Design challenges and decisions for a new ship data network

Ørnulf Jan RØDSETH
Research Director
MARINTEK Dept. Maritime Transport Systems
OrnulfJan.Rodseth@marintek.sintef.no

Morten Jagd CHRISTENSEN
Software Technology Manager
Thrane & Thrane A/S
MJC@thrane.com

Kwangil LEE
Electronics and Telecommunication Research Institute (ETRI), Daejeon, R. O. Korea
leeki@etri.re.kr

Acknowledgements: The IEC 61162-450 (LWE) standard has been jointly developed by several members of IEC TC80/WG6 of which the authors of this paper were only three. Part of the funding for this work was supplied through the Flagship project, Contract number TIP5-CT-2006-031406 under the 6th Framework R&D Program in EU. This research was also supported by the ICT Standardization program of MKE (The Ministry of Knowledge Economy) in Korea.

Abstract

Ship operations have characteristics that in part have accelerated development of certain types of technology while hindering other developments. One example of the latter is tools for open integration of ship control systems. New developments in legislation have made it necessary to look closer at improved system integration tools such as data networks. This is part of the background for the new IEC 61162-450 standard on ship data networks that has recently been published by the International Electrotechnical Commission (IEC). This is an Ethernet based network specification with a relatively low level of protocol complexity, hence its nick-name “Light-Weight Ethernet” (LWE). LWE is a result of a trade-off between technology complexity and specific requirements from the ship equipment industry. This paper will look at where this standard fits in a typical integrated ship control system, some of the decisions that were made during the development of this standard and how these relate to some constraints of the ship equipment industry.

1 A brief history of data networks on ships

The most important standard that has been developed for ship systems interconnection is arguably NMEA 0183, with version 1.5 being the first with wider acceptance in the international shipping business [1]. NMEA 0183 is based on transmission over RS 232 (later RS 422) serial lines with one talker and up to 10 listeners. Data is transmitted as 7 bit ASCII text sentences at up to 82 characters including various formatting information. In 1995, NMEA 0183 was transliterated into the international standard IEC 61162-1 [2].

One of the first ship data network standards published was the US Navy’s SAFENET (Survivable Adaptable Fiber optic Embedded Network) standards I and II [3]. These used IEEE 802.5 fiber optic token ring for version I and FDDI (Fiber Distributed Data Interface) for version II. Both had double fiber rings for redundancy. The transport layer used XTP [4] for transport and MAP [5] as application layer protocol. These standards were complex and expensive to implement and did not get any significant use outside the US Navy. ATOMOS was a later project that also used a token ring based transport layer, although ATOMOS selected ARCNET [6]. ATOMOS was developed through a series of European research projects and was intended to eventually be an open specification. This never happened.

SAFENET and ATOMOS both used token passing on the data link layer. The main reason for this was to get better real time performance, particularly by having more deterministic latency

from the network. It became more and more obvious from 1990 and onwards that Ethernet would be the physical network technology of choice. This was accompanied by developments on higher level protocols where the Internet Protocols (IP) became predominant. Also, higher speeds and switched Ethernet has made the latency argument less relevant.

MiTS (Maritime Information Technology Standard) was developed as a Norwegian research project in the period 1991 to 1993. It used a single, non-redundant Ethernet on the physical layer and the IP protocols, mainly TCP/IP up to the transport layer. A specific companion standard specification was used for application level interfaces [7]. In the period 1993 to 1996 several projects deployed the MiTS protocol on a number of ships and the specification as well as software was offered to the general ship control community.

Uptake of MiTS was slow, in part because of no standard support for redundancy. A new European project called PISCIS running from 1998 to 2000 to solve this problem. It resulted in specifications and prototype software for a fully redundant network system based on dual Ethernets and the IP protocols. The specifications were taken up by IEC TC80/WG6 and were developed into the IEC 61162-400 series of standards [8]. However, also this standard failed to get any significant market penetration. The reasons for this mainly being that no profession software was available and that the standard was too complex for inhouse development.

On another branch of the developments, NMEA published its NMEA 2000 standard in 2001 [9]. It is based on the Controller Area Network (CAN) standard [10] and with a capacity of 250 kbps it is mainly intended for real-time instrument and controller integration. Currently it is widely used in leisure crafts and smaller ships. NMEA 2000 supports both a single bus (Class 1) and a redundant bus solution (Class 2). This standard was also adopted as IEC 61162-3 [11]. Another similar initiative was taken by CAN Open to develop a standard for ship engines control [12]. This seems to be in common use, but not finally adopted as a standard.

2 New developments

The slow developments in integration technology on ships have many reasons as will be discussed later. One obvious reason is that there have been no really compelling technical reasons to adopt one. This is changing with developments in international legislation.

- The introduction of the Voyage Data Recorder (VDR) on ships in 2002 necessitated new data acquisition methods for storage of data in the VDR. An example is the latest radar standard that allows the radar to send images to the VDR via Ethernet and TCP/IP.

- Also the introduction of the Automatic Identification System (AIS) in 2003 increased the integration requirements. An AIS requires several serial line interfaces to cover data input and output requirements. This is awkward without bus type systems.
- The Integrated Navigation Systems (INS) performance standard requires INS equipment to interface to a Central Alert Management (CAM) system. This requires bidirectional communication that is not directly supported by the older standards.

More general technical developments are also pushing developments in the direction of more integrated systems, but not necessarily based on international standards. Virtually all manufacturers of bridge equipment have their own proprietary network solutions, normally based on Ethernet, that are able to handle many of the integration requirements. However, standards are needed for efficient interfacing between different manufacturers' equipment and will also be beneficial where incremental improvement or refurbishment of navigation components is an issue.

In 2007 Sweden proposed the new work item 80/506/NP to the IEC on an Ethernet based interface standard. This proposal was accepted in March 2008 and work group 6 (Digital interfaces) of technical committee 80 (Maritime navigation and radiocommunication equipment and systems) of IEC went to work on the development of the standard. The final standard was published in April 2011 and issued as IEC 61162-450 [13]. It is popularly called Light Weight Ethernet (LWE) as one of the design goals was ease of implementation.

3 Integrated ship control - ISC

3.1 A ship network architecture

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 monitoring and control etc. Different manufacturers produce the different systems and general differences in requirements to each sub-system make it difficult to find one common standard for the networks used in the different parts of the ship. An example of layered ship network architecture is shown in Figure 1, with a schematic representation of the network types on each layer and some example applications. The architecture is divided into the following layers:

1. *Instrument layer* interconnects various sensors and actuators to the higher level components that are using them. IEC 61162-1 belongs in this category.
2. *Process layer* interconnects components associated with a specific control function on the ship, e.g., navigation, cargo and engine control etc. LWE is in this category.
3. *Integrated Ship Control (ISC) layer* is mainly an interconnection system between the process segments. MiTS and IEC 61162-4 belong on this layer and LWE may be used.
4. *Ship layer* contains other networks on the ship. Normally there is an administrative network for the ship office, but there may also be crew and passenger services available.
5. *Off ship layer* is networks on shore, usually connected to the ship via satellite. This often includes the owner or operator with secure data links to the ship, e.g., through a Virtual Private Network (VPN).

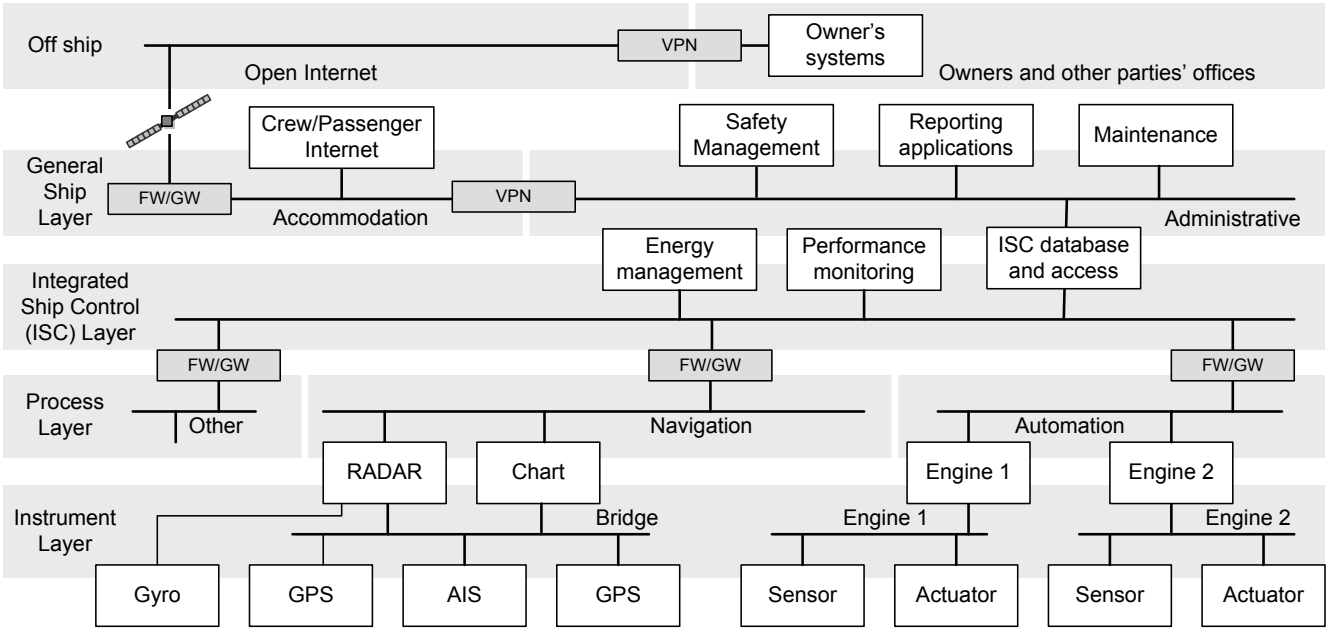

Figure 1 – Schematic Ship network architecture

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).

3.2 The place for IEC 61162-450

The IEC 61162-450 standard has mainly been developed as an instrument or process layer network. It is primarily intended for navigation and radiocommunication equipment. Some specific requirements that have to be satisfied by the protocol implementation are:

1. It needs to be suitable for embedded computers (e.g., AIS or VHF receivers) as well as workstations (e.g., ECDIS or integrated bridge consoles).
2. It should provide a simple migration path from the use of existing interface standards to the new specification. The existing standard is generally IEC 61162-1.
3. It needs to be able to handle network traffic corresponding to a complete bridge system, with high speed sensors as well as high volume data transfers.
4. It should also be able to operate as an ISC network to connect equipment on different parts of the ship. This may require cable distances of up to 1000m.

These requirements are revisited in Table 1 in section 5.

3.3 T-profile and A-profile

The LWE design used the concept of dividing the Open System Interconnect (OSI) [14] stack into two main profiles for respectively data transport (T) and application interface (A). This concept is illustrated in Figure 2.

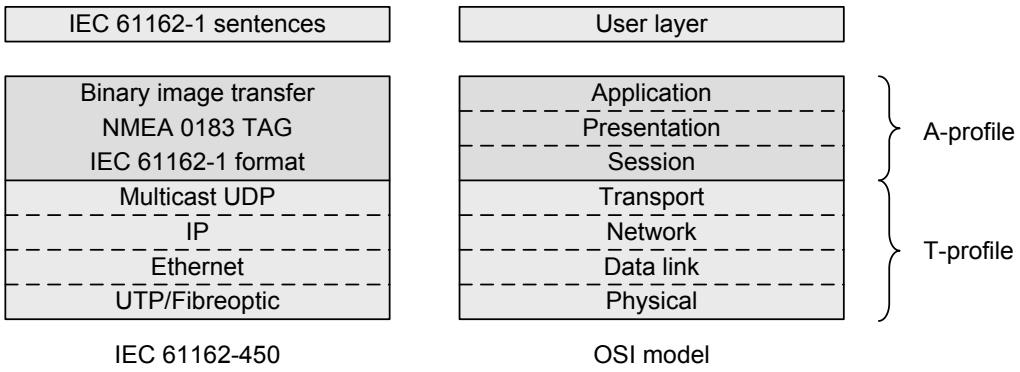

Figure 2 – T- and A-profiles with corresponding OSI protocol layers

The figure also shows the specific relationship between the layers of LWE and the OSI model. The user layer represents the specific information that is transmitted over the A-profile.

3.4 Different data transport patterns

Most data transmissions are susceptible to bit errors due, e.g., to high energy ambient noise or aging electrical connections. Data loss may also occur due to trade-offs in the protocol implementation, e.g., the Internet UDP protocol does not guarantee delivery and allows network devices to drop messages to handle congestion and buffer overflow.

The use of non-reliable protocols like Ethernet and UDP has consequences for the design of new network protocols.

For the purpose of ship data networks, four general patterns for data transmissions have been identified and included in the new standard:

- *Sensor broadcast message (SBM):* These are typically measurements or data from radio navigation systems that are transmitted as a short message to a number of receivers. Each measurement can be used independently of previous measurements.
- *Multi-Sentence Message (MSM):* A combinations of different data that needs to be used together to get the correct context and which may require more than one transmission unit to be transferred in full. An MSM is independent of previously transmitted MSMs.
- *Binary Image Transfer (BIT):* A transmission of a large general data image (electronic chart update, radar image or an update of a program file) that requires many transmission units to transfer, typically on the order of 100 units or more.
- *Command-Response Pair (CRP)*: These are command messages that require a response message from the equipment they are sent to, e.g., an alarm and its acknowledgement.

Each of these patterns has their own requirements regarding data loss and how that should be handled. Generally, demands get stricter from top and down.

4 Challenges of ship data networks

4.1 Complex systems

Ships are essentially “floating villages” with a full complement of life support systems in addition to power generation and distribution, propulsion, navigation and other systems. IEC 61162-1 defines about 50 talker identifiers for individual types of navigation and radio-communication equipment alone. Another report [15] identifies about 130 different functions onboard the ship, most of them associated with some form of computerized equipment that performs supervision and control related to that function. A data network standard must be able to support many different systems and support easy interconnection of these.

4.2 KISS

Deep sea shipping can include voyages of 20 days or more at sea. All systems need to be maintainable and to some degree repairable without access to specialists. This normally

mean that one applies the KISS principle – Keep it Simple, Stupid – in most systems. For critical networks it means that there is a strong resistance against using advanced and to some degree unproven technology. It should be possible to detect, understand and repair most faults without use of complex monitoring and analysis equipment.

4.3 Long lifetime

Ships have a design life time of between 25 and 35 years or even longer. Although electronic systems need to be updated at regular intervals, these intervals tend to be much longer than on shore. Major refurbishments tend to be done during dry dockings and the period between these can be more than 5 years in some cases. Thus, solutions on ships should be based on proven technology that has an expected further life time of up towards ten years. This will normally limit the choices for new standards.

4.4 Conservatism

Shipping is a very competitive business and is to a large degree controlled by uniform international legislation that applies equally to all ships, independent of trade and flag. This legislation is generally prescriptive and conservative. This increases the preference for proven technology. Any new developments must satisfy existing and emerging regulations.

4.5 Flexibility

In spite of conservative legislation, ship equipment and systems do evolve. New interface standards must allow a great deal of flexibility. This is in particular the case regarding what functionality that is integrated in one equipment unit. A new standard must be flexible with respect to what kind of equipment it is used in and how that equipment is configured.

4.6 Equipment focus

Standards in the shipping industry are very often based on individual equipment performance standards. There are very few system standards: The main SOLAS regulation is Ch. 5, Regulation 15: Principles relating to bridge design, design and arrangement of navigational systems and equipment and bridge procedures. This has recently been supported by a new guideline [16]. The performance standard on Integrated Navigation Systems [17] also has some requirements for technical solutions that will apply to integrated bridges. Integration on the ship is to a large degree dependent on the assumption that all equipment satisfy their

relevant standards and that the standards have sufficient provisions for interoperability. This also applies to the data network standard.

4.7 No system integrator

An effect of the equipment focus is that one rarely has a system integrator. The assumption is that all equipment works directly “out of the box” with minimal configuration. This means that any new network specification must support some form of “plug and play” functionality.

4.8 Low cost

The shipping industry is very mature and cost conscious. New functionality will not be paid for unless it has well described and obvious benefits. Also, complexity of equipment varies from relatively simple sensors to integrated bridge consoles. A new standard must be simple enough to run on embedded computers and should add minimal cost to the equipment.

4.9 Continuous availability

Ships require that many systems must be available continuously. If the power generation or maneuvering system fails during a critical operation, the result can be a severe accident. Ships traditionally implement a strategy by which no single failure shall be able to disable a critical system. This must also be supported by the data network.

4.10 Security

Data networks are critical part of critical ship safety systems. It must not be possible for unauthorized persons to influence on the systems. Traditionally, this has been done by physically isolating the network from areas where it can be accessed by non authorized persons. However, in new development where one wants more integration between ship systems and even may want to access the network from shore, this problem needs to be addressed. A new standard must address the security of the network itself, of functions implemented over the network and of the equipment connected to it.

5 Design solutions

The main design challenges as outlined in the previous sections are summarized in the below table. The table also lists the corresponding solutions selected for LWE.

Table 1 – Cross reference between requirement and solution

Challenge	Solution

Challenge		Solution	
3.2	Different transport patterns	5.7	Specify additional patterns
3.2	Embedded support	5.1-5.3	Ethernet and IPV4 UDP
3.2	Migration path	5.4, 5.6	IEC 61162-1 A-profile. gateway
3.2, 3.4	Capacity and latency	5.1, 5.3	Switched Ethernet and UDP
3.2	Length requirements	5.1	Allow fibre optic cable.
3.1, 4.1	Diverse systems	5.1, 5.2	Internet protocols
4.9	Continuous availability	5.8-5.10	Diverse structure/error detection
4.2-4.5, 4.8	Simple and low cost, flexible	5.1-5.5	Simple modular structure
4.6, 4.7	No system integrator	5.11	Equipment focus

5.1 Ethernet with switches

Ethernet is supported on all types of equipment including single-chip computers. It is low cost, well understood and easy to install. Copper as well as optical fiber can be used. However, LWE has limited its specification to only allow the use of level 2 switches:

1. Hubs, i.e., level 1 repeaters without message buffering, are not allowed. This is because the use of hubs severely decreases the capacity of the network as discussed in 6.
2. Switches with higher than level 2 functionality, i.e., multicast snooping, or routers with Internet address translation functionality are not allowed. The reason for this is to avoid effects of the use of multicast management protocols as discussed in 7.

Note that the specification does not disallow the use of routers and other special equipment to connect one IEC 61162-450 network to other systems. However, this has safety and security implications that need to be analyzed carefully (see section 5.9).

5.2 Internet Protocol Version 4 - IPV4

IPV4 was selected for IEC 61162-450 as IPV6 would add considerable complexity and cost with little additional benefit. The depletion of IPV4 address space, the main driver for IPV6, is of no practical consequence for a ship automation network: For safety and security reasons it would not in any case be connected directly to the Internet (see section 3.1). Other features of IPV6, such as quality of service control, could be useful in a ship automation network, but it would require the use of relatively costly network infrastructure equipment that may also be difficult to acquire and maintain for safety critical systems such as a ship bridge. A final issue is also that developers and crew lack operational experience with IPV6.

5.3 UDP Multicast

The IEC 61162-1 standard is a single talker broadcast system, message oriented, connection-less and do not guarantee delivery. This paradigm was also selected for LWE as it simplified migration and simplified the software implementation. A broadcast mechanism also reduces overall network traffic as most messages are intended for more than one listener. The message length is limited to 1472 bytes (the maximum size of the UDP payload in a single Ethernet frame) to avoid potential problems with incorrect fragmentation and assembly of IP multicast messages. This also reduces need for buffering on embedded computers.

Table 2 – Node filtering levels

OSI level	Filtering methods	Node level
1 – Physical	Not used (need level 3 switch)	
2 – Link layer	MAC address filtering (Ethernet multicast groups)	HW
3 – Network layer	IP multicast groups	Network SW
4 – Transport layer	UDP ports	Network SW
5-7 – A-profile	Header multiplexing and message parsing	Application SW

IP multicast was selected rather than IP broadcast although both support UDP. The reason for this was to allow efficient message filtering for *nodes* on the network. As only level 2 switches are allowed (see section 5.2), the switches will flood all messages to all nodes on a network. Node level filtering can occur at various OSI layers and, correspondingly, on different hardware or software layers in the receiving node as shown in Table 2. The lowest level for filtering is at the Link layer where most Ethernet controllers today have hardware assisted Ethernet multicast address filters. The LWE standard use 65 multicast addresses for current and future systems. Different UDP port numbers are allocated to each multicast address which allows for message filtering in network drivers for those computers that do not support hardware filtering. Further filtering must be done on application level.

5.4 IEC 61162-1 as A-profile

LWE has adopted the IEC 61162-1 A-profile with some modifications to support system concepts such as redundancy, sender/receiver identification and error detection:

- Added “Transport Annotate and Group” (TAG) functionality from NMEA 0183 to allow additional attributes to be added to the basic IEC 61162-1 sentences.
- System Function Identifier (SFI) gives each logical function (possibly several on each node) a system unique ID. This is a mandatory TAG attribute to all outgoing messages.

- Required use of, e.g., grouping and destination TAG's to support MSM and CPR message patterns as well as a TAG attribute for line count and error detection.

Using the IEC 61162-1 specification makes integration of old and new equipment much easier. It also provides equipment interface specifications through existing standards.

5.5 A function block approach

The standard is designed as a set of partly independent requirement sets to different types of functions that can co-reside in one piece of equipment. This simplifies type approval of equipment, independent of what combinations of functions it contains. The function block requirements also include a minimum requirements "Other Network Function Block" that can be used to test equipment that co-resides on the same network, without using the LWE protocol. This may, e.g., be a storage device or a printer.

5.6 Including a gateway specification

The new standard also includes requirements for the design of a serial gateway network function that can be used to interface legacy IEC 61162-1 equipment to LWE. This specification is an important component in ensuring easy migration from old systems to new as well as for providing a standard interface to existing serial line interfaced equipment. An LWE based system can be built from the first day – more or less based on existing and already type approved components.

5.7 Additional transport patterns

The standard A-profile based on IEC 61162-1 provides the SBM transport pattern directly (see 3.3). Safe transmissions with the multiple message pattern (MSM) is supported through a required TAG grouping of related sentences (see 5.4). The binary image transfer (BIT) pattern has specific support through a separate transport mechanisms for binary images. The specification includes rudimentary and optional retransmission support as well as some mechanisms for limiting bandwidth use. The Command Response Pair (CRP) pattern is supported through a required procedure for transmission of CSR classified sentences. With this, the protocol will be able to support most common data exchange patterns, but it is primarily designed to carry connection-less and broadcast type messages.

5.8 Support for redundancy

Implementation of “no single point of failure” requires some form of redundancy in system components and interconnections. Several possibilities exist to achieve this, from adding some additional serial lines to a fully duplicated set of components and data networks. As it is not possible to easily select one “best” way to implement redundancy, it was decided to leave this to the system integrator.

However, a number of features were included in the specification to support the task of providing a redundant interconnection system:

- A unique SFI (System Function Block Identifier) must be assigned to all functions in the LWE network. This will distinguish between two function blocks with same functionality.
- An IP address must be statically assigned to each network node on an LWE network. This provides a mechanism to set up an identification regime for functions and network nodes.
- An informal annex outlines some possibilities for redundancy implementations and issues that should be taken into account for the different solutions.

5.9 Security support

There is no direct functionality to support security functions in the network standard. However, the specification contains an informal annex outlining some of the issues one needs to consider and pointing out some possible solutions.

5.10 Error detection and reporting

For the “no single point of failure” principle to work it is also necessary that the error is detected and repaired as soon as possible. LWE requires that several network related errors are logged. This includes buffer overflow as well as format and checksum errors. Errors can be logged internally in equipment, but it is recommended to use the Syslog protocol [19] to send error reports to one or more logging nodes on the network. The Syslog protocol is also supported by many switches and other network equipment.

5.11 Equipment focus

Most of the new standard specification is written to address individual equipment and is aimed at making it possible to approve equipment for use in an LWE network system, without requiring additional tests for the network itself. There is little need for configuration except for

setting an IP address for each equipment and an SFI for each function block. These functions may be automated, but the IDs are required to stay constant after commissioning. In addition, the standard contains documentation requirements that enable an overall system load analysis to be performed. One also needs to perform a system wide safety and security analysis, e.g., FMEA (Failure Mode and Effects Analysis) to ensure that no single point of failures exists. Thus, there is a need for a system integrator, but this is on a relatively high level and can be taken on by the yard or one of the major equipment manufacturers.

6 Capacity analysis

This section gives some results for a simulation of high network loads. For the network analysis, simulation analysis was performed using OPNET 14.5 PL8.

Table 3 – Types of connected equipment for simulation

Type	# of Units	Msg/sec.	Msg size
DEVA	15	1	79-200
DEVB	15	50	79-200
DEVC	15	50	79
DEVD	15	1	79
MISC1	10	1	79
MISC2	10	1	79
BG	0 ~ 9	32	50000

Table 3 lists the types of devices used in the simulation. The DEVA to DEVD devices represent navigation and radiocommunication equipment with different transmission characteristics. This would typically be GPS or AIS receivers, Radar tracks or other similar equipment. The MISC devices are other types of equipment on the network acting as receivers and also generating some traffic. The BG row represents background traffic from high load sources. The table lists how many units were used in the simulation, messages sent per second and message sizes. More information on background traffic is given in the specific sections. In the simulation, both a 128 port hub and a layer 2 switch were used in a single star topology. The performance of each was then compared under equal traffic loads. Simulations were done both with multicast and broadcast traffic. As expected, the simulation showed only marginal differences between multicast and broadcast, typically less than 0.5% of values. These differences are due to artifacts from the stochastic nature of the simulations. Thus, only results from multicast simulations are included here.

6.1 Hubs versus switches

In the first analysis, shown in Table 3 and Table 4, the performance of the switch and hub with different background traffic were analysed. The background traffic was adjusted to between 30% and 90% of the link speed (100Mbps). Packet loss rate and average delay were measured. In the experiments, the switch capacity is set to 36,000 packages per second (pps). Packet loss occurs for the hub when background traffic reaches 30%. After that loss increases gradually. Note that loss is much higher for units with low repetition rates. The switch suffers no data loss at all, but at the cost of increased and significant delay. This is caused by the buffering done in the switch.

Table 4 – Packet loss rate (%) – Hub versus switch

Background traffics (Mbps)		**30**	**40**	**50**	**60**	**70**	**80**	**90**
Hub Multicast	DEVA	12.8	18.6	23.4	28.3	34.2	41.6	46.0
	DEVB	1.1	1.5	2.1	2.5	3.1	3.8	4.6
	DEVC	1.1	1.4	2.0	2.5	3.1	3.8	4.5
	DEVD	13.0	17.9	22.0	29.0	34.3	39.3	46.9
Switch Multicast	DEVA	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	DEVB	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	DEVC	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	DEVD	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Table 5 – Average delay (ms) – Hub versus witch

Background traffics (Mbps)		**30**	**40**	**50**	**60**	**70**	**80**	**90**
Hub Multicast	DEVA	1.1	1.2	1.2	1.5	1.5	2.0	2.3
	DEVB	4.0	5.2	7.1	9.1	11.3	13.8	16.9
	DEVC	4.0	5.0	6.9	8.6	11.0	13.3	16.4
	DEVD	1.1	1.2	1.3	1.4	1.7	1.9	2.3
Switch Multicast	DEVA			91.3	150.7	223.9	311.0	412.0
	DEVB			96.1	155.7	229.1	316.0	419.5
	DEVC			95.9	155.5	228.9	315.8	419.3
	DEVD			90.9	150.4	223.5	310.6	411.7

6.2 Switch capacity

Table 6 lists the simulated network performance as a function of the switch capacity. Packet size is 64 bytes. This result was obtained with a background traffic load of 90%.

For the example topology, the minimum capacity of the switch should be 36 000 packages per second. As shown in the table, the queue size, delay and packet drop is reduced as the switch capacity is increased. Many switches claim much higher performance than 36 000 pps and increasing switch capacity will obviously improve performance. However, this also increases the cost for the switch. The switch should be selected based on the traffic and performance requirements in a ship network design phase.

Table 6 – Network performance as function of switch capacity

Switch Capacity (Packet/s)	**6k**	**12k**	**18k**	**24k**	**30k**	**36k**	**42k**	**48k**	**54k**
Queue size (kilobytes)	1573	1624	1611	1595	1539	115	97	84	30
Queue size (packets)	9916	10087	9963	9842	9467	705	595	515	182
Queue Delay (sec)	40.00	20.18	13.35	9.86	7.63	0.48	0.40	0.35	0.12
Avg. Packet Drop (per sec)	6008	4762	3517	2271	1025	0	0	0	0

7 Use of multicast snooping or routers

LWE makes use multicast to distribute information in the network. IP Multicast normally uses the IGMP (Internet Group Management Protocol) for dynamic notification to multicast routers about listeners in the network. This section discusses some potential problem related to the use of IGMP. The configuration is shown in Figure 3, where the right-most figure is the one used in following diagrams and where the shaded boxes are IGMP enabled. Two transmitters and two talkers communicate, where both listeners are assumed to listen both for talker A and B messages. One of each type of device is not IGMP enabled, i.e., cannot send or process IGMP messages.

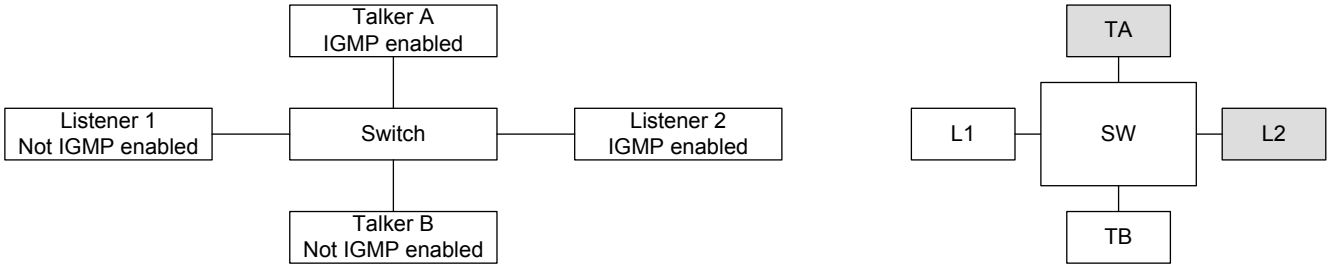

Figure 3 – IGMP registration with dumb switch

7.1 Start up of system

When transmission of data starts, there are two scenarios to consider dependent on the switch being able to process IGMP (IGMP Switch) or not ("Dumb" Switch). The IGMP protocol is dependent on sending and receiving join messages for setting up a proper forwarding scheme and the two switches process these messages differently.

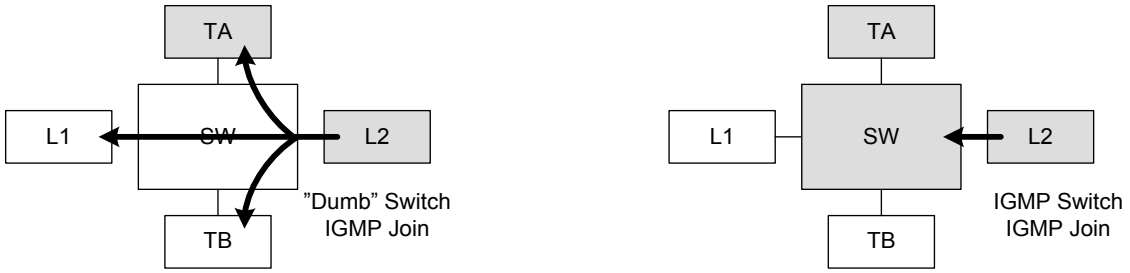

Figure 4 – Start up

If the switch is "Dumb" it will automatically flood the network with the join messages which are subsequently ignored. The IGMP enabled switch will absorb and process the join messages and use them to set up routing tables. Only L2 sends the join as L1 is not IGMP enabled.

7.2 Data transmission

During data transmission the talkers send their data to the switch as multicast messages. The "Dumb" switch will flood all multicasts to all ports and devices. All receivers get all data, independently of being IGMP enabled or not. The IGMP enabled switch will only send the multicast messages to the receivers that have subscribed to them.

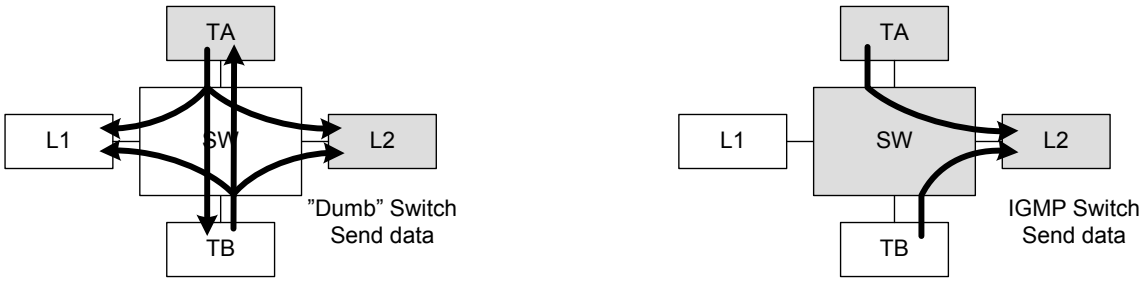

Figure 5 – Data transmission

This shows the benefit of using IGMP snooping: There is a very significant reduction in network traffic and node load. The drawback is that all listening devices must be IGMP enabled or they will not get the expected data. The general rules that control snooping and transmission is described in RFC4541 [18]. The rules may, despite being best current practices, make IGMP snooping switches, with snooping enabled, fail in some circumstances:

1. When there is a mix of IGMP capable and not capable devices.
2. In a short period after a power cycle where forwarding tables are being reconstructed.
3. Special combinations of IGMP versions in hosts, routers and switches.

To solve this problem there are some possible solutions:

1. Require all devices to implement IGMP version 3 and include exhaustive tests to make sure that it works correctly.
2. Use the 224.0.0.X multicast address range which inhibits IGMP filtering. This is not recommended by the standards and will have the same effect as solution three below.
3. Require use of “dumb” switches that always forward multicast to all ports (flooding). There is no state which must be reconstructed after a power cycle.
4. Allow IGMP snooping switches but require disabling of snooping for these. This has the same effect as solution 3.

The proposed solution is that “dumb” Ethernet switches are used. This is the most robust and also the cheapest solution. Although this solution gives a significantly higher network load, the load analysis shows that this can be accommodated. A more significant problem may be load on individual, particularly simpler embedded devices, but this can be alliviated by use of hardware filtering on multicast addresses as discussed in 5.3.

8 Future outlook and conclusions

This paper has described some of the history related to integrated data networks on ships, some of the special considerations that need to be taken when designing new network standards and how these considerations influenced the design of the LWE standard.

The argument for the new standard was that the older serial line based IEC 61162-1 standard has some important shortcomings that needed to be addressed:

- Separate cables are needed for each individual talker and maximum fan-out is limited to 10. This significantly increases cabling for modern integrated bridges.
- Two-way communication, e.g., for alarm management, requires double set of cables for each pair of equipment. This makes for even more complex cabling.
- IEC 61162-1 does not allow transfer of high volume data.

Bridge systems with, e.g., new central alert management module and increased integration, will be more common in the future. This requires more capacity on protocol level as well as better transport mechanisms and patterns. It can be argued that the capabilities of LWE is a necessary prerequisite for the introduction of improved and more advanced bridge systems.

There are several possible new developments that could be done in the existing IEC 61162-450 standard. Some of these were discussed during the development phase, but was dropped due to the need to keep the specification and implementation as simple as possible:

- An even higher focus on the semantic level with better specifications for how to use the mechanisms and capabilities available in LWE.
- Further developments of standard solutions for redundant and fault tolerant system implementations.
- Additional functionality for network management, fault detection and performance monitoring, including time synchronization and improved error reporting.
- An additional connection oriented communication mechanism, e.g., based on TCP/IP. This can be used in more complex communication patterns.
- Improved and standardized security support, e.g., for remote monitoring and maintenance of systems on board.

There are also other possible items on the “to do” list for future developers. However, users of ship technology are relatively conservative and not very willing to accept complexity that is not deemed absolutely necessary. On the other hand, there will certainly be a need for more system complexity in the future and this may increase the demand for better support also at the protocol level.

References

[1] NMEA 0183 (1987) Standard for Interfacing Marine Electronic Navigational Devices, version 1.5, National Marine Electronics Association, 5 December 1987.

[2] IEC 61162-1 Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 1: Single talker and multiple listeners

[3] Paige J.L., Howard E.A. (1990), SAFENET II-The Navy's FDDI-Based Computer Network Standard, Proceedings of SPIE OE/Fibers 1990, V. 1364, September 1990.

[4] XTP 3.4 (1989), Xpress Transfer Protocol Definition - Revision 3.4, Protocol Engines Inc., Jul 1989.

[5] MAP (1988), Manufacturing Automation Protocol Specification - Version 3.0, North American MAP/TOP Users Group, Aug 1988.

[6] ARCNET Local Area Network Standard (1992), ATA/ANSI 878.1. Technical report. ARCNET Trade Association.

[7] Rødseth Ø.J., Haaland E. (1993), “MITS: An Open Standard for Integrated Ship Control”, proceedings of ICMES ‘93, Hamburg September 1993

[8] IEC 61162-400 series (400, 401, 402, 410, 420: 2001) Maritime Navigation and radiocommunication equipment and systems - Digital interfaces: Multiple Talker and Multiple Listeners - Ship Systems Interconnection.

[9] Luft L. A., Anderson L., Cassidy F. (2002). NMEA 2000 A Digital Interface for the 21st Century, Institute of Navigation’s 2002 National Technical Meeting, San Diego, CA.

[10] ISO 11898-1:2003 Road vehicles -- Controller area network (CAN). All parts.

[11] IEC 61162-3 ed1.0:2008 Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 3: Serial data instrument network

[12] Etschberger, K., Schlegel C., Schnelle O., Wiulsrød B. (2003). CANopen Maritime – A New Standard for Highly Dependable Communication Systems, 9th international CAN Conference, iCC 2003, Munich.

[13] IEC 61162-450 Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 450: Multiple talkers and multiple listeners - Ethernet interconnection.

[14] ISO/IEC 7498-1:1994, Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model

[15] Flagship deliverable D-B4.3 (2009), Modes of operations, EU Project Number TIP5-CT-2006-031406, Issued 2009-12-31, Version 2.0 – Public.

[16] IMO SN.1/Circ.288, 2 June 2010, Guidelines for Bridge Equipment and Systems, Their Arrangement and Integration (BES).

[17] IMO RESOLUTION MSC.252(83), adopted on 8 October 2007, Adoption of the Revised Performance Standards for Integrated Navigation Systems (INS)

[18] RFC4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

[19] ISOC RFC 5424, The Syslog Protocol. Internet Society Standard.