



Project contract number: **TIP5-CT-2006-031406**

FLAGSHIP

European Framework for Safe, Efficient and Environmentally-friendly Ship Operations

Instrument type: IP

Specific programme: **Sustainable Surface Transport**

D-C1.4 Interface standards

Start date of project: 2007-01-01

Due date: 2008-12-31

Duration of project: 48 months

Actual delivery date: 2009-02-12

Lead contractor: Autronica Fire and Security AS

Revision: 1.0

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	Confidential

Document summary information**Authors and contributors**

Initials	Author	Organisation	Role
ØJR	Ørnulf Jan Rødseth	MARINTEK	Editor
ÅT	Åsmund Tjora	MARINTEK	Contributor

Revision history

Rev.	Who	Date	Comment
0.1	ØJR	2008-08-26	First outline of TOC
0.2	ÅT	2009-01-15	Filled in with functions and demonstration needs
0.3	ØJR/ÅT	2009-01-23	Content review and additional details
0.4	ÅT	2009-01-30	Added material on bus solutions
1.0	ØJR	2009-02-04	Final version

Quality Control

	Who	Date
Checked by lead partner	Ørnulf Jan Rødseth, MTEK	
Checked by SP	Per Norman Oma, AFS	
Checked by internal reviewer	Julian Stephens, MJC2	

Company internal coding (if any)

Main responsible	Internal reference number

Disclaimer

The content of the publication herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the FLAGSHIP consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the FLAGSHIP Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the FLAGSHIP Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Executive summary

This document contains requirements and specifications for the necessary interfaces of the ISEMS system described in the Flagship C1 subproject. The work focuses mainly on the use of ISEMS on passenger ships; however the use on merchant ships is also briefly discussed.

Several varieties of ISEMS for passenger ships are shown, with discussion on both physical and functional setup.

The document also contains specifications for a demonstration setup for the ISEMS as well as the prognosis tools discussed in the Flagship C2 subproject. Both the physical topology of the demonstration system as well as the functions to demonstrate and the needed specifications to protocols are shown.

State of the art and need for improvements

There are no standard interfaces for such systems today and this work is required, minimum for doing the Flagship demonstration, but more generally for assessing the possibilities for standardising such interfaces, particularly for third parties, such as search and rescue centres and third party analysis providers.

The potential impact of the results

The main target for this report is the actual Flagship demonstration, but some of the results in this deliverable can be used as basis for published interface standards.

However, the work has shown that interfaces based on standard HTTP/HTML data transfers seems to be best for general parties that are not normally part of the information sharing loop (e.g., search and rescue) and that proprietary protocols may be required for more integrated parties. Thus, there is less potential in general standardisation than originally suspected.

Contributions to the work

Most of this report has been written by MARINTEK with contributions from Autronica and Lodic. Other partners in the sub-project have contributed by commenting and suggesting new contents.

List of abbreviations

- C1 – Sub-project C1 of Flagship (The sub-project responsible for this deliverable)
- CAM – Centralized Alert Management system (developed in subproject B4)
- HTTP – Hypertext Transfer Protocol
- IMO – International Maritime Organization (www.imo.org).
- IP (communication) – Internet Protocol
- IP (enclosure) – International Protection Rating (IEC 60529 standard, specifying the protection against intrusion of objects, dust and water in electrical enclosures)
- ISEMS – Integrated Safety and Emergency System
- ROPAX – RORO Passenger ship (typically car and passenger ferry)
- RORO – Roll On, Roll Off ship
- SAR – Search and Rescue (Organization)
- SOLAS – International Convention for Safety of Life at Sea (IMO convention)
- SSL – Secure Sockets Layer (cryptographic protocol, predecessor of TLS)
- TLS – Transport Layer Security (cryptographic protocol, successor of SSL)
- VSAT – Very Small Aperture Terminal (for satellite communication – commercial system).

Table of contents

1. Introduction	7
1.1 Scope	7
1.2 Overview of previous work.....	7
1.3 Potential benefit of this work	7
1.4 Structure of document	7
2. Functionality of Flagship ISEMS	8
2.1 Overview of functionality	8
2.2 Functions to be shown in the demonstration.....	9
2.2.1 Using the system for training	9
2.2.2 Mobile station.....	10
2.2.3 Communication with shore	10
3. ISEMS physical design	10
3.1 Full ISEMS – Safe return to port	11
3.2 Ship only – no wireless	12
3.3 Ship and shore – no wireless	12
3.4 Demonstration system	13
3.4.1 Overview	13
3.4.2 On-shore ISEMS demonstration	14
3.4.3 Ship demonstration.....	15
3.4.4 Prognosis system.....	16
3.4.5 Third party demonstrator.....	16
4. Requirements to ISEMS interfaces	16
4.1 Internally in ISEMS onboard	17
4.2 ISEMS wireless onboard.....	17
4.3 ISEMS to other systems onboard.....	18
4.3.1 Navigation systems	18
4.3.2 Other systems	18
4.4 ISEMS onboard to shore	19
4.5 ISEMS shore to prognosis.....	19
4.6 ISEMS shore to third party.....	19
4.7 ISEMS to technical maintenance	20
5. Specifications for ISEMS interfaces.....	20
5.1 Internally in ISEMS onboard	20
5.2 ISEMS to other systems onboard	20
5.2.1 Navigation systems	20
5.2.2 Other systems	21
5.3 ISEMS wireless onboard.....	21
5.4 ISEMS onboard to shore	21

5.5 ISEMS shore to prognosis..... 22

5.6 ISEMS shore to third party..... 22

5.7 ISEMS to technical maintenance 22

6. Demonstration specification..... 22

6.1 System topology 23

6.2 Equipment 23

7. ISEMS for merchant ships..... 24

7.1 General 24

7.2 Possible merchant ship ISEMS 24

7.3 Demonstration 25

8. References 25

1. Introduction

1.1 Scope

This document is the final specification of the C1 subproject ISEMS (Integrated Emergency and Safety Management System) demonstration. As part of that, it will also contain the interface specifications for the systems.

During the C1 work, it has become clear that the main application for an ISEMS is on passenger ships. This document will focus on that application area, but will also outline an ISEMS for general merchant ships. It is expected that subproject C2 will look into some of the demonstration aspects of this type of ship. Thus, this deliverable contains the following information:

- A high level functional specification of the ISEMS system for a passenger ship.
- A system diagram for an ISEMS with links to shore and to onboard wireless networks.
- Interface specifications for communication within the ISEMS and between the ISEMS and other external systems. This also includes the maintenance system interfaces.
- A specification for the C1 demonstration, including necessary modifications to systems.
- An outline of an ISEMS for a merchant ship.

Note that the C1 demonstration system also will include prognosis functions from C2. The specification for the interfaces and topology is contained herein.

1.2 Overview of previous work

This work represents a continuation of the work performed in the Flagship subproject C1. In C1.1 assessments of emergencies have been performed, in C1.2 functions and requirements are specified, and in C1.3 a cost/benefit analysis for an ISEMS system is performed. The C1.3 deliverable also contains descriptions of the functions that may be used in an ISEMS. The demonstration system described in this deliverable will also use a prognosis system described in subproject C2. Requirements to on-board networks and protocols are discussed in subproject D1.

1.3 Potential benefit of this work

While the requirements and specifications to the interfaces in this work will not be very detailed, the most important requirements for the ISEMS interfaces are listed. This will serve as an input to other of the Flagship subprojects, e.g. subproject D1. It will also serve as an indication of what kind of equipment is necessary for implementing an ISEMS.

Also, this document will describe how the demonstration system will be set up, with descriptions of equipment, communication links and protocols. The demonstration description will give an indication on how an actual system may be designed.

1.4 Structure of document

The rest of the document is structured as follows:

In section 2 the functionality of the Flagship ISEMS system is summarized, with focus on the functions that are to be demonstrated in the Flagship demonstration.

Section 3 reviews the physical setup of an ISEMS system, and discusses the setup that shall be used in the Flagship demonstration.

In section 4 the requirements for the communication interfaces used by ISEMS are discussed.

Section 5 contains the specifications for the communication interfaces used by a generic ISEMS.

Section 6 contains the specifications for the system used in the Flagship ISEMS demonstration.

Section 7 contains a brief description on how an ISEMS system for a merchant ship will be set up.

2. Functionality of Flagship ISEMS

2.1 Overview of functionality

The functions that were discussed in the cost benefit analysis [D-C1.3] have been listed in the table below, and a number of ISEMS system classes have been defined by specifying what functions to include. The classes listed are:

- Conv.: A conventional on-ship ISEMS with typical functionality as of today. This indicates a state of the art system that currently is found only on the largest passenger ships.
- Shore: An ISEMS that communicates with an on-shore facility. This is not generally available today and represents one of the possible results of the Flagship contributions.
- Demo: The functions of the demonstration system.

A full ISEMS system will include all functions as specified and possibly more. A real ISEMS will in most cases not be directly covered by the specified classes.

Function	Conv.	Shore	Demo
General status overview functions			
Fire safety plan / general damage control plan	X	X	X
ISM checklists	X		X
Electronic plotting table (EPT)	X		X
CCTV control and display	X	X	
Fire management	X	X	X
Fire detection and indication	X	X	X
Smoke spread and heat			
Fire door and damper monitoring and control	X	X	X
Dangerous goods location			

Evacuation support and situation assessment			
Passengers needing assistance and searched areas			X
Muster status			X
Smoke extraction status and control	X	X	X
Evacuation control – directional evacuation signs			
Stability and strength			
Indication of watertight and shell doors	X	X	X
Water ingress and tank levels			
Stability			
Strength			
Prognosis functions			
Fire prognosis			X
Evacuation overview			X
Flooding prognosis			
Ship-shore coordination and management			
Duplication of ISEMS on shore		X	X
Ship shore messaging or chat function			
Wireless ISEMS			
Wireless ISEMS			X

This list is tentative and may be adjusted during the final phase towards the demonstration.

2.2 Functions to be shown in the demonstration

The Flagship ISEMS demonstration will show some of the most important functions and possibilities of the ISEMS system. The demonstration will target a fire scenario as that is arguably the most critical situation on a passenger ship.

The C2 demonstration is expected to be targeted at a merchant ship that does not carry passengers. The focus here will be on hull damage with resulting strength and stability problems. This is not covered in this deliverable.

2.2.1 Using the system for training

An important aspect of an ISEMS is that it can record the results of drills and real events, when such happens. Thus, there is a great potential in using the tool for debriefing and for constructing training scenarios.

This will be to some degree demonstrated as the tool will have storage and some playback functionality. However, this is not currently a major issue in the demonstration as some functionality in the tool is not sufficiently developed.

2.2.2 Mobile station

The mobile station demonstrator will show how a portable device can be used to get information from the ISEMS system to personnel on scene.

In addition to demonstrate how the mobile unit can be used, the demonstration can also be used to get important feedback on how this unit and supporting infrastructure should be set up. The size and weight of the unit, the unit's ruggedness, the user interface, how information is displayed and what information to display, as well as the wireless network infrastructure on the ship are factors that should be considered.

2.2.3 Communication with shore

The data exchange between the ship and on-shore facilities should be demonstrated. Situation data from the ship should be available at the owner's office, and data from the office, such as decision support and prognoses, should be available on the ship.

The demonstration will also show how limitations of the communication link (i.e. bandwidth limitations and delay) will affect the data exchange and the ship-shore integrated operations.

2.2.3.1 Owner's office

The on-shore owner's office demonstrator will show how the data from the ISEMS at the ship can be received and presented at the owner's office.

The use of the owner's office in integrated operations with the ship, where the owner's office provides advice, decision support, analysis results etc. to the bridge, should be shown.

The use of prognosis tools, including integration of the tools with the system and display of the prognoses in the owner's office and on the ship, should be demonstrated.

2.2.3.2 Third party station

The third party station demonstration will show how a third party using commonly available and fairly inexpensive equipment can communicate with an ISEMS system during an emergency. The needed computer and communication equipment and software should be of a kind that is commonly found at most marine rescue coordination centres all over the world as well as at specialist's offices and other parties, e.g. a simple computer and web browser setup.

3. ISEMS physical design

This chapter is to a large degree repetition from earlier deliverables, but is included here for completeness. Some additional comments have been added where appropriate.

3.1 Full ISEMS – Safe return to port

The full ISEMS system must have at least two workstations on the ship; a primary station at the bridge's safety centre and a secondary at the engine control room. The stations have the same functionality, so that if the safety centre station fails, the ECR station can function as a backup.

The networks used to connect the system nodes must have sufficient redundancy to fulfil Safe Return to Port regulations, e.g. the system must be able to function after full vertical or horizontal zone damage on the ship. Worst case will, thus, be either a full vertical fire zone damaged or a horizontal damage that extends over more than one vertical zone, which may be the case, e.g., in the engine room or on a car deck.

One or more tertiary stations may also be used, e.g. it may be desirable to have a station at the hotel section on the ship. The tertiary stations may be set up with a functionality that is reduced and reliability should be set up with a wireless infrastructure on the ship, so that the mobile stations may communicate with the main ISEMS system.

The system on the ship must be able to communicate with a system on shore (typically at the owner's office). This will require a satellite or radio link. The communication link to shore should have a high availability, and may require a redundant satellite link. Note that most passenger ships use a VSAT link for day to day operations and have an Inmarsat B or Fleet link for backup. Thus, there may be some redundancy in the connection.

The on-shore station is set up with an ISEMS that receives and displays the situation data from the ship.

A prognosis system may also be used, this system may be at the same site as the on-shore system, but it may also be at another site, e.g. as a third party service. If a prognosis system is used, the on-shore station transmits the data from the ship to the prognosis tools and receives the prognoses from the tools.

It may also be of interest to let third parties, like specialists and maritime rescue coordination centres, get information from the on-shore ISEMS system. These should be able to connect to the on-shore system using commonly available, inexpensive technologies, e.g. a computer with a web browser.

Below is shown a schematic drawing of how a general ISEMS could be organised. One would most likely design it as two independent sub-systems, e.g., on bridge and in engine. Additional workstations (tertiary) can be added so that additional command positions can be had or for additional redundancy. Tertiary stations should be connected to both primary and secondary networks to be operational in case of a major damage.

A mobile station would be connected to a wireless network. It is not at this stage clear if redundancy is required, but that would be desirable. However, this is a trade off between cost and robustness.

Shore stations would be connected to the system to trusted data links and additional parties can in principle access data through a HTML gateway to the shore office.

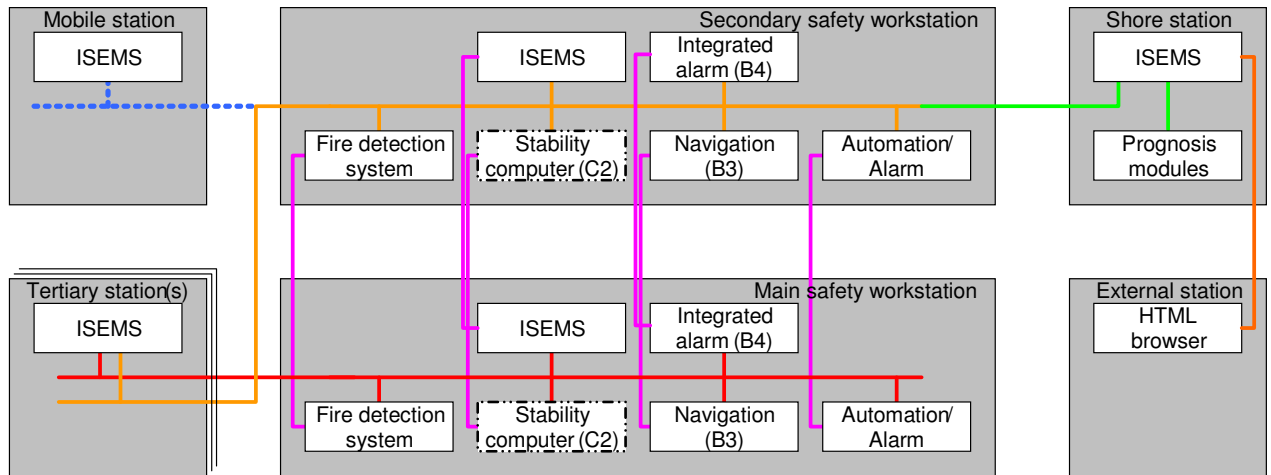


Figure 1: Full ISEMS structure

3.2 Ship only – no wireless

For a system with ISEMS only on the ship and no wireless terminals, the setup is similar to the full setup, but without the wireless infrastructure, the satellite links and the on-shore systems. The system must still fulfil the requirements to reliability, ability to function after full vertical or horizontal damage etc.

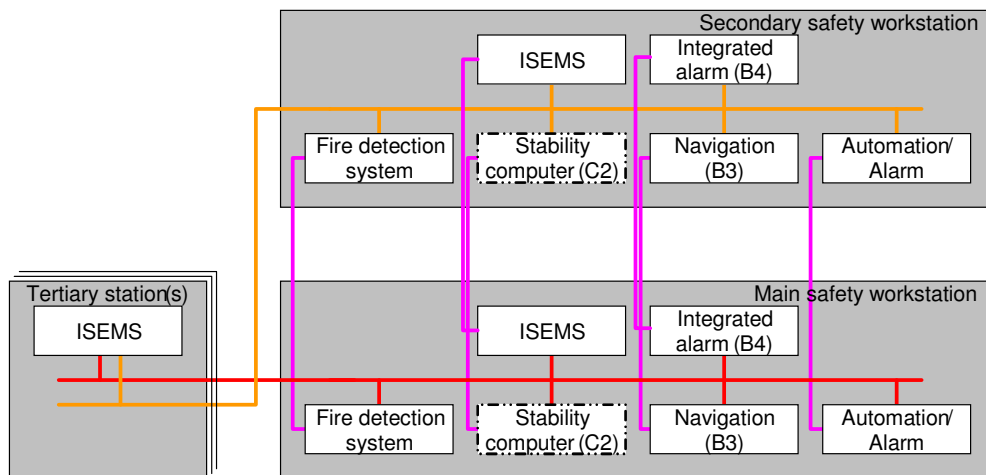


Figure 2: Ship only system

3.3 Ship and shore – no wireless

For a system with ISEMS on ship and shore, but with no wireless terminals, the setup is the same as the full setup, but without the wireless infrastructure.

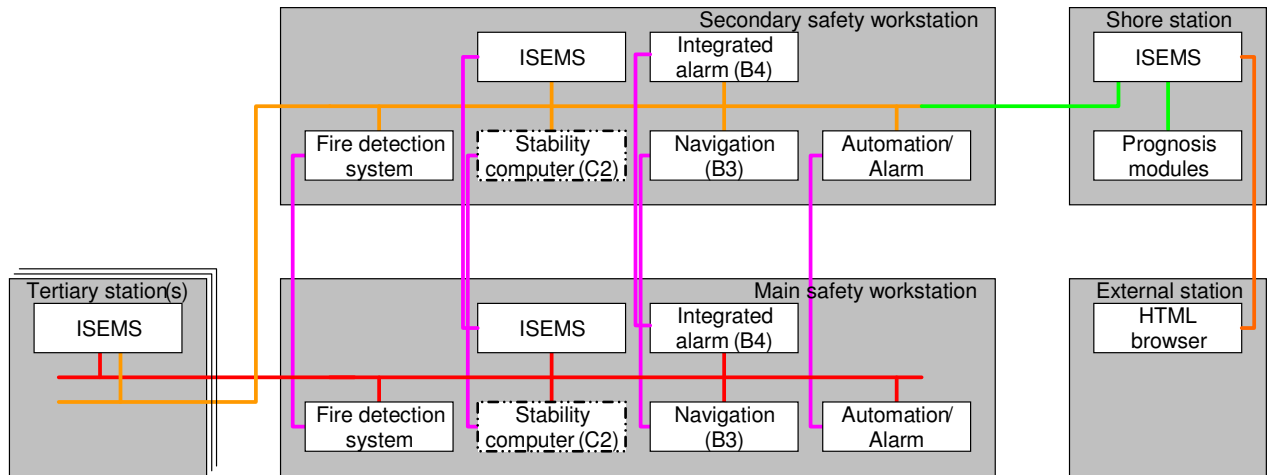


Figure 3: Ship and shore system without wireless terminal

Note that the external station is collected to the shore station and not to the ship directly. This is done to ensure control of the communication between ship and shore.

3.4 Demonstration system

The demonstration system will not be a complete ISEMS in terms of redundancy. The main point is to demonstrate functionality.

Currently, various options for demonstrations exist and the actual ship will be agreed upon between sub-projects C2 and C1.

3.4.1 Overview

The main parts and communication links of the demonstration setup are shown in figure 4. The setup consists of

- a ship with an ISEMS set up at the bridge's safety centre and a mobile station
- an owner's office demonstration running AutoMaster, communicating with the ship using a satellite connection
- the prognosis tools, communicating with the owner's office using Modbus/TCP
- an on-shore third party setup with a standard HTTP connection to the owner's office.

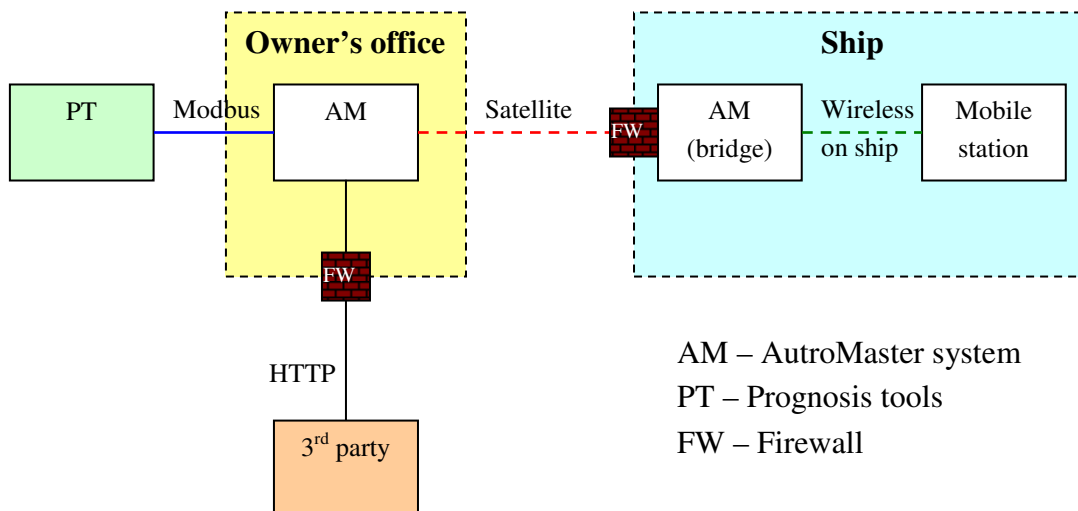


Figure 4: Demonstration setup

The firewall (FW) on the ship side may be removed if the communication is performed over a trusted link, e.g., a VPN link and with limited capacity so that the AM workstation cannot be overloaded.

3.4.2 On-shore ISEMS demonstration

The on-shore (“owner’s office”) demonstration is set up in the integrated operations room “Nautilus” at Marinteknisk Senter in Trondheim, Norway.

However, there is symmetry in this setup, so that it may be possible to run the ship demonstration also at the MARINTEK facilities, with shore facilities located somewhere else.

3.4.2.1 Screen and computer setup

The room has four high resolution (1920x1080) main screens, set up in a 2x2 array and connected to a DVI matrix.

There are six standard inputs to the DVI matrix available from the desk positions in the room. Four of these will be used for the demonstration computer setup, leaving two inputs available for laptops or other display sources¹.

The demonstration computer setup consists of two ordinary computers running AutoMaster; each computer uses two of the four main screens.

The system communicates with the prognosis tool computers, located at the University of Strathclyde, Scotland, using the Modbus/TCP protocol over the general Internet.

¹ This is the “simple” setup that will be used in the demonstrator. For a more advanced setup in a room dedicated to these kinds of operations (e.g. at a real owner’s office), the main computers running the system will typically be “built in” as a part of the room’s computer system.

In a typical setup, two screens will be used for the mimic, one screen will be used for check- or alarm lists, and the last will be used for CCTV, chat function, analysis results or for displaying other data that may be useful. The screens for the mimic may be set up horizontally (showing a larger part of a deck) or vertically (showing a larger part of a fire zone).

The screens can easily be set up to temporarily show results from other sources (e.g. other workstations or laptops used by experts in the room).

The system will use a small test network.

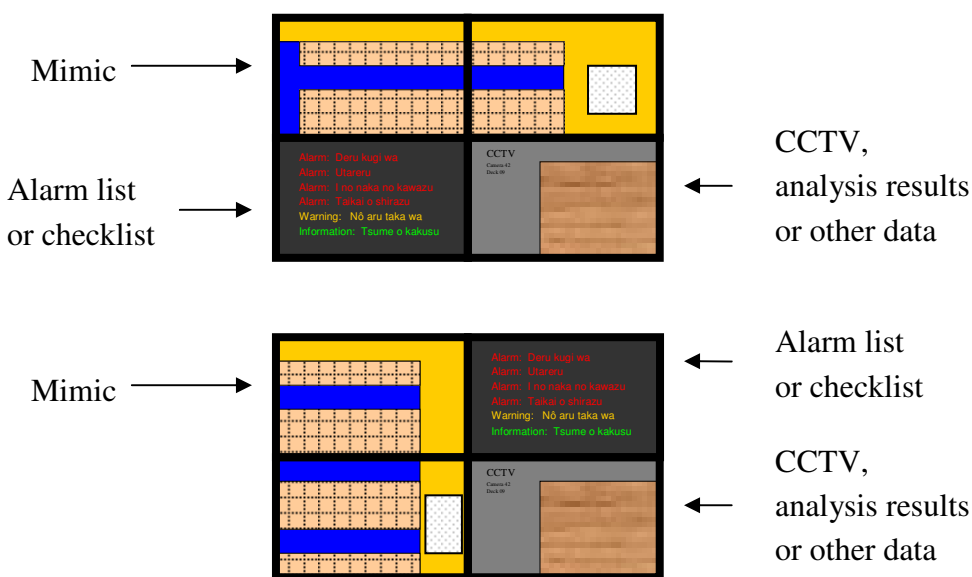


Figure 5: Two possible screen configurations on Nautilus.

The most likely screen configuration is the second (lower) one. The reason for this is that a ship incident often will have a local extent limited to one fire zone and one deck. The people responsible for handling the situation will then need to see the decks above and below as well as the fire zones aft and for of the incident. With the normal 16:9 aspect ration, this is best done with two screens stacked on top of each other.

3.4.3 Ship demonstration

The reference ship used in the demonstration will either be MF Ikarus, Color Fantasy, or Color Magic. It is also possible to use the RCCL Oasis of the Seas. The decision will depend on to what degree we can demonstrate issues on board and what data we have of the ship. All above mentioned ship have Autronica fire alarm systems and the last three of them has also been entered into the C2 prognosis tool system.

The demonstration on the ship is in principle set up with a full ISEMS at the bridge’s safety centre. In addition, a mobile station is demonstrated. The system communicates with the on-shore system using a satellite link.

However, reservations are currently made regarding the actual possibility to do much onboard. The ships are either in operation or being built and it is not quite clear how easy it is to get useful integration with the actual ship.

3.4.3.1 Primary station: Safety centre/Bridge

The primary workstation should be placed in the ship's safety centre. This station should provide full system functionality, including communication links to on-shore facilities.

3.4.3.2 Mobile station

For the mobile (on-scene) station, a small laptop or tablet PC is used in the demonstration. In a "real setting" a rugged portable device (PDA, laptop or tablet) will probably be used.

The station will be set up to display information relevant to the on-scene commander and the crew working with damage control and evacuation assistance, e.g. location of fire and smoke, location of passengers in need of help, searched areas etc.

3.4.4 Prognosis system

The prognosis system may be located outside the owner's office as a third party service. In the Flagship demonstrator, the prognosis tools will be located at the University of Strathclyde. The owner's office system will communicate with the prognosis tools using the Modbus/TCP protocol.

In future systems, one can easily imagine the prognosis tools located at the owner's office and operated by superintendents or other specialists.

3.4.5 Third party demonstrator

For the third party demonstrator, a standard computer setup should be used. The computer will communicate with the system in the owner's office using an HTTP connection.

This will demonstrate how a widespread inexpensive technology that can be assumed to be available everywhere can be used to interface with the ISEMS.

4. Requirements to ISEMS interfaces

This chapter contains the requirements to the interfaces of ISEMS. This includes requirements to the interfaces for internal communication between ISEMS stations, communication with other on-board systems and the mobile ISEMS stations, communication with the on-shore station, and communication between the on-shore station and prognosis tools and third parties.

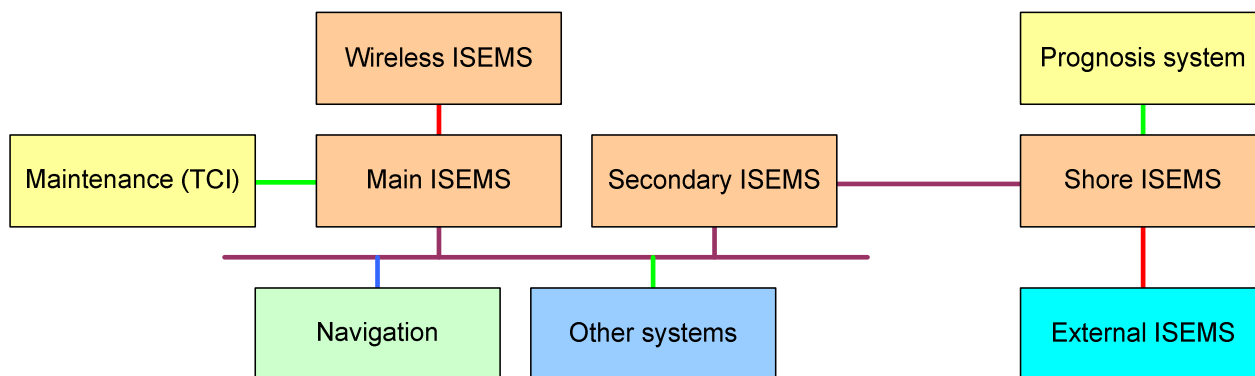


Figure 6: Interface schematics.

The above figure shows the main interfaces in the system. The following sub-sections list applicable requirements.

A more in-depth study of the requirements to on-board networks will be presented by the Flagship Subproject D1.

4.1 Internally in ISEMS onboard

The system that is used for communication between ISEMS devices and workstations on the ship must fulfil any applicable regulations, like the Fire Safety System code and the Safe Return to Port regulations.

The system must be reliable, with sufficient redundancy so that no single point failure or likely combination of failures will cause the system to fail.

The system should have availability category R0, i.e. continuous availability.

The system should be able to run on standard ship infrastructure, this will typically mean an Ethernet based system, normally with IP type protocols.

As this is the internal interface between the ISEMS components on the ship, the protocols used do not have to be open standard.

4.2 ISEMS wireless onboard

The requirements to the wireless system may differ with how the wireless terminals are used; the terminals may be used by on-scene commanders in relatively sheltered areas, but it is also possible that the damage control teams will use the terminals in areas that have hostile environments (e.g. areas filled with smoke and heat). If the terminals are to be used in hostile environments during the emergency, both the terminals and the wireless infrastructure on the ship must be built to handle this.

It may be necessary to move the unit around during the emergency. This means that a unit may be moved from an area covered by one access point to an area that is covered by another access point. It is also possible that some access points will fail during an emergency, so the unit will

have to reconnect to a working access point. This kind of handover should be as seamless as possible. This can probably be solved by using stateless communication protocols (e.g. HTTP).

The possibility of access point failure also means that there should be redundancy requirements, e.g. any area on the ship should be in range of more than one access point. The network backbone should have sufficient redundancy so the network has a high availability during emergency situations.

Requirements to the equipment may differ depending on where the equipment is placed. Some areas on the ship may have requirements to the casing of electrical equipment placed in the areas, e.g. a specific IP code stating the minimum requirements to dust and water resistance. It is important that access points and other network equipment placed in these spaces should fulfil the necessary requirements.

As there will be access points placed in public spaces on the ship, proper network security should be in place, so the system is protected from any unauthorized use.

4.3 ISEMS to other systems onboard

The ISEMS system will have to communicate with some of the other systems on the ship. It is important that this communication has sufficient security, both to avoid unauthorized (accidental or malign) access and to avoid that any problems or failures of the equipment that ISEMS communicates with propagate to the ISEMS system.

The protocols used for this communication should be open standard, allowing easy setup of communication with a wide variety of systems.

4.3.1 Navigation systems

The ISEMS will need to interface to the voyage data recorder (VDR) and possibly also to the navigation system, e.g., to fetch current position, speed and direction. In the future, the ISEMS should also consider interfaces to a central bridge alert management system.

There are no general requirements to these interfaces, but there are specific requirements, e.g., given by performance standards for various systems. This applies in particular to VDR and central alert management.

For other systems, it will mainly be a question of getting non-critical information and, hence, requirements are less severe.

4.3.2 Other systems

There is a host of other systems that the ISEMS may have to interface to. Examples are automation or stability systems for information about water ingress and the general stability (and possibly strength) situation. HVAC systems are important for fire management, system time providers, automation systems and others may also provide more or less critical information.

There may also be a need to interface to public announcement, CCTV and water tight door systems for either control or monitoring.

Some of the above systems are highly critical, e.g., PA and water tight door control, and interfaces to these need to be carefully designed to ensure adherence to rules laid down by manufacturers. However, there are no standard interface descriptions and interfaces must be designed on an ad hoc basis.

4.4 ISEMS onboard to shore

The communication with on-shore facilities should be redundant to provide the necessary availability; the system will typically use VSAT with Inmarsat C/B as backup. The communication protocols with on-shore facilities must be designed so that the bandwidth provided by the satellite solutions is sufficient, e.g. 64 kbit/s for Inmarsat B.

The communication link should be sufficiently secure, hindering any unauthorized access. It is also important that faults occurring in any of the on-shore systems do not propagate to the on-ship system.

The communication is between dedicated systems and do not have to use open standards.

Note also that communication requirements may not be very high, even in very hectic situations. A fire alarm sample may be sent in 16 bits and one may not need to support more than a few alarms per second, even when the fire is at its highest.

4.5 ISEMS shore to prognosis

The protocol for communication between the ISEMS at the owner's office and the prognosis tools should be open, allowing easier integration of tools from different vendors.

If the prognosis system is located at a third party's site, the communication link must have proper security, so unauthorized access to the systems is hindered.

The protocol also needs to be able to run over the general Internet, possibly over VPN, to allow the greatest flexibility.

4.6 ISEMS shore to third party

An important aspect of the interface to third party systems is that the third party should not need to use expensive or uncommon equipment, hardware or software at their site. Thus, a system using a well known interface without any need for special software or hardware should be used, e.g., HTTP, Java and similar technology.

The communication link should be secured so unauthorized access to the system is hindered, but it is also important that access from authorized partners is granted quickly without problems.

4.7 ISEMS to technical maintenance

The ISEMS will integrate a fire alarm system with supervision of thousands of fire detectors as well as other detectors for, e.g., fire doors or other fire fighting equipment. Thus, it would be highly useful if the system had a direct interface to a maintenance system so that technical problems could be reported directly to the engineers or electricians as well as to the officer of the watch.

This is batch data that need not be sent in real-time. Normally, it is sufficient if such data can be updated once an hour or so. Even lower update rates can be acceptable.

Data needs to contain the physical tag of the device and, if available, data on type of device. However, the latter may be available directly from the maintenance system. It is also necessary to specify type of problem and likely action to fix it, e.g., repair, cleansing or replacement.

5. Specifications for ISEMS interfaces

These specifications are mainly developed for the C1 demonstrator, but they should be useful for general ISEMS constructions both based on Flagship principles and also outside Flagship constraints.

The focus of the following descriptions is on protocol specifications.

5.1 Internally in ISEMS onboard

The protocol used internally in ISEMS is proprietary, using the ship network infrastructure for communication.

Currently, this will require the use of a dedicated fire/safety network, although D1 looks into the possibility of using a general ship network also for safety applications.

The protocols should be based on IP protocols and employ mechanisms that make it safe to use the protocol and network. This typically includes filtering mechanisms to avoid unauthorized access, heart-beat mechanisms to keep track of status of equipment, some form of connection management to provide refresh after power down etc. Again, these are general requirements that will be addressed by D1.2.

5.2 ISEMS to other systems onboard

5.2.1 Navigation systems

Navigation systems (including voyage data recorder) normally use the [IEC 61162 1/2] interface standard. This is also the most applicable standard for the ISEMS. This standard provides most required data from the navigation system and will also provide incoming interfaces to, e.g., alert management and voyage data recorder.

A new standard for Ethernet connections are under development will not be finished before later in 2009.

5.2.2 Other systems

The ISEMS will also need to interface to other systems than navigation. Mostly, there are no standards available that covers both data transport and interpretation of received data. One restriction is that interfacing occurs over serial lines or Internet networks. This normally precludes a long range of fieldbus type standards.

The Modbus protocol, either over serial line [MODBUS RTU] or TCP/IP [MODBUS IP] is fairly widely used and is one obvious alternative. There is also an ASCII variant of the serial line protocol, but that may not be so attractive here. However, this standard only transports data without giving meaning to them. Thus, all uses of this standard will require the development of a companion standard covering the meaning of exchanged data. Typically, this is done on register level, e.g., Modbus operates with a register concept where one can send a 16 bit message in each register. For fire alarms, this is normally sufficient (e.g., two bit for alarm status, 7 bit for smoke density and 7 bit for heat level).

One may also use OPC in some cases. OPC Data Access [OPC DA] is currently the most common although the Alarms and Events [OPC AE] also may be applicable. These protocols are based on Windows mechanisms and have some drawbacks related to configuration and multi-machine configurations. Also, OPC is not normally used in safety critical applications and will be mostly applicable for longer latency and less critical data.

A new development is OPC Unified Architecture [OPC UA] that offers more advanced functions as well as transport over architecture independent mechanisms, e.g., TCP/IP or HTTP. This may be an interesting alternative for future systems.

Except for these protocols, there are also a number of other more or less proprietary standards in use.

5.3 ISEMS wireless onboard

The mobile station should communicate with the ISEMS using HTTP over a standard IEEE 802.11- type Wireless LAN. Encryption schemes can be used to protect the network and the wireless communication link from unauthorized access.

The wireless unit can use proprietary protocols although it may be useful to modify the general ISEMS protocols to cater for less robust environments. One may, e.g., support roaming over several base stations and this may be simpler to do with a connection less protocol such as HTTP or UDP.

5.4 ISEMS onboard to shore

The protocols used for communication between the ship and the shore ISEMS are proprietary. The protocols used should be designed so that the restrictions to bandwidth are fulfilled.

These links are normally switched circuit and can use normal connection oriented protocols such as TCP/IP. Other IP type protocols may also be used.

It is necessary to consider backup solutions over, e.g., Inmarsat B, where bandwidth can go down to 64 kbps. Thus, one may use compression or special versions of the protocol to minimize load on the network bandwidth.

5.5 ISEMS shore to prognosis

If the prognosis system is not located at the same site as the on-shore ISEMS, the communication will typically be over the Internet. Some sort of security protocol, like TLS/SSL, VPN or similar, should be used if communication over the Internet is used. If the prognosis system is at the same site as the on-shore ISEMS, a local connection between the systems will be used.

The communication should use a standard protocol suitable for this kind of data exchange, e.g. IEC 61162, Modbus/TCP, OPC UA or similar.

For the demonstration, it has been agreed to use Modbus TCP/IP.

5.6 ISEMS shore to third party

Generic third party systems will typically be connected to the on-shore ISEMS using the Internet. Security protocols like TLS/SSL should be used. As no special hardware or software can be expected to be in place at the third party site, an open protocol usable by commonly available systems, e.g. HTTP, must be used.

5.7 ISEMS to technical maintenance

As has been specified from subproject D1, it may be useful to provide a general interface between all larger shipboard systems and the maintenance system. This is partly for transfer of technical condition indexes, but also for transfer of general maintenance and spare part requests. This is particularly important for the fire system which may be connected to 5000 or more individual detectors and sensors. On the RCCL Oasis of the Seas, there are more than 10 000 sensors and detectors with an expected life time of 10 to 15 years.

The protocols need to be open so that different maintenance systems can be interfaces. They are not directly safety critical, but it is necessary that they are reliable in the sense that data will be transferred eventually, i.e., speed is not normally an important factor, but reliability may be.

[D-D1.1] has specified the general data model for exchange of technical data that may be used in this context. However, this standard is not yet implemented so it will not be demonstrated in this sub-project.

6. Demonstration specification

This chapter contains a very brief overview of the equipment and protocols used in the demonstration setup. These specifications are derived from the requirements and protocol specifications in the previous section.

6.1 System topology

The demonstrator system network is basically a tree with the main on-ship ISEMS as the root. Note that each node in the network can consist of more than one workstation if these are integrated with proprietary networks and protocols.

The main on-ship ISEMS is connected to a mobile unit using an on-board wireless connection and to the on-shore facility using a satellite connection. The on-shore facility is further connected to the prognosis tools at a third-party site and to a generic third party observer, using Internet connections for both.

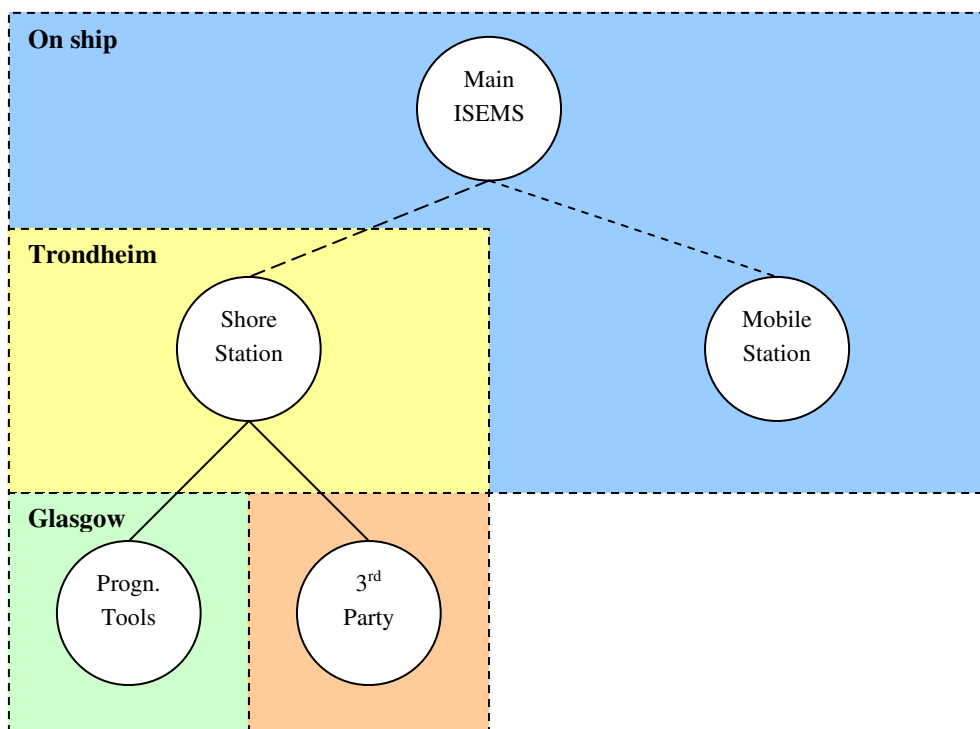


Figure 7: Communication tree for demonstration system

The protocols used between the nodes are as follows:

- Main-Mobile: Proprietary connection-less, UDP or HTTP.
- Main-Shore: proprietary connection-oriented, however, with low-bandwidth capability. Shall be able to run on 32 kbps or less.
- Shore-3rd party: HTTP over general Internet. The link will not be encrypted for our demonstration, but that would possibly be the case for a real set-up.
- Shore-prognosis: Modbus TCP/IP over open Internet. Again, encryption could be used for a real set-up.

Figure 6 gives a more complete, but somewhat more abstract picture of this with an emphasis on the identified interfaces.

6.2 Equipment

The following equipment will be used in the demonstration:

- Main: A set of AM5000™ Workstations connected together in a proprietary network. This will most likely be at Autronica premises or onboard a real ship.
- Shore: One or two AM5000™ Workstations connected together with proprietary network. If it is possible to drive four screens from one workstation, this is the preferred solution.
- Mobile: Portable tablet PC with HTML browser. May run Java.
- Third party: HTML browser on any type of PC.
- Prognosis: Special equipment provided at SSRC premises in Glasgow.

All AM5000 computers run Linux. Others may run Linux or Windows.

7. ISEMS for merchant ships

7.1 General

The merchant type ISMES have to satisfy space and cost constraints that will have a great impact on the actual functionality. Also, a typical merchant ship will only have on the order of hundred fire detectors and in general a much simpler electronics supervision system. The merchant ship will neither be required to comply with safe return to port, have crew that are familiar with the ship and safety systems and has in general another type of safety constraints. On the other hand, it will be much more susceptible to strength and stability problems, particularly strength, if it is a large bulk carrier.

Thus, a merchant ship type ISEMS will be very different from the one one will see on a passenger carrier. This issue was also discussed in [D-C1.2] and [D-C1.3], with similar arguments being made.

7.2 Possible merchant ship ISEMS

As shown in [D-C1.3], the ISEMS for a merchant ship will be simpler than that of a passenger ship. In Flagship, the graphic capabilities of the stability computer will also be used to present fire and other relevant information.

A typical ISEMS for a merchant ship is shown in the below figure. It consists of a main decision support station based on a stability computer that is connected to the fire alarm system and selected signals from the automation system. A VDR would also be connected to the system for recording of events – however, this is outside this discussion.

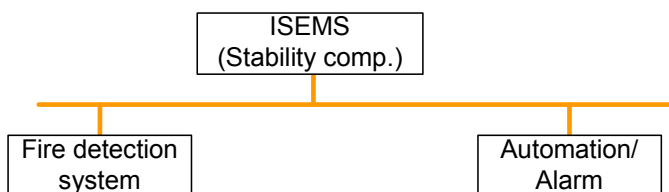


Figure 8: Simple ISEMS for merchant ships

Using the stability computer as main station is one possibility. One could also use the automation system with similar links to the stability computer. However, the stability computer does already contain drawings of ship and is in itself a decision support tool. Thus, it may make more sense to extend it rather than building a new function into the automation.

The fire alarm system is not appropriate as it is normally not screen based on small ships. It will consist of an alarm panel with a few lines of text display.

7.3 Demonstration

Sub-project C2 will address merchant ship problems and is expected to cover that in their demonstrations, possibly with an interface to the fire alarm system from C1. This has not yet been determined.

The demonstration in C1 will focus on passenger ships, but some of the analysis of cost and benefits may be applicable also to merchant ships.

8. References

[D-C1.2] Flagship – Deliverable D-C1.2: Safety Analysis for Technical Systems

[D-C1.3] Flagship – Deliverable D-C1.3: Cost/Benefit Analysis

[D-D1.1] D-D 1.1 TCI and status indicator specification, 2008-09-26.

[IEC 61162-1] IEC 61162-1, Maritime navigation and radiocommunication equipment and systems – Digital interfaces, Part 1: Single talker and multiple listeners, Third edition, 2007-04.

[IEC 61162-2] IEC 61162-2, Maritime navigation and radiocommunication equipment and systems – Digital interfaces, Part 2: Single talker and multiple listeners, high-speed transmission, First edition 1998-09.

[MODBUS IP] MODBUS Messaging on TCP/IP Implementation Guide V1.0b, Modbus-IDA - <http://www.Modbus-IDA.org>, October 24, 2006.

[MODBUS RTU] MODBUS over serial line specification and implementation guide V1.02, Modbus-IDA.ORG - Modbus.org <http://www.modbus.org/>, Dec 20, 2006.

[OPC AE] OPC AE Specification 1.10.1.00, 2002-10-02 (www.opcfoundation.org)

[OPC DA] OPC DA Specification version 3.00.1.00, 2003-03-05 (www.opcfoundation.org).

[OPC UA] OPC Unified Architecture Specification, Part 1: Overview and Concepts, Release 1.01, February 5, 2009