal from terrestrial network and Internet via satellite network, it need to be transformed into understandable data and repackaged in order for it to be transmitted out through the satellite network. Therefore, this is a job for the different software programs installed on modems in the SES communication stations. Each ship's SES terminal is operated and controlled with a suitable desktop computer (PC) or laptop to perform all functions related to receiving and sending messages and their printing. Therefore, an external computer is usually competed with its own keyboard, screen, hard disk/diskette drive and printer. This computer may be used to format and store messages, and also to run specialized software, for example formatting the data into a data report for sending to a reporting centre, or compressing input data to save transmission time.

Ideally, computer hardware with appropriate onboard ships software solutions should be dedicated exclusively to the management of SES terminals, but in some installations it can assign other multi-task functions onboard the ship. In such a way, the following precautions on ships must be organized in connection with the use of multi-tasking computers

1. A position reporting system is using external or internal the current US GPS, Russian GLONASS and other GNSS solutions to provide the ship's position.
2. Input devices as some sensors, connected via a computer or interface unit for monitoring example a ship's machinery, structure, cargo, environment, and so on.
3. Special devices for output control, such as electrical switches, relays or valves, typically used to control operations at remote installations, for example a lighthouse or oil platform.
4. The Data Terminal Equipment (DTE) unit also provides storage for different messages created on the keyboard, before they are transmitted over the satellite link. These messages may be created for commercial communications with shore customers and in particular for security purposes due to GMDSS distress networks.

For instance, if a multi-tasking computer is used to operate Inmarsat SES terminals, no unnecessary software should be installed, to avoid the computer being busy when required to perform an Inmarsat satellite communication functions. This is also important specially to avoid the danger of the computer becoming infected by viruses, which could adversely affect SES communications.

The software used on the maritime SES terminals is called Management System Software (MSS), which can be installed in PC as integration part of each SES transceiver. For the Local Area Network (LAN) interface to work without any further setup, the PC must be set up to obtain an IP address and a Domain Name System (DNS) server address automatically in any time.



TAG NO	DATE	TIME	MSG TYPE	DECODER	TX STN	ADDR
592	01-Jul-2009	05.56.42	Test Call	DSCDECS	352153000-0	SHANGHAI CHINA
590	01-Jul-2009	05.55.29	Test Call, reply	DSCDECS	565050000-0	565050000-0
589	01-Jul-2009	05.54.56	Test Call, reply	DSCDECS	565050000-0	565050000-0
587	01-Jul-2009	05.54.46	Station Call	DSCDECS	EMERALD SKY/A8CM7	RCC AUSTRALIA

Figure 4. GMDSS Operator Cosoles (A shortened version of the screen) – Source: TransOceana

All GMDSS versions of Inmarsat Ship Earth Station (SES) terminals have approved voice and Data Terminal Equipment (DTE) that interfaces with the user and which generally refers to the PC and screen, keyboard and printer (or user interface).

Inmarsat GEO mobile satellite operator recommends that the recommended client version of the Transmission Control Protocol (TCP) accelerator be installed on GMDSS SES terminals as it improves performance when sending files. The TCP accelerator must be installed on Windows 10/11 Operating Systems (OS), which overcomes the drawbacks of standard TCP and enhances the performance over a satellite network by: (1) Improving true bandwidth estimation, so customers with high QoS can start at a higher transmission rate. It can also withstand occasional packet drops and is resilient to sudden band width changes; (2) Increasing window size, and thus improves TCP performance in larger bandwidth applications; and (3) Ensuring high transfer rates and less delay through delay-based congestion control. Thus, TCP handles communications between applications and network software. It breaks messages into packets before they are sent by IP (Internet Protocol) and reassembles them when they arrive.

4 SOFTWARE SOLUTIONS IN GMDSS COAST TERMINALS

In the terminal infrastructure of GMDSS radio and satellite stations, the Windows server typically operates in a virtualized environment of the type provided by Citric, VMware, and Microsoft. The

Windows server provides a desktop session to each fixed or mobile user, with the thin client only displaying the session. Thus, in the box terminal server, the specially deployed browser, such as stead R&S product, does not run in the Windows server desktop session, but on a separate virtual machine. Only the browser interface is transmitted to the desktop session for display. This allows for a reliable isolation of the intranet from the Internet.

Thanks to its flexible architecture, this browser can be integrated into any existing virtual infrastructures. It is no longer necessary to use dedicated terminal servers (which have high administrative overhead and lack the desired level of security) as a surfing alternative. Central management makes it easy to implement security policies and configurations as well as to generate, certify and distribute the necessary guest images.

4.1 *Software Solutions in GMDSS Coast Radio Terminals*

The GMDSS coast stations for VHF and MF/HF are delivered in compliance with relevant IMO and ITU specifications, including DSC, NAVTEX, NAVDAT, R-AIS, VDES, voice and data logging, and interface with landline telephones, which GMDSS Operator Cosoles are shown in Figure 4. Both hardware and software are developed for Coast Radio Station (CRS) facilities that serve GMDSS radio solutions. As technology and technique continues to develop IT and OT systems onboard GMDSS oceangoing ships and CRS terminals are being networked together and more frequently connected to the Internet.

Figure 5. GMDSS Server – Source: Kenta

The GMDSS operator consoles installed in the CRS terminals are an advanced GMDSS shore station console providing features and networking capabilities to meet the complex challenges of today's fast paced maritime environment. These operator consoles of CRS terminals are integrated with a TransOceana software application that runs on the Windows Operating System (OS), which are used to receive and transmit DSC messages, send and receive Narrow Band Direct Printing (NBDP) traffic, send and receive NAVTEX traffic, provide radio control over various radiotelephone equipment, monitor various hardware assets and separately support all VHF and MF/HF transmission solutions. The console software can run on an industrial rack mount computers (PC), a desktop PC or a laptop. Multiple operation consoles can run on the same PC if required.

4.2 *Server Software Solutions in GMDSS Coast Radio Terminals*

The GMDSS server solutions are special software based applications acting as a central point for any GMDSS network. As a key component of the GMDSS network, the GMDSS server is specially designed for 24/24 hours and 7/7 days operations. Thus, in order to warranty such robustness, many key points are continuously considered since preliminary design such as: (1) Robust and modular software design; (2) Detailed logging of every operation (regular and abnormal); (3) Strict checking of every inputs (configuration and Data); (4) External User interface based on a Web Server; and (5) Redundancy and backup considered since first design.

Therefore, the special GMDSS server software infrastructure used in coast radio terminals is structured on a robust software-based stream routing matrix able to route both input streams coming for example from receivers or operator consoles and output streams going to transmitters or operator consoles, which server is shown in Figure 5. The routing matrix may be configured such a way to feed Voice/DSC/NAVTEX/NBDP Encoders/Decoders and also operator console with any stream depending on the needs. Symmetrically, the routing matrix is also able to feed back any stream to any transmitters or transceivers.

In addition, the GMDSS server is fully integrated inside a 19" - 4U rack with hot-swappable dual power supplies from 100/240 VAC - 50/60Hz, a Redundant Array of Independent Disks (RAID 1) system (hot swappable disks on front panel) and the possibility to change the Air Filter on the front panel for an easy maintenance on site. This server has basic LED indicators available on the front panel for Fan monitoring, Temperature monitoring, Power indication and hard disk activity. The GMDSS Server works under Windows 10 operating system (license included).

The GMDSS server in CES terminal uses Graphical User Interface (GUI) for system setup, monitoring and maintenance available through user friendly HTML pages (Web remote control), and it provides multiple management tools for the following solutions: (1) Network architecture management; (2) Network supervision and monitoring management; (3) DSC, NAVTEX and NBDP Database messages editor; (4) Voice, DSC and NAVTEX system scheduling management; (5) DSC and NAVTEX system history log; (6) MMSI database management;

(7) User database management; (8) Public Switched Telephone Network (PSTN) and Private Branch Exchange (PBX) system management; and voice recorder and DSC archiver.

The GMDSS Server for software solutions in CES can handle several remote transmit and receive stations in MF, HF or VHF different products and third party using an IP based network topology. For voice radio transmission, the traffic through the server in CES terminal uses VoIP with SIP format (ED137B).

4.3 *Radio VoIP Software Solutions in GMDSS Coast Radio Terminals*

The Voice over Internet Protocols (VoIP) operator console is a software-based solution connected to the GMDSS server in CES maritime terminals, which can be located in the same PC as the console or in a separate PC depending on the application. The VoIP operator console is providing: (1) Suitable for simplex or complex radio communications systems whatever the used frequency bands (VHF, MF, HF etc), (2) Suitable for GMDSS CES applications; (3) Suitable for Vessel Traffic Service (VTS) or Coastal surveillance applications; (4) Suitable for seaport authorities; and (5) Suitable for off-shore platforms operators and for river authorities.

The VoIP Operator Console main features friendly and ergonomic touch screen graphical user interface, VoIP based with Session Initiation Protocol (SIP) ED137B compliant, phone

conference setup possibility and DSC console in option. These CES radio consoles also can provide mufti sites, multi radios, multi users possibilities, and radio remote control and monitoring suitable frequencies for MF, HF or VHF radios.

The Voice over IP (VoIP) Operator Console in CES terminal is supplied with a PC Workstation, Windows 10, a 22'' - 16/9 flat touch screens, a headset and a footswitch (PTT), otherwise, other accessories such as loudspeakers or microphones can be supplied as options.

4.4 *Radio DSC Software Solutions in GMDSS Coast Radio Terminals*

The DSC Operator Console (OC) is a Web-based software solution connected to the GMDSS server in CES terminal, which can be located in the dedicated computer (PC) as the console or in a separate PC depending on the appropriate application. The radio software is suitable for simple or complex radio communication systems whatever the frequency bands (MF, HF, VHF etc.), for shore CES GMDSS applications, for VTS or coastal surveillance applications, for seaport authorities, inside waters and for off-shore platforms operators.

The functions of the DSC software are as follows: Friendly and ergonomic Web graphical user interface, The console can receive and send DSC messages; Distress alert, emergency, security and routine messages; Messages history and logging MMSI database management; Multi sites and users access; Radio remote control and monitoring suitable for VHF, MF or HF stations. The DSC is supplied with a PC Workstation with Windows 10/11 and a suitable flat color screen, with optional printer and other PC accessories.

4.5 *Radio NAVTEX Software Solutions in GMDSS Coast Radio Terminals*

The NAVTEX Operator Console is a Web-based software solution connected to the CESGMDSS Server, which can be located in the same PC as the Console or in a separate PC depending on the application. The NAVTEX Operator Console is suitable for MSI broadcast in MF (490 and 518 kHz) and HF (4,209.5kHz); for GMDSS (Coast Guards) applications; and for VTS or Coastal Surveillance applications.

The NAVTEX OC main features are: friendly and ergonomic Web-based graphical user interface; messages database editing and transmitting scheduler; messages history and logging; multi sites, multi radios and multi users possibilities; and radio remote control and monitoring suitable for MF and HF radio stations. The NAVTEX OC is also supplied with a PC (computer) Workstation with Windows 10 OS and a corresponding flat color screen, with optional printer and other PC accessories, (TransOceana, 2018; Kenta, 2018).

5 SOFTWARE SOLUTIONS IN GMDSS COAST SATELLITE TERMINALS

When the Coast Earth Station (CES) receives a signal from either the satellite or terrestrial telecommunication network and Internet, it need to be transformed into understandable data and repackaged in order for it to be transmitted out through the next network. This job will be supported by the different software programs installed on modems and hardware in the land earth station.

The required hardware, firmware and software solutions delivered as part of the satellite communications network at CES terminals shall be field proven and at the most current and new revision level. All modifications and changes necessary to meet this requirement shall be completed prior to the start of the factory tests or under special circumstances, on written approval by owner, prior to the completion of SES terminal.

1. General Software and Firmware Requirements – Due to various alternative and technical design approaches in each CES terminal, it is neither intended nor possible to specify all software and firmware characteristics. At this point, it is the intent herein to provide design boundaries and guidelines that help to ensure a demonstrated, integrated software program package that is maintainable and meets both hardware systems requirements and the customer's operational requirements.
2. Operating System Software – Operating system software, such as Windows and others, shall be provided to control the execution of system programs, application programs, and management devices, to allocate system resources, and manage communications among the system processors in hypothetical CES terminal. In this way, the contractor shall make no modifications to the Original Equipment Manufacturer (OEM) operating system, except as provided as user installation parameters.
3. Applications Software – All applications software for use in CES terminals shall be written in a high-level programming language unless certain developed using industry proven application programs and development tools provided with the system. The contractor shall make no

modifications to the applications program except as provided as user development tools.

4. Software Utilities – An utility for CES terminal shall be provided to convert all reports into standard PC application formats, such as Database, Drawing eXchange Format (DXF), Excel, ASCII etc. as applicable.

Therefore, maritime CES terminals in GMDSS satellite communication service can use Ground Station Software (GSS) to provide the following solutions: (1) Command and Control Software; (2) Central Communication Controller Software; (3) Telecommand Subsystem Software; and (4) Network Interface Software.

When the CES terminal receives a signal from SES terminals, it interfaces these signals to the terrestrial network and Internet via satellite network. This signal needs to be transformed into understandable data and repackaged to be forwarded to terrestrial users. Each maritime CES terminal is operated and controlled with a suitable desktop computer to perform all functions related to receiving and transmitting messages and their printing.

Therefore, an external computer is usually competed with its own keyboard, screen, hard disk/diskette drive and printer. This computer may be used to format and store messages, and also to run specialized software, for example formatting the data into a data report for sending to a reporting centre, or compressing input data to save transmission time. Ideally, the computer with suitable software should be dedicated solely to operating the CES terminals, which can support all service received from SES terminals regarding GMDSS.

6 SOFTWARE SOLUTIONS IN GMDSS COSPAS-SARSAT GROUND TERMINALS

The Local User Terminal (LUT), such as LEOLUT, MEOLUT and GEOLUT stations in the Cospas-Sarsat network must be able to operate fully in all weather conditions that can be expected at the EPIRB location for Search and Rescue (SAR) operations of ships in distress. The Mission Control Centre (MCC) stations around the world are connected to LUT stations and should be fully compatible with MCC software functionality to allow distress data fusion requirements.

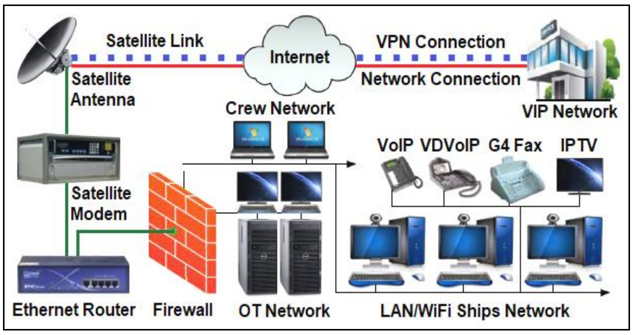


Figure 6. Shipborne LAN Onboard Network – Source: Ilcev

This software compatibility is required to allow the merging of LEOSAR, MEOSAR and GEOSAR distress data by the Operator Control Console (OCC) 600 of Honeywell and display on a single computer monitor. The terrestrial MCC stations supported by certain software must be also able to monitor, control, and receive alarms from the LEOLUT, MEOLUT and GEOLUT equipment.

Based on a Windows OS service-oriented architecture, the OCC 600 terminal provides a full suite of tools that have been designed to automate distress SAR alert data distribution to RCC stations for fast and efficient SAR operations. The adequate software features an easy-to-use graphical user interface for accurate and intuitive visualization of each distress incident. The OCC 600 satisfies all Cospas-Sarsat requirements for automatic data processing at an MCC and is commissionable according to it standards for both national and nodal MCC stations. The In-Service Support (ISS) system requirements may include items such as equipment sustainment support including middle life engineering analysis, maintenance, configuration management, the provision of spares and spares management, and program upgrades to the latest LEOLUT, MEOLUT and GEOLUT software release.

All member countries of the Cospas-Sarsat service and mission have LEOLUT, MEOLUT and GEOLUT monitoring the LEOSAR, MEOSAR and GEOSAR satellites which have proprietary software that allow the LUT to maintain a database of interfering signals which is sent to its associated MC stations. Each participating country uses the interference data bases from its LUT startion to prepare a Monthly 406 MHz Interference Report for ITU regulations, which an example of the report format can be found in Annex 2.

7 CYBERSECURITY SYSTEMS IN GMDSS SAFETY MANAGEMENT

All types of oceangoing ships in the GMDSS network are increasingly using systems that rely on digitization, integration, software and automation, which calls for cyber risk management onboard. As systems continues to develop, Information Technology (IT) and Operational Technology (OT) onboard ships are being networked together and more frequently connected to the Internet via ships communication systems.

This brings the greater risk of unauthorized access or malicious attacks to ships' systems and networks, which LAN onboard network is illustrated in Figure 6. Malicious attacks on the ship's LAN may occur on the crew or passenger network, the OT network and in particular on the ship's business LAN administration. Risks may also occur from personnel accessing systems onboard, for example by introducing malware via removable media and connecting hardware to the Internet.

The ships safety in the GMDSS network, environmental and commercial consequences of not being prepared for a cyber-incident may be significant. In fact, responding to the increased cyber threat, a group of international shipping organizations, with support from a wide range of stakeholders (please refer to annex 4 for more details), have developed these guidelines, which are designed to assist companies develop resilient approaches to cyber security onboard ships.

Approach to cyber security will be company and ship-specific, but should be guided by appropriate standards and the requirements of relevant national regulations. The guidelines provide a risk-based approach to identifying and responding to cyber threats. An important aspect is that relevant ship personnel should have training in identifying the typical modus operandi of cyber attacks.

In accordance with chapter 8 of the ISPS Code, the ship is obliged to conduct a security assessment, which should include all operations that are important to protect. Thus, the assessment should address radio and telecommunication systems, including computer systems and networks (part B, paragraph 8.3 of the ISPS Code). This calls for controlling and monitoring "the ship to shore" path of the internet connection, which is important owing to the fast adoption of sophisticated and digitalized onboard OT systems that in many cases have not been designed to be cyber resilient.

The objective of the company's Safety Management System (SMS) is to provide a safe working environment by establishing appropriate safe practices and procedures based on an assessment of all identified risks to the ship, onboard personnel and the environment. In the context of ship operations, cyber incidents are anticipated to result in physical effects and potential safety and/or pollution incidents. This means that the company needs to assess risks arising from the use of IT and OT onboard ships and establish appropriate safeguards against cyber incidents. The SMS solutions should include instructions and procedures to ensure the safe operation of ships and protection of the environment in compliance with relevant international and flag state legislation. These instructions and procedures should consider risks arising from the use of IT and OT on board, as appropriate, taking into account applicable codes, guidelines and recommended standards.

The IMO office has developed guidelines that provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. In fact, the IMO guidelines on cyber security onboard ships are aligned with the IMO guidelines and provide practical recommendations on maritime cyber risk management covering both cyber security and cyber safety. The aim of this document is to offer guidance to shipowners and operators on how to assess their operations and put in place the necessary procedures and actions to maintain the security of cyber systems onboard their ships. The guidelines are not intended to provide a basis for and should not be interpreted as calling for auditing or vetting the individual approach to cyber security taken by companies and ships.

Company plans and procedures for cyber risk management should be complementary to the existing security and safety risk management requirements contained in the International Safety Management (ISM) Code2 and ISPS Code3. Cyber security should be considered at all levels of the company, from senior management ashore to onboard personnel, as an inherent part of the safety and security culture necessary for the safe and efficient operation of the GMDSS ships.

Availability of Internet connectivity via satellite and/or other wireless communication can drastically increase the vulnerability of GMDSS ships. Namely, the existing cyber defense mechanisms onboard ships implemented by the IT service provider should be carefully considered but should not be solely relied upon to secure every shipboard systems and data. Ships are becoming more and more integrated with shoreside operations because digital communication is being used to conduct business, manage operations, and stay in touch with head office. However, vulnerable systems, equipment and technologies for assessing their exposure to cyber risk may include: Communication systems, Software operating systems, Threats against IT and OT systems Bridge systems, Propulsion and machinery management and power control systems, Access control systems, Cargo management systems, Crew and passenger servicing and management systems.

Further, critical GMDSS ships onboard communication systems have been increasingly digitalized and connected to the Internet to perform a wide variety of legitimate functions such as: (1) Obsolete and unsupported operating systems; (2) Outdated or missing antivirus software and protection from malware; (3) Inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords; (4) Ineffective network management which is not based on the principle of least privilege, shipboard computer networks, which lack boundary protection measures and segmentation of networks; (5) Safety critical equipment or systems always connected with the shore side; and (6) Inadequate access controls for third parties including contractors and service providers.

Protection measures should be implemented in a way that maintains the system's integrity during normal operations as well as during a cyber incident. Every network onboard ship has several endpoints such as workstations, servers, routers, input and output modules, transducers etc. The endpoints are very important as they control the operation and the security of the system. A secure running environment can be established by using a testing environment isolated from networks and computers, which provides additional protection against cyber threats by isolating executable software from the underlying operating system. This prevents unauthorized access to the operating systems, on which the software is running. The sandbox enables software to be run under a specific set of rules and this adds control over processes and computer resources. Therefore, the sandbox system helps prevent malicious, malfunctioning, or untrusted software from affecting the rest of the system.

8 CONCLUSION

The GMDSS network is the largest space (radio and satellite) network in the world and the only network that offers true SAR operations and save lifes and property at sea. Uniquely, enhanced GMDSS network cover the entire Earth, including the poles, and provide safety, security and emergency communications between oceangoing ships and EPIRB devices with CES and LUT terminals. All radio and satellite systems, devices and Cybersecurity Systems described above will provide the further modernization of GMDS networks and devices.

REFERENCES

[01] Sandvine, TCP Accelerator, Sandvine Communications, San Jose, CA, USA, 2019.

[02] Ilcev D. S., Global Mobile Satellite Communications for Maritime, Land and Aeronautical Applications, Volume 2, Applications, Springer, Boston, USA, 2017.

[03] Bimco, The Guidelines on Cyber Security Onboard Ships, Bimco Co., Copenhagen, Denmark. 2020.

[04] Lee J. at al, Network Integrated Transparent TCP Accelerator, 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, WA, Australia, 2010.

[05] Rohde & Schwarz, Browser in the Box – Terminal Server, Munich, Germany, 2021.

[06] DBS, Guidelines on Maritime Cyber Risk Management, Dromon Bureau of Shipping, Limassol, Cyprus, 2018.

[07] DND, Medium Earth Orbit Search and Rescue (MEOSAR) Project Ground Segment, Department of National Defence, Ottawa, Canada, 2020.

[08] Anglo-Eastern Group, The uidelines on Cyber Security Onboard Ships, Cruise Lines International Association, Cyberkeel, International Group of P & I Clubs, SOFTimpact Ltd. Hong Kong, China, 2020.

[09] Ilcev D.S. Global Maritime Radio and Satellite CNS Systems, CNS Systems, Durban, South Africa, 2019.

[10] Rohde & Schwarz, (), Trusted VPN Client - Cybersecurity, Munich, Germany, 2019.

[11] Ilcev M., New Aspects for Modernization Global Maritime Distress and Safety System (GMDSS), TransNav, Vol. 14, No 4, Gdynia, Poland, pp. 991-998, 2020.

[12] Inmarsat, Maritime Emergency and Safety Service, London, UK, 2008.

[13] ITU-R, NAVDAT Guidelines, ITU, Geneva, Switzerland, 2019.

[14] ITU-R, Technical Characteristics for a VHF Data Exchange System (VDES) in the VHF Maritime Mobile Band, ITU, Geneva, Switzerland, 2015.

[15] Kenta, DSC Operator Console, Kenta Natutel Company, Ergué-Gabéric, France, 2019.

[16] Kenta, GMDSS Server, Kenta Natutel Company, Ergué-Gabéric, France, 2021.

[17] Kenta, NAVTEX Operator Console, Kenta Natutel Company, Ergué-Gabéric, France, 2018.

[18] Kenta, VoIP Operator Console, Kenta Natutel Company, Ergué-Gabéric, France, 2020.

[19] Trans Oceana, DSC Encoder, Transoceana, Auckland, New Zealand, 2020.

[20] Trans Oceana, DSC Map Function, Transoceana, Auckland, New Zealand, 2021.

[21] Trans Oceana, DSC Software Solutions on Radio GMDSS Networks, Auckland, New Zealand, 2015.

[22] Trans Oceana, GMDSS Operator Console, Transoceana, Auckland, New Zealand, 2019.

[23] Trans Oceana, NAVTEX, Transoceana, Auckland, New Zealand, 2018.

[24] Trans Oceana, Software Solutions on Radio GMDSS Networks, Auckland, New Zealand, 2017.

[25] Trans Oceana, VoIP Software Solutions, Auckland, New Zealand, 2016.