Grant Agreement number: 314286
Project acronym: MUNIN
Project title: Maritime Unmanned Navigation through Intelligence in Networks
Funding Scheme: SST.2012.5.2-5: E-guided vessels: the 'autonomous' ship

D4.3: Evaluation of ship to shore communication links

Due date of deliverable: 2012-12-31
Actual submission date: 2012-12-30

Start date of project: 2012-09-01 Project Duration: 36 months

Lead partner for deliverable: MARINTEK(MRTK)
Distribution date: Document revision: 1.1

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013)		
Dissemination Level		
PU	Public	**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)	

Document summary information

Deliverable	D4.3 Evaluation of ship to shore communication links
Classification	Public

Initials	Author	Organisation	Role
ØJR	Ørnulf Jan Rødseth	MARINTEK	Editor
BK	Beate Kvamstad	MARINTEK	Contributor

Rev.	Who	Date	Comment
0.1	ØJR	2012-10-26	First outline for comments
0.2	ØJR	2012-11-05	More contents
0.3	BK	2012-12-14	Quality attributes and type of systems
0.4	ØJR	2012-12-18	Distribution for internal review
1.0	ØJR	2012-12-30	Final deliverable after changes
1.1	ØJR	2014-02-07	Editorials before final publication

Internal review needed: **[X] yes** **[ ] no**

Initials	Reviewer	Approved	Not approved
HCB	Hans-Christoph Burmeister, CML	With comments	
MS	Michele Schaub, HSW	With comments	

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 MUNIN 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 MUNIN 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 MUNIN 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 report goes through some critical issues related to communication in autonomous ship systems. This includes ship to shore, internal ship and internal shore issues. The report develops general requirements to communication for unmanned ships and analyses current technology to see how it can be used to satisfy these requirements.

This evaluation shows that current technology should be able to support the necessary requirements. However, some areas of special attention are identified:

- A special rendezvous protocol for remote control of ship during crew embarkation, e.g. after communication failures, is needed. This should probably be based on AIS or Digital VHF technology.
- Protocols for low latency control of the ship may need special developments if bandwidths and packet loss rates are too high to use standard technology for guaranteed delivery like TCP/IP.
- The ship control systems should be designed to operate with different levels of communication quality. Three levels are suggested with respectively 4 Mbps, 128 kbps and low bandwidth rendezvous services.
- The ship systems must also be able to handle cases where positioning systems fail. GPS is vulnerable to jamming and spoofing.
- Special scenarios must be developed to define actions when either positioning systems or communication systems, including the rendezvous mechanisms, are lost.

A high level service layer interface is outlined for the autonomous ship control programs at the end of the report. This includes information to programs about system autonomy and communication integrity states as well as services to perform communication tasks. Details of the interfaces will be provided in deliverable D4.4.

List of abbreviations

3G, 4G	Third and Fourth generation mobile telephony systems
AIS	Automatic Identification Systems
API	Application Program Interface
ASC	Autonomous Ship Controller
BER	Bit Error Rate
BGAN	Broadband Global Area Network (Inmarsat)
DSC	Digital Selective Calling (for VHF radio)
ETSI	European Telecommunications Standards Institute
FMEA	Failure Mode Effects Analysis
FtS	Fail-to-safe
GNSS	Global Satellite Navigation System
GMDSS	Global Maritime Distress and Safety Services
IETF	Internet Engineering Task Force
ICAO	International Civil Aviation Organization
IP	Internet Protocols
ISC	Integrated Ship Control
ISM	Instrumentation, Scientific and Medical frequency bands (unlicensed)
ITS	Intelligent Transport System
ITU	International Telecommunication Union
LOS	Line Of Sight
kbps	Kilobits per second
Mbps	Megabits per second
ms	Milliseconds
MTU	Maximum Transmission Unit
NAVTEX	Small safety text messages sent via radio to ships.
QoS	Quality of service
RCU	Rendezvous Control Unit
RTCA	Radio Technical Commission for Aeronautics

RTCM	Radio Technical Commission for Maritime Services
SCC	Shore Control centre
SNR	Signal to Noise Ratio, same as S/N
TCP/IP	Transmission Control Protocol/IP
UDP	Unreliable Datagram Protocol (IP)
VHF	Very high frequency
VPN	Virtual Private Network (Protocol)
VSAT	Very Small Aperture Terminal (highly directional dish antenna)
WiMAX	Worldwide Interoperability for Microwave Access.
ZigBee	Local area personal network for ISM band use

Table of contents

1. Introduction

1.1 Scope

The purpose of this report is to evaluate existing maritime communication systems and services to see how they can be used to satisfy requirements for unmanned ship operations.

Furthermore, the report will give necessary background to the structure and mechanisms of the communication system and the corresponding model. This latter objective also implies an evaluation of available communication services.

1.2 Definitions

Latency: In this report latency is defined as the mean one-way delay from a specific byte of information is sent by sender until the same byte is received by receiver. A formal definition can be found in section 3.6.

Link budget: For a satellite transmission, the satellite operators use a certain output power which is used to overcome various damping factors related to the signal transmission through space, atmosphere, antenna, cables and electronic systems. The calculation of output power versus the various losses to be overcome is the link budget or link power budget.

Link layer: This term is used to describe issues or effects caused by the physical transmission of data messages through air or space as well as effects related to systems involved in this transmission.

Liveness: Here used to denote the ability to send messages over a connection oriented data link, i.e. that the link connection is not broken. Broken links normally occur after it has been impossible to send a message between the parties for an extended period (time out).

QoS: Quality of service (for communication). In this report, QoS is defined through a set of quality attributes defined in section 3.6.

Rendezvous: The operation of retrieving or releasing manned on-board control of an autonomous ship. This can be after a full communication failure or as a regular operation, e.g. a pilot point. The operation involves a high security ship to ship communication link.

Wide/Spot beam: Satellites use a number of transponders and antennas to provide coverage in a geographic area. The covered area will share the bandwidth provided in that beam and bandwidth will be limited by the frequency and modulation the satellite uses for the beam. Spot beams will allow the satellite to give higher bandwidth in a smaller geographic area and several spots can be directed to different areas to reuse the frequency and modulation system, thus providing a higher total bandwidth to the users of that one satellite. Wide beams are used to give coverage to wider geographic areas with few users, e.g. high seas, to avoid using up the limited number of transponders and antennas the satellite carries.

1.3 Application and user level focus

The report will focus on communication services as seen from the program system that implements the different parts of the autonomous control system in MUNIN. The report will therefore not delve into details of physical communication system issues unless where it has impact on the application level QoS. This perspective is also the same as for the on-board or shore users for manned ships, so the report should also be of interest in that context.

1.4 Wireless safety critical communication focus

The report will also mainly consider safety critical communication in the scope of unmanned ship control. This means that the main focus is on wireless communication over long or very long distances and on the safety critical part of the communication. For unmanned ships this will normally be all communication. For the perspective of the manned ship it means that the report will not consider crew infotainment and related applications.

1.5 Structure of report

Chapter 2 gives a brief overview of some of the requirements to the communication system. Chapter 3 describes the QoS model and how to use it. The usage description will address all the three main areas listed above and includes the relevant functionality seen by the application programs.

Chapter 4 gives some general background on communication service types and how they could be used in MUNIN applications. Chapter 5 discuss the failure modes in satellite systems and chapter 6 radio propagation issues. Chapter 7 discusses ship and shore system failure modes and chapter 8 security issues.

2. Summary of requirements and evaluation

The general conclusion from this study is that the communication services that are available today are sufficient to implement an unmanned ship. However, there are some special issues that need to be taken into consideration during design of autonomous control system and communication services and they are summarized in the following sections. The first section will make a summary of the requirements defined in chapter 3.

2.1 Requirements summary

Chapter 3 goes through the requirements that are relevant for communication solutions for an unmanned ship. Table 1 lists the general communication channel requirements identified there together with the three main communication modes and what parts of the communication streams they utilize. The columns are capacity in kbps, maximum latency in seconds, security rating and reliability (1 is highest quality for both).

Table 1 – Summary of general communication requirements

Stream	Type	Bandwidth	Latency	Security	Reliability	Normal	Backup	Rendezvous
Rendezvous	LOS	2	0,05	1	1			X
Remote control	LOS/SatCom	2	1	1	2	X	X	
Telemetry	LOS/SatCom	32	1	2	2	X	X	
Radar and targets	LOS/SatCom	75	1	2	2	X	X	
HD Video	LOS/SatCom	3000	2,5	2	3	X		

The unmanned ship needs satellite communication for all data streams except the rendezvous type communication. The latter needs to be operational in a range up to 2 km from the ship and will be used to control the ship directly through boarding and disembarkation processes.

The accumulated bandwidth requirement of up to 4 Mbps will not be required at all times. The high capacity services are mainly used to handle unexpected situations where intervention often can be delayed until bandwidth becomes available. However, certain situations such as analysis of objects detected in the sea may need to be prioritized and may also require high definition (HD) video. If this can be handled with still pictures or lower definition video, bandwidth requirements are lower than indicated in the table.

A high capacity line of sight service (LOS) may also be used for other data streams when the ship is within range of shore mobile telecommunication services.

2.2 Special low capacity rendezvous LOS data link

For rendezvous type communication various communication means are available. The most interesting may be AIS, e.g. using the binary message structure. Digital VHF or DSC type communication may also be options although Digital VHF is not commonly used today and DSC may have too low capacity.

The problems with current VHF protocols are that they are easy to listen in on and easy to jam. Thus, sufficient security means must be in place to avoid hostile interruption or hijacking of these communication links. The project may also have to look at alternate communication links to use as backup in case of problems.

WiFi or ZigBee could also in principle be used. ZigBee in particular, offers better security and reliability than VHF based solutions. However, range is probably too limited to make them useful alternatives.

The conclusion is that AIS or Digital VHF should be used as the main carrier for this type of communication.

2.3 High capacity satellite data links

The high capacity communication link for use at high seas should be able to provide around 4 Mbps bandwidth. This can be supplied by modern VSAT services in the K_a and K_u bands. The availability of bandwidth may be lower in certain deep sea areas as there are very few customers there and services will probably be provided by wide beam transponders only. This is based on commercial considerations and satellite communication providers will be sure to satisfy users' demands, but at a cost. The new Inmarsat Global Express or any of a number of competing service providers should be able to deliver the required bandwidth if somebody is able to pay for it.

One need to be careful with the selection of service providers as they often share the available bandwidth between several users within the area the beam covers. Thus, to save money, one may use a shared service with a minimum bandwidth of, e.g. 256 kbps where higher capacities are available when needed, but not necessarily continuously or instantly. This should be acceptable as high capacity requirements not normally are critical with respect to immediate availability.

2.4 High capacity Line of Sight (LOS) data link

4G or advanced 3G mobile telephony services will be good alternatives to satellite communication in shore areas, with high security and reliability for ship to shore communication. However, these will only be secondary to satellite as the latter still is necessary outside shore radio range.

WiMAX is technically also a very good candidate. However, problems with licensing and frequencies make this technology less relevant.

Other communication systems, such as WiFi could also be used, but must be implemented in a way that overcomes some inherent security and range problems in the protocols.

2.5 Transmission protocols

For high latency and relatively low bandwidth links where there are possibilities for packet loss, it may be necessary to use a more efficient protocol than TCP/IP for transmitting time critical information (9.5). A simpler UDP based protocol with periodic handshakes as well as negative acknowledgements only will be investigated.

For the rendezvous protocol, one will have to implement reliable communication mechanisms in a similar manner or via application layer three way handshakes. It is not likely that the selected link layer protocol (e.g. based on VHF) will be suitable for direct implementation of, e.g. TCP/IP.

2.6 Security issues

Communication security is a main factor for unmanned ship. Pirates could conceivably use security holes in command data links to hijack ships and intentional jamming could lead to serious accidents. To address this, the following measures must be taken:

- The rendezvous and command data link must be secure against hostile attacks as they are intended to be used close to the ship and will be attractive for hijacking attempts. All critical data must be encrypted and authenticated before use.
- Other data links must also be protected from attacks, but these links are somewhat less critical to the operations and may use less strict security arrangements.
- The ship must have fail to safe procedures to handle loss of communication due to hostile attacks.
- The ship also needs to have fail-to-safe procedures for loss of GNSS data feeds.

Scenarios will be developed to address GNSS and rendezvous communication loss.

2.7 System redundancy requirements

Later chapters discuss various components of the total communication system and the following requirements are defined:

1. MUNIN will need two independent communication systems. Iridium and a VSAT solution are suggested (Chapters 3 and 6).
2. Suitable redundancy should be supplied on board (7.2). However, only one Autonomous Ship Controller is deemed necessary if the Rendezvous Control Unit is implemented as a separate unit.

3. Shore redundancy can be supplied by multiple control centres (7.4).
4. The rendezvous control mechanism is critical and needs careful design (see chapter 4).

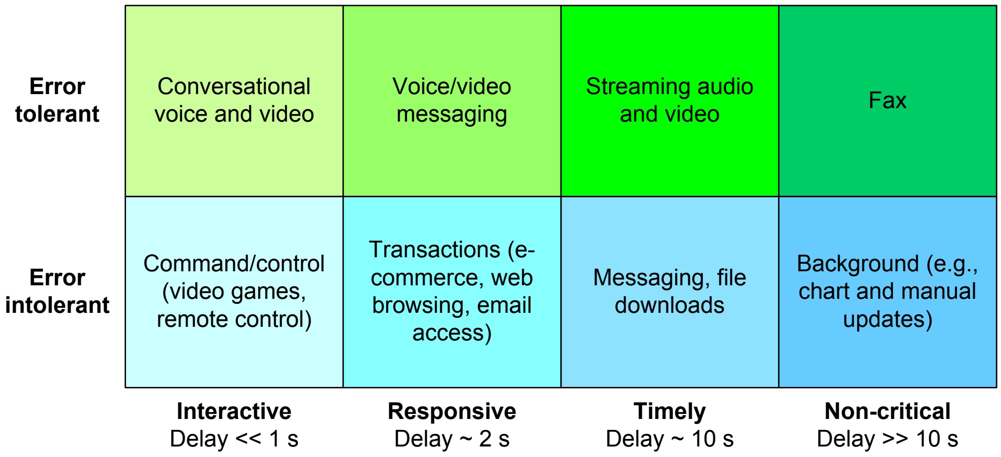
These requirements can be satisfied with more or less standard technology. Deliverable D4.4 will provide final definitions of what technology to use.

3. Unmanned ship communication requirements

This chapter will define communication requirements for operation of an unmanned ship, including a quality of service (QoS) model. Chapter 10 outlines a possible implementation of a software service layer that will cater for these requirements.

3.1 User centric response requirements

The ITU-T Recommendation G.1010 /5/ has analysed the error tolerance for different types of communication services. Figure 1 illustrates how they assess the effects of latency in communication services. They classify the criticality of services as interactive, responsive, timely and non-critical, and the communication services error tolerance.



Error tolerant	Conversational voice and video	Voice/video messaging	Streaming audio and video	Fax
Error intolerant	Command/control (video games, remote control)	Transactions (e-commerce, web browsing, email access)	Messaging, file downloads	Background (e.g., chart and manual updates)
	Interactive Delay << 1 s	**Responsive** Delay ~ 2 s	**Timely** Delay ~ 10 s	**Non-critical** Delay >> 10 s

Figure 1 – Model for user-centric categories

Maritime autonomous systems will belong in the "Command/control" box, and hence they are classified as error intolerant and it is assumed that they will have strict timing/latency requirements. However, ship control is a relatively slow process, so one can in most cases accept a few seconds delay here. This is also necessary as an unmanned ship will be dependent on relatively high latency satellite communication when far from the shore. Autonomous control functions must be designed so that faster response requirements are handled on-board.

3.2 Main communication requirements for MUNIN

There are a large number of communication services available for manned and unmanned ships, but not all are relevant for MUNIN. Some, such as AIS and NAVTEX, have a special purpose that is the same for an autonomous ship as a normal manned vessel and are not included in the discussions in this report. The exception here is the rendezvous control protocol that may be implemented over, e.g. AIS. Other protocols are related to crew use and infotainment and are omitted also. The services that have been identified as critical are listed in Table 2. Column three lists the estimated bandwidth requirement, based partly on rough estimates for different communication system availability. The estimates are based on the following assumptions:

- *Normal remote control and monitoring*: All communication streams in Table 3 with some additional spare for more extended telemetry.
- *Backup remote control and monitoring:* All communication streams in Table 3, except video, with some additional spare for video stills.
- *Rendezvous control*: Only the rendezvous stream listed in Table 3.

Table 2 – Main communication requirements for unmanned ship

Service	Purpose	Bandwidth
Normal remote control and monitoring	Normal operation and monitoring of vessel. Sufficient for direct monitoring and control of all relevant operations on the ship with access to high bandwidth video feeds.	< 4 Mbps
Backup remote control and monitoring	Medium capacity link for backup when main link fails. Sufficient for remote monitoring and control of all important functions, but limited bandwidth for live video feeds.	128 kbps
Rendezvous control	Low capacity link for remote control of ship when within eyesight. For use during entry to the ship by rescue team.	2 kbps

These requirements are related to full remote control of the ship, e.g. when the operator has full control of the ship. During monitoring and autonomous control operations, the actual bandwidth demands are significantly lower. However, these requirements also reflect the availability limits for when the operator in the SCC and the ASC needs to be notified that full communication functionality is no longer available.

Table 3 – Importance of communication streams

Type	Bandwidth	Latency	Direction	Security	Reliability
Rendezvous	2 kbps	50 ms	Ship<->ship	High	High
Remote control	2 kbps	1 sec	Ship<->shore	High	Medium
Telemetry	32 kbps	1 sec	Ship->shore	Medium	Medium
Radar and targets	75 kbps	1 sec	Ship->shore	Medium	Medium
HD Video	3 mbps	2.5 sec	Ship->shore	Medium	Low

Within each of these categories, different data streams have different importance. Table 3 lists some of these streams and indicates their importance. The classification shown here is tentative and may be changed over the project's life time. Classification is also relative so "low" does not mean one can generally do without that particular data channel. The intention is mainly to show what types of traffic need to be supported and that each type has different properties with respect to what services it requires.

The bandwidth column indicates required bandwidths for the different streams and the latency column specifies the maximum acceptable latency. The actual delay perceived by the user will typically be twice this value as most interactions require controls sent to ship and thereafter some response.

For VSAT type communication, latencies will minimum be 280 ms due to the physical distance to the satellite in geosynchronous orbit. Normally, one will experience latencies around 0.3 seconds. For Iridium, one report indicates that the latency is on the order of 600 ms for a one way transmission /15/. Thus, the values listed here should be achievable with available communication services.

The streams listed are:

- *Rendezvous:* This is a communication channel used to control the ship by a boarding team to facilitate entry to the ship. This may be after loss of communication or during normal boarding and disembarkation procedures. This needs to have high reliability and security, i.e. protection against false control signals and listening in to the exchange of data as well as good protection against link or message loss. Only simple telemetry such as position, speed, heading and similarly simple controls are transmitted so a 2 kbps channel should be sufficient (see also next paragraph).
- *Remote control:* This includes communication between ship and shore for high level monitoring and control of the ship. Security has to be high, but reliability requirements are lower than for the previous as the ship has the possibility to go to autonomous modes if communication is lost. Bandwidth requirements are more or less the same as for rendezvous. ITU estimates that an unmanned aircraft will be able to operate with a maximum requirement of about 15 kbps in flying mode for remote control functions /21/ A ship should be able to operate at substantially lower bandwidth due to much slower changes in operational status, so around 2 kbps should be sufficient.
- *Telemetry:* This is status updates from the ship beyond high level monitoring, but excluding visual data streams such as radar and video images. Here, both security and reliability is a medium strong requirement. Security is lower than previous as it is assumed that hostile intervention in transmission will be less critical here

than for remote control. 32 kbps is sufficient for about 5000 data values updated each 2.5 seconds. This satisfies most requirements except very high sample rate signals from engines or other fast moving equipment. Telemetry is not normally mission-critical, but is important in cases where problems have developed and diagnostic procedures are required.

- *Radar and radar targets:* These data are similar to telemetry, but the transmission requires higher bandwidth. The calculation here is that the operator may need one image of 1024*1240 pixels transferred each 30 second with an effective compression down to 2 bits per pixel. This data stream may also include some still pictures from video systems. Reliability is set to medium.
- *HD Video:* This stream contains high definition live video from the ship. This can include external as well as internal views. It is assumed that basic control of the ship normally can be done without video, so the criticality is set to low. ITU-T Recommendation G.1010 /5/ lists about 400 kbps as needed for video conferencing and similar applications. A typical bandwidth requirement for high definition video (films etc.) is between 2 and 4 mbps according to various Internet resources. Thus, 3 mbps is selected to allow a mix of at least one high quality channel and one or more lower quality channels. This will also allow transfer of high bandwidth telemetry data that can be used, e.g. in detailed engine diagnostics.

The quantitative bandwidth requirements are not based on very accurate analysis at this stage, but have been set from previous experience and estimates. It is believed that they are representative, but they may be updated in later publications from the project.

3.3 Multiple Unmanned Ships

This report will mainly focus on the requirements and possibilities for supporting *one* unmanned ship. However, in the future several unmanned ships may operate under the same satellite beam and all will require reliable communication services. This issue is similar to the problem one is faced with when multiple unmanned aerial systems are operating in the same radio communication area /21/ However, as unmanned ships have very different high capacity demands, e.g. high capacity streams are only necessary in special situations, the situation should be simpler to handle. One will obviously require more bandwidth, but as demand on bandwidth normally will vary between ships, one can argue that statistical distribution of demand will keep accumulated requirements at a level that can be satisfied by available satellite systems. Also, if a situation where many unmanned crafts are operating simultaneously in the same area occurs, higher demands for bandwidth should also lead to a higher supply. The main limiting factor for satellite bandwidth in high seas today is the lack of customers and, as a consequence of that, a correspondingly lower offered bandwidth.

3.4 Shore based (LOS) or space based communication systems

In general terms, communication from ship to ship or ship to shore is either with line of sight (LOS) type communication or communication via a "relay station" which almost always is a space satellite. It is in principle possible to use airplanes, balloons or blimps as relays to extend the LOS range, but this is currently not common and will in any case only give limited range extensions. Thus, for MUNIN, Table 4 lists the most relevant systems to be used.

Table 4 – Communication systems use

System	Type	Usage area	Protocols and capacity
Ship to ship	LOS	Ship rendezvous.	AIS, Digital VHF (DSC). Special protocols: 2 kbps
Ship to shore	LOS	Ship control and monitoring during coastal approach.	3G-4G, WiFi or WiMAX. TCP/IP and UDP: < 4 Mbps
Main ship to shore via satellite	SatCom	Ship control and monitoring at high seas.	VSAT systems, such as Inmarsat or commercial suppliers. TCP/IP and UDP: < 4 Mbps
Backup ship to shore via satellite	SatCom	Backup ship control and monitoring at high seas.	Iridium typically. TCP/IP and UDP: 128 kbps

3.5 Communication types suggested used in MUNIN

Section 9.1 discusses possible communication types and section 9.5 discusses some problems when using TCP/IP for time critical communication. Table 5 lists the communication services that will be used in the MUNIN project.

Table 5 – Overview of MUNIN communication types

Service type	IP	Description
Stream (reliable)	TCP/IP	Point to point data stream, e.g. file, sound, video. Typically used for high criticality and large data images, e.g. radar images and software or data image updates.
Reliable message	UDP with retransmit	Point to point messages with guaranteed delivery and sequencing. Same properties as stream. Typically used for remote control and monitoring.
Unreliable message	UDP	Point to point messages, typically used for high volume data where packet loss is tolerated, e.g. video or sound.
Unreliable message for Rendezvous	n/a	This will be an unreliable message service where retransmissions and acknowledgements must be used to get a suitable integrity level.

The two first services should be implemented over standard Internet protocols through a software API. The API will also provide notification when data link breaks down or QoS attributes change significantly. Thus, the applications need not implement functionality for handling lost messages or data other than a more general broken data link call-back function.

The three first services should also be connection oriented, i.e. the application will always know that the communication link is alive until notified otherwise by the system AÅI layer.

The rendezvous service will probably *not* be connection oriented. A relatively low level communication mechanism will be used and it will be too costly in terms of delays and bandwidth to implement the necessary session control and retransmission mechanisms. It is more efficient to implement, e.g. a three-way hand shake directly in application protocols (see Figure 8).

3.6 A Ship-Shore Communication QoS Model

This section will define a quality of service (QoS) model for communication between the unmanned ship and shore. This model will be used in the development of autonomous ship control functions, with the following main uses:

1. It will provide an analysis of failure modes and likelihood of failures for the communication system. This shall be used to determine *what* alternative or fail to safe (FtS) functions are required in an autonomous shipping system.
2. It will be a reference for design of the high level control strategy. This includes quantitative measures for the different quality attributes so that one can determine *how* alternative or FtS procedures are activated.
3. It will also provide a method for continuously communicating the values of the actual QoS attributes to the ship or shore functions so that these can determine *when* to activate alternative or FtS procedures.

With this in mind, it is suggested that MUNIN uses a QoS model that includes four parameters to describe different aspects of the communication service. These are listed in Table 6.

These attributes will not be communicated back and forth between application code and communication software during normal operation of the autonomous or unmanned ship. Rather it is expected that the application code will define their minimum requirements for various operational conditions and that the communication software will manage the data transfer requirements based on these specifications.

Table 6 – Quality attributes

Attribute	Unit	Description
Bandwidth c_{kbps}	kbps	Mean expected bandwidth available for the application program (kilo-bits per second). This may be different for different programs, dependent on status of communication link and the priority of the program service.
Latency t_{lat}	ms	Mean expected delay from a one byte message or stream element is sent from sender application until it is available for the receiver. Note that for messages, the bandwidth and message size will add a delay not captured in this measurement. $t_{tot}=t_{lat}+\frac{8\,m_{byte}}{c_{kbps}}$ (Eq. 1) The total delay (t_{tot}) in milliseconds will be the sum of the latency (t_{lat}) and the ratio of 8 times the bytes to send in the message (m_{byte}) to the bandwidth in kilobits per second (c_{kbps}).
Reliability q_{rel}	1-4	High (1) to low (4) representing the possibility that the data link or a message is lost unexpectedly. Level 1 corresponds to Inmarsat GMDSS integrity level while level 4 represents a very high probability that the link may be lost.
Security q_{sec}	1-4	High (1) to low (4) security representing the inverse of the possibility that data is spied upon or manipulated during transit. Level 4 represents open unencrypted transmissions while level 1 represents a tamperproof system which in the context of MUNIN should mean that messages cannot be decrypted within a time frame of about one hour. Note also that both encryption (hiding data) and digital signatures (verifying sender) or similar systems are required.

As specified in section 3.2, there are a number of different communication scenarios that the application software should be ready to adapt to. In principle, the applications should specify their specific requirements to QoS in each of these scenarios and the communication software will do its prioritization between requirements to select what application gets what level of service.

4. Radio propagation and coverage issues

This section discusses radio propagation issues in general, but with a strong emphasis on satellite communication. The reason for this is that satellites normally have a more restricted link budget than terrestrial communication systems as power must be generated from limited area solar panels and also because transmission distances are much longer.

4.1 Radio transmission bands

IEEE /18/ has defined standard letters for different frequency bands that are relevant for radar and satellite transmissions. These bands are typically in the centimetre to the millimetre wavelength range. The most common band codes are listed in Table 7. Additional rows are added for VHF and UHF frequency bands. Note that both L and parts of S band are within the UHF band.

Table 7 – IEEE Radio band codes

Band	Frequency	Origin of name
VHF	30 to 300 MHz	Very high frequency (marine 156 to 174 MHz)
UHF	0.3 to 3 GHz	Ultrahigh frequency (marine 457 to 467 MHz)
L band	1 to 2 GHz	Long wave
S band	2 to 4 GHz	Short wave
C band	4 to 8 GHz	Compromise between S and X
X band	8 to 12 GHz	Used in WW II for fire control, X for cross (as in crosshair)
K_u band	12 to 18 GHz	Kurz-under
K band	18 to 27 GHz	German Kurz (short)
K_a band	27 to 40 GHz	Kurz-above

The most relevant bands for satellite communication are L (Inmarsat and Iridium), C (various VSAT providers, normally quite expensive services), K_u (most common VSAT band) and K_a (newer VSAT services including Inmarsat Global Express). K_a is becoming increasingly more popular as demand for bandwidth grows. Note that S (3 GHz) and X (10 GHz) are also used for maritime radars.

4.2 Multi- or single user outage

Given that link interruptions and system component failures can lead to service outages, and each outage requires varying restoration times, availability characterizes the impact of interruptions, failures and service restoration times on the usability of a system. Outage occurs when a service achieves a certain Bit Error Rate (BER), where transmitted data packages cannot be restored by embedded data correction codes, or when physical equipment fails.

The Radio Technical Commission for Aeronautical Services (RTCA) considers two categories of outages /17/:

- Multi-user service outage: A service outage simultaneously affecting multiple users within a defined service volume. This is normally a result of system component failures, involving space or ground segment systems.
- Single-user service outage: A service outage affecting any single user within a defined service volume. This will normally be a failure associated with local atmospheric problems, typically represented as package loss due to high BER, or user equipment problems.

Both categories will be important for maritime autonomous systems. If an error occurs in a communication system it could either affect several ships within a defined region or it could affect only one single ship. Satellite failures and signal attenuation due to, e.g. ionospheric effects could affect multiple ships, while failure on ship equipment is an example that will lead to single ship service outage.

General availability may also be dependent on the geographical location of a ship. E.g. in polar areas at higher latitudes than 75° there is limited access to communication signals from satellite systems based on geostationary satellites as, e.g. Inmarsat. However, availability can also be restricted in other areas, e.g. in fjords and in ports where communication system signals can be shadowed from surround mountains or buildings.

4.3 Signal degradation sources

There are different external influences on communication systems that can lead to reduced bandwidth, higher latency, lower reliability and security and they can occur within different parts of communication system architecture. The main problems were listed in Table 8, but will be discussed in some more detail here. The table indicates that reduced availability is most likely to happen due to impacts on the physical transmission path from the satellite to the ship or vice versa. In particular, effects related to atmospheric loss and ionospheric scintillation will be important. This section will describe these problems in some detail.

Degradation factors for radio transmissions can loosely be collected in three groups. The main group is loss due to distance and frequency which is independent of the medium the radio signal passes through:

- *Free space dispersion loss* is caused by the spatial propagation of the radio signal and will be proportional to the square of the distance.
- *Antenna aperture loss*, which is generally proportional to the square of the frequency.

- *Antenna gain*, which for the same size directional antenna is proportional to the square of the frequency. As there is both a transmitter and receiver, the total effect is a gain increase by the fourth power of the frequency increase.
- *Transmitter electronics loss,* which can be expected to be about linear with frequency. This is mainly an issue for the satellite with a limited power budget.

Thus, for the same transmission power one can roughly expect a proportionally better signal to noise relationship by increasing frequencies.

The second group consists of factors that can give significant environmental signal loss either due to dispersion in atmosphere or due to effects of the electromagnetic field surrounding the earth. There are two main factors in this group:

- *Scintillation loss:* Rapid changes in amplitude and phase due to changes in atmosphere's refractive index. This is typically most noticeable on low latitudes near the equator, but it will also occur in the aurora regions near the poles. The effects will be stronger for lower frequencies, e.g. more pronounced for L-band transmissions than for K-band.
- *Rain fade:* Humidity in the atmosphere, rain and in particular sleet can have a substantially negative impact on signal strength. This effect is also frequency dependent and is stronger with higher frequencies and becomes significant from about 10 GHz and up (K_u and K_a bands)

These effects can in severe cases cause communication outages. The effects are, as stated above, dependent on position on Earth and other factors such as time of year and solar activity. Although the link budget for satellites will take these effects into consideration and will provide better power margins for the most affected frequencies and areas, severe cases will from time to time exceed these margins.

Other examples of environmental degradation factors for radio communication are listed below. These factors are normally relatively small, but can have significance in some cases.

- *Ionospheric losses:* Mostly for lower frequency signals and vary considerably with time of day and sunspot activity.
- *Beam dissipation:* Loss due to the spreading of signals passing through the atmosphere.
- *Polarization loss:* Losses due to phase rotation of the signal passing through atmosphere.
- *Rayleigh fading:* Interference between main signals and the same signal arriving through other paths through the atmosphere.

- *Doppler effects:* If the sender is moving at high speeds relative to the receiver, Doppler effects occur that may cause losses in transmission.

L- and K_u-band are the most common frequency bands used today in communication systems. K_a is becoming more common as demand for bandwidth grows. Thus, for the analysis in this report, it is scintillation for L-band and rain fading for K_u- and K_a-band that has been considered. One should note that C-band may be more robust against any of these effects and may also be a candidate. However, C-band is less readily available and may be more costly in use.

4.3.1 Rain fading

Higher frequencies are in general less robust to humidity, rain and sleet and as a rule of thumb one can say that the attenuation increases with the square of the frequency. This means that signals in the K_a-band (30/20 GHz) are more than four times affected than signals in the K_u-band (14/11 GHz).

One may compensate for such problems, e.g. by using a larger antenna to increase SNR at the receiver or transmitter. Systems will also compensate for these effects by increasing transmission power in the satellite and on ship terminals.

The fading effect is dependent on geographic location. Longer paths through the atmosphere at higher latitudes increase attenuation and areas around the equator tend to have higher humidity and more rain than temperate zones.

4.3.2 Ionosphere scintillation

Scintillation is the rapid fluctuation of the amplitude and phase of radio waves caused by electron density irregularities in the atmosphere. The effects tend to be more severe for lower frequencies, e.g. VHF to L-band than higher frequencies. The effects also occur most strongly in special areas near the equator and to a lower degree in the aurora areas and near the poles. These effects can cause significant problems for L-band transmissions. Fluctuations of the amplitude of more than 20 dB have been measured for GPS signals /9/ and for Inmarsat near the equator/10/. This can be expected to be less problematic for higher frequencies such as K_u-band, but it may be noticeable for C-band.

Iridium has its lowest satellite density near the equator. Simulations indicate that there will be in sum about 17 seconds each 24 hours where no satellites are visible at all /11/ at the equator. This should not be a problem during normal operation, but combined with the scintillation effects and decreased SNR, it may impair Iridium coverage. It is difficult to find actual measurements of performance in the literature, but one paper /12/ discusses the performance of Iridium in the USA. It quotes a frequency of not being able to connect or losing the connection before 3 minutes as 3 and 4 respectively out of

359 attempts in North California and correspondingly 4 and 15 out of 359 in Texas. Both places are at latitude above 30˚N and scintillation is probably not the cause here. However, it illustrates that there are significant disturbances in communication even at more optimal latitudes.

L-band transmissions for Inmarsat C and Fleet 77 may also be impaired by scintillation, but the GEO orbit will in most cases give shorter transit through the atmosphere and no problems with Doppler shifts. It is also possible to use higher gain antennas to reduce or overcome this problem.

4.4 Frequency allocation

One potential challenge for safety critical systems is the frequency allocation plan. If maritime mobile services need to share frequency spectrum with other types of mobile services, this can lead to crowded spectrum and possibilities for interference. The ICAO working group for navigation, communication and meteorology (sub group 15) has pointed this out as a concern for the aeronautical industry.

4.5 Geographic coverage

Another issue that may cause degraded availability of satellite services is where on the globe a service is used. Figure 2 shows the world where red colour coding has been added to indicate areas where service quality may be lower. This is not an accurate description of actual service availability, but a principal sketch to illustrate geographic issues.

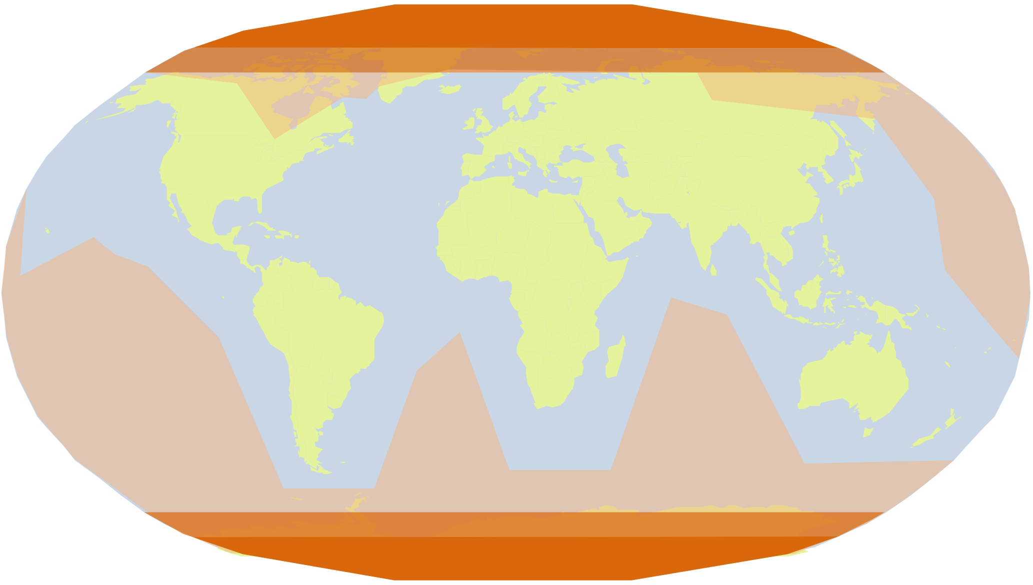


Figure 2 – Principal differences in service availability

The main geographic factors that have been used in this figure to indicate limitations in available satellite communication services are:

- *Polar regions:* Above 80 degrees one cannot normally use geostationary satellites. Only Iridium, of the main services, is available.
- *Sub-polar regions*: Between 70 and 80 degrees various factors may make geostationary satellite communication unreliable. This may be shadow effects, atmospheric or ionospheric effects or satellite position far to east or west of the ship. In some cases and regions, the limit of use may be as low as 60 degrees.
- *Deep sea areas*: Satellite services are based on commercial viability and one will generally see fewer services available in areas with few customers, i.e. on deep seas and in sparsely populated land areas. However, as this is a commercial effect and as there is a low number of users, this should not normally cause problems for unmanned ships.

For MUNIN it is expected that the necessary bandwidth will be available in all relevant areas. Although MUNIN has identified substantial communication requirements, the full bandwidth may not need to be available at all times. The outlined system has for instance the ability to go to autonomous operation to reduce the required bandwidth. Also, as any realization of an actual unmanned ship will be several years into the future, one can probably assume that necessary bandwidth will become available as communication demands increase.

5. Line of sight communication systems

Line of Sight (LOS) communication is relevant for two cases in the MUNIN project:

1. It is necessary for ship to ship communication and for implementation of the rendezvous control protocol. This needs to be a special purpose protocol with a high integrity level, but not very high bandwidth.
2. It may be used for high capacity main control links during coastal passage and port approach. LOS type communication may give high bandwidth at low cost and with much lower latency than satellite systems.

In the following, a brief overview of possible systems is given with some discussion on suitability for the possible applications.

5.1 Mobile telecommunication systems

The most relevant high capacity system for MUNIN will probably be mobile data transfer technology. With fourth generation (4G) system now coming up, these will provide bandwidth and security that is well suited to the requirements for MUNIN. However, developments in this segment will be driven by high population density requirements which typically mean higher bandwidth in smaller cells and shorter range than ships will generally require. In port and port approaches, high capacity and high quality LOS communication should therefore be quite feasible.

3G systems may also be used for high capacity data links when suitable 3G systems are available. The original IMT-2000 specification /26/ had a minimum high capacity rate of 200 kbps, but this has been increased substantially in newer “IMT-Advanced” /27/ specifications.

A problem for ships in international traffic is to establish roaming agreements in the ports of calls, but unmanned ships will probably be most relevant for scheduled shipping where such agreements easily can be established.

Mobile telecommunication systems could in principle be used for rendezvous control, but then only when both ships can access a base station. While it is possible to install a GSM base station on a ship for use in open waters, this is not considered to be an optimal solution for MUNIN. It is much better to develop a special protocol based on direct communication between the two ships.

5.2 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) /28/ has long been promoted as a very good solution for high bandwidth applications over long distances. However, as customers to such services are far between and not generally willing to pay for the service, WiMAX has slowly been delegated to special applications and the frequencies previously allocated to WiMAX are now being freed for other use. In general, WiMAX operates on licensed frequency bands and cannot easily be used for specific maritime applications without having the proper licenses.

Apart for the frequency issues, WiMAX would have been ideal for unmanned ships as it provides high security, high bandwidth and high integrity over distances up to 20 km. WiMAX may also be a candidate for rendezvous communication. However, frequency availability and licensing issues are problems that make this impractical.

5.3 WiFi, ZigBee and other ISM services

WiFi operates in unlicensed frequencies in the "Instrumentation, Scientific and Medical" (ISM) bands. It may be a possibility for rendezvous type services and possibly also other LOS remote control applications. However, WiFi is very easy to jam and the bandwidth is often shared between multiple protocols so it may not be optimal for this service.

The other protocols in the ISM band may also be of interest. Bluetooth is a much safer protocol than WiFi, but has much shorter reach, in the range of a few tens of meters. A rendezvous service should at least operate on one to two kilometre ranges.

ZigBee /29/ is another option that could be used, but ZigBee is also primarily intended for short range communication. ZigBee PRO is claimed to be able to operate on longer distances, but as ISM use limits the maximum power output, this will also be in the area of a few hundred meters.

None of these services are currently considered suitable for either of the two MUNIN LOS cases.

5.4 AIS, DSC and other VHF services

VHF is mainly used for voice communication, but ITU specifications have been developed for digital VHF communication over one 25 kHz channel that will give about 22 kbps per channel /19/ More digital bandwidth can be achieved by bundling channels before modulation. Some of these systems are in operation, e.g. in Norway, and it is very likely that the IMO e-Navigation initiative will increase the deployment of this technology in other areas. In MUNIN it may be relevant for rendezvous type services and it may also be used for remote control and simple telemetry. The system is relatively easy to intercept and jam so it needs to be used with care and probably only as one option in a multi-channel set-up.

Also normal VHF communication uses digital modulation to implement Digital Selective Calling (DSC). However, this only provides 1.2 kbps in channel 70 of the VHF band and is of limited use for MUNIN. One might use the same technology to implement a rendezvous type service, but VHF is again vulnerable to hostile attacks.

AIS has an effective bandwidth of about 6 kbps per 25 kHz channel. If standard binary messages are used, one will get even less throughput, but the service may still be used as part of a rendezvous type communication link. AIS is not relevant for other types of communication than very low bandwidth services. AIS is also easy to intercept or jam by hostile parties.

AIS is currently the best option for the rendezvous function, but Digital VHF should also be investigated. Digital VHF may also be a backup option for medium capacity communication, but availability of Digital VHF systems is currently an issue.

5.5 UHF

UHF may also be an option for rendezvous control. However, this will require the development of a suitable digital modulation protocol on top of the UHF bands that are reserved for maritime use today. The benefit is again that frequencies are allocated and that they may be used for such services as long as relevant requirements from ITU regarding cross talk and power are satisfied.

Note that the UHF channels used for maritime communication are also used by land services. Thus, it may be problematic to use UHF close to shore.

UHF is not considered relevant for either of the MUNIN services at this stage, but may be investigated further if other alternatives become less relevant.

6. Satellite system architectures and failure modes

This chapter discusses the physical effects that may cause problems for satellite communication systems. These are generally related to physical failures in one of the system components or to propagation problems for radio waves through space and atmosphere.

6.1 Methodology

The analyses performed in this section are based on the "SatCom Availability Analysis" performed by the ICAO working group M, Iridium subgroup /7/. This analysis was performed in 1996 in order to develop technology evaluation criteria for evaluation of new technologies for mobile aeronautical communications. The analyses were based on a methodology presented in RTCA DO-270 /31/, and both new terrestrial and satellite-based technologies were assessed. As for maritime autonomous systems the aeronautical systems are associated with high security and safety requirements.

6.2 System architecture and failures

The system architecture for fault analysis is shown in Figure 3. The red and green boxes correspond to the elements looked at in the ICAO analysis. The blue boxes are discussed in the next chapter.

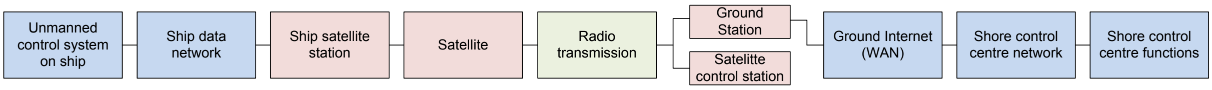

Unmanned control system on ship
Ship data network
Ship satellite station
Satellite
Radio transmission
Ground Station
Satellite control station
Ground Internet (WAN)
Shore control centre network
Shore control centre functions

Figure 3 – System architecture for fault analysis

The ICAO analysis defines a fault tree as shown in Figure 4.

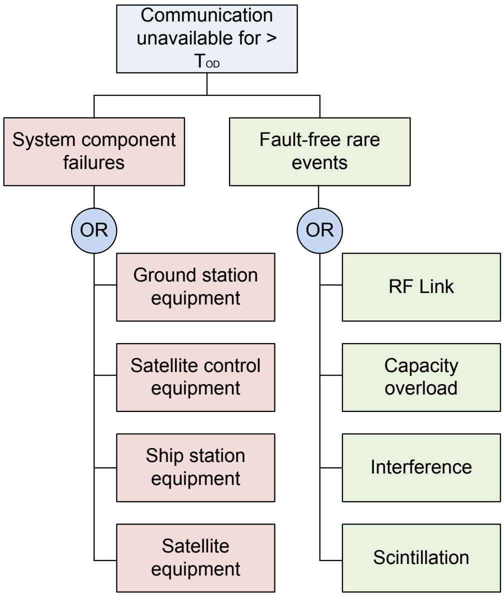


Figure 4 – Satellite system fault tree

The "fault-free rare events" are events related to the communication link. They are discussed in more detail below. The colour coding corresponds to the colours used in Figure 3. System component failure can occur within different physical parts of the communication system:

- Ground station equipment. This is the equipment on ground used for data transmissions to and from the satellite. In a technical well proven system it is very unlikely to have failures in the ground station equipment. The systems have typically been operated for many years, and redundancy, maintenance and monitoring are well taken care of by the satellite operator. The satellite operators guarantee a certain level of service quality within defined coverage areas, and they will put large efforts into ensuring that accessible ground system components are well functioning at all times. If there are several ground stations components that exist in a network, failures could appear in the network itself, although this is also unlikely to happen.
- Satellite control equipment. This is equipment in a ground control station that is used to control the satellite, e.g. how to use on-board radio transponders or management of satellite power use and generation. Failure in this component may also cause loss of some or all communication links operated over that particular satellite. This is also a component which the satellite operator has control over, and it is very unlikely that errors will occur also in this part of a communication system.
- Ship station equipment – Failure events could be associated with the radio equipment. This is a more likely event to occur due to e.g. age of system, non-correct installation etc.
- Satellite equipment – Failure events could be associated with the satellite itself. Developing and launching communication satellites is expensive, and large effort will be put into testing and verification before the satellite is in operation. Most systems are redundant and there are spare satellites that can be put into operation if another one fails. This could take some time and lead to a short service outage. Although a failure in the satellite may have severe consequences for the service level offered to the ship, it is also a rather unlikely failure event.

The fault-free event availability elements are:

- RF link event – This accounts for random radio frequency events (such as severe fading) for which defined system link budgets are not met and which could lead to service outage. The probability for such events depends on the geographical location of the ship and weather conditions. Rain attenuates signals in higher frequency bands such as K_u- and K_a-band. K_u-band is to a large extent used by satellite communication systems today, while more and more satellite service providers offer K_a-band. In polar areas the signal traverses a long distance through the atmosphere, and they will be more affected by atmospheric effects. The overall probability of such failure events is much higher than system component failures. This issue is discussed in Chapter 4.

- Capacity overload event – This accounts for conditions where available communications capacity is overloaded. Communication services based on global beams from the satellites are more vulnerable to such events, especially in high traffic density areas. For MUNIN, this may mean that the operator has to buy a prioritized service from the satellite service provider to ensure a suitably high QoS.
- Interference event – Accounts for aggregated interference environmental effects from external sources that may lead to service outage. This could occur from e.g. emissions from other radio systems installed on board a ship, such as, e.g. the radars. Interference could also occur from intentional jamming.
- Scintillation event – The ionosphere, the sun and earth's magnetic fields could produce random variations in electromagnetic waves traversing the ionosphere. See more information about this effect in Chapter 4. The ionosphere has highest impact in signals in L-band, which is the frequency band dedicated to GNSS and communication systems (such as, e.g. Inmarsat and Iridium).

A summary of the potential failure components in a satellite communication system is given in Table 8.

Table 8 – Failure components in satellite communication systems

Failure component	Prob.	Comment
Ground station	+	Satellite service provider control.
Satellite control equip.	+	Satellite service provider control.
Ship equipment	++	Old equipment, non-correct installation.
Satellite	+	Satellite service provider control.
RF link	+++	Atmospheric effects, depends on position of vessel. Higher probability in polar areas due to low elevation angles.
Capacity	++	Many users in one cell (global beam), operation on the edge of coverage areas.
Interference	++	Intentional and unintentional.
Scintillation	++(+)	Ionospheric effects, depends on position of vessel. Higher probability in polar areas and near equator.

The assumed probabilities for failure events in the above discussion is based on the analyses performed by the ICAO working group M, Iridium sub group /8/ These probabilities are illustrated in the table, where +++ means that a failure is possible (availability better than 0.995) , ++ means not likely, but possible (availability better than 0.9995) and + not likely (availability approximately one). Availability of 0.995 means approximate downtime of 40 hours per year. Note that figures are very uncertain and should be looked at as "order of magnitude".

6.3 Use of satellite communication for autonomous crafts

ITU has published two reports dealing with spectrum and bandwidth allocation to unmanned aircrafts /21/ /22/ Data from these reports have also been used as basis for the analysis in this report, although applications are very different.

ITU has also proposed to develop similar reports for unmanned marine vessels, but this is currently focusing on small vessels for inspection or data collection /30/.

6.4 Use of redundant communication systems

As discussed in other sections, there are several failure modes associated both by the infrastructure and the atmospheric transmission. To provide a robust solution, the MUNIN project will stipulate that two independent satellite systems are available for remote control and monitoring. One should be a VSAT system operating outside the L-band, i.e. not Inmarsat. The second should be an alternative system operating in L-band, e.g. Iridium or Inmarsat GMDSS services.

The use of different frequency bands will minimize the chances of disturbance to signals due to atmospheric effects.

7. Ship and shore physical network systems

This chapter will look at failure modes related to the physical data networks on the ship and in the shore control centre. Figure 3 in section 6.2 shows the system architecture of the full communication system. The blue boxes correspond to ship and shore equipment outside the satellite system discussed in the previous chapter. This chapter briefly discusses issues related to these two system components.

7.1 General ship and shore systems

In general, a ship data network can be illustrated as in Figure 5 /14/. This figure illustrates the network as a layered architecture, with fast real-time networks at the bottom and increasingly higher levels of integration as one moves up in the system.

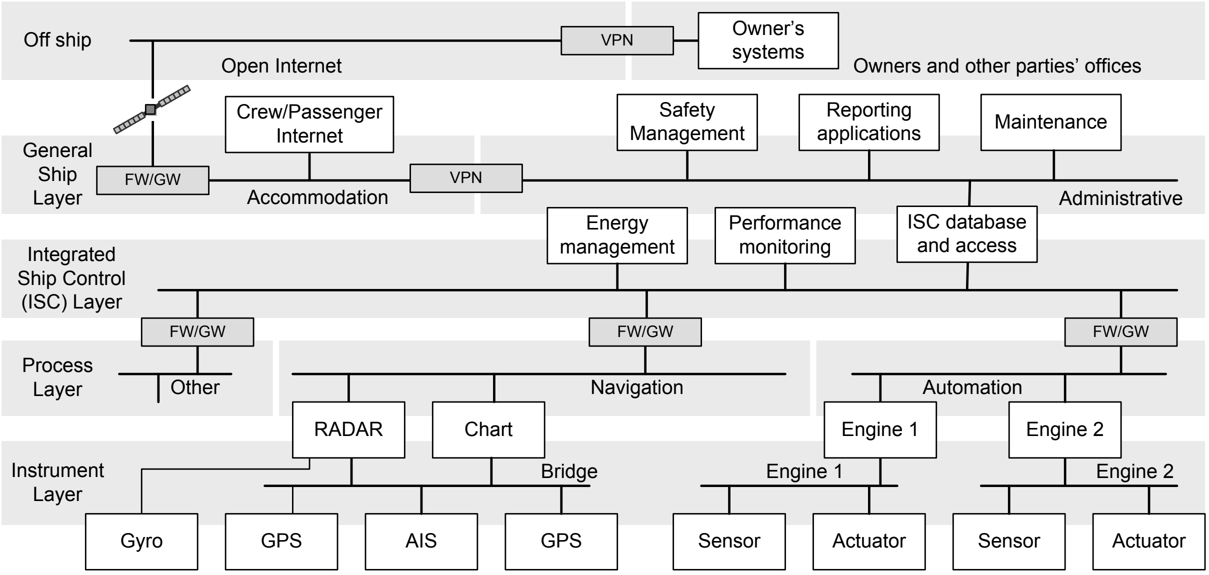


Figure 5 – General ship data network architecture

The autonomous control functions will normally reside on the Integrated Ship Control (ISC) layer with an application level firewall separating it from the general ship layer. This firewall would most likely be integrated in the autonomous control functions themselves and typically in the form of the system level communication services (see Figure 10). This would in turn use, e.g. Virtual private Network (VPN) or similar secure protocols to communicate with the shore systems.

7.2 Special considerations for LOS communication systems

LOS networks, e.g. GSM, VHF and WiMAX, are susceptible to the same radio propagation problems as are discussed in chapter 4. However, as transmission distances are shorter and as transmission power may be more easily adjusted up, these effects will normally not be a significant issue. In long distance communication, e.g. with WiMAX and VHF one may see some effects in rare cases.

The LOS communication systems can be roughly divided into two categories:

1. Direct point to point communication. This can be VHF or WiMAX used as a direct radio link. Failure modes are only related to sender and receiver and potentially radio transmission disturbances, mostly from jamming or interference.
2. Infrastructure based communication. These are typically GSM systems where one or more base stations are involved. This introduces more failure modes than direct point to point links. AIS based communication via land based base stations is also in this category.

GSM systems are normally part of critical infrastructure for the society at large and will have protection against failures in system components or intentional jamming. However, as base stations are relatively accessible there are chances of intentional or unintentional interruptions of services when only one base station is available. This can be alleviated by having redundancy in base station coverage, but this may not be possible for more sparsely populated areas. Thus, there are security risks associated with using this type of infrastructure.

Direct point to point communication will mostly be susceptible to jamming as equipment is more or less under control of the users. As is discussed elsewhere, VHF, including AIS and WiFi is easy to jam while WiMAX may be more complicated to disturb. This is a direct consequence of the modulation techniques employed. WiMAX is unfortunately difficult to employ due to licensing restrictions so special care must be taken when this type of communication is used.

7.3 Ship system failure modes

In a critical application like autonomous control, some selected details of the specific architecture would probably look as in Figure 6. This configuration avoids failure modes associated with network problems and system connectivity. Any single fault will not impact data transmissions in system. In addition, duplication of the satellite stations will create a backup in case of failure in one satellite system.

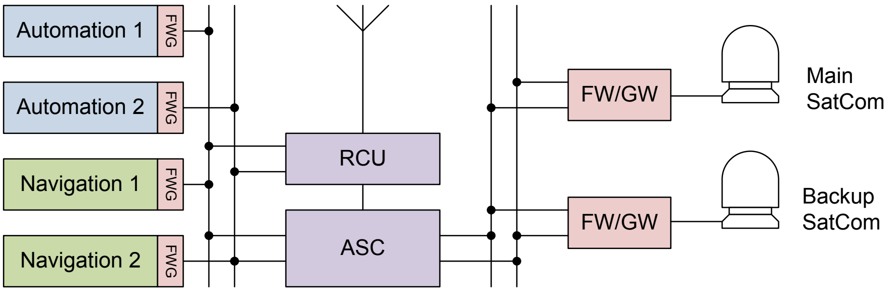


Figure 6 – Ship system redundancy

A similar redundancy will typically be found in ship systems, both on navigation and automation side to avoid problems related to system component failure. Suitable firewall or gateway functions (red boxes) are inserted to avoid that any failure in or attack on external systems propagate back to the more critical components.

It is also possible to duplicate the Autonomous Ship Controller (ASC) function, but this is complicated as it also requires synchronized update of state in the two redundant functional units. Although additional robustness can be achieved by doing this, the complexity of synchronization could in itself introduce more failure modes in the system and possibly make it more error prone. A reasonable alternative is to make the ASC able to restart itself so that it can shut itself down and restart in case of internal problems. As power supply failures are relatively common, the ASC should be supplied with two independent power sources.

Using the single point of failure paradigm, it is only the ASC itself that is left as a critical component. Using well tried hardware components and good software practices, the probability of an unrecoverable error should be relatively low.

To add to overall system robustness and fail to safe capabilities, one should also make the Rendezvous Control Unit (RCU) independent of the ASC. The RCU should also be able to switch the ASC off when a rendezvous operation is started. The RCU should also be directly connected to the radio receiver system used for rendezvous communication.

7.4 Shore systems failure modes

One assumption in MUNIN is that the shore control centre (SCC) can be located in different places and even time zones, e.g. to avoid using night shifts in a single SCC. This concept will also provide a high level of redundancy for the SCC as the function can be geographically moved in the case of problems in one location. There is obvious safety and legislative issues related to the actual movement of control from one SCC to another, but this can be done by use of communications means other than what is being used for control of the ship, e.g. mobile or fixed telephone lines. Thus, the safety problems are limited to establishing operational procedures that ensure safe transfer of control in cases where one SCC is unable to perform its function.

The procedures can also be enhanced with technical means by which the ASC itself changes to the next SCC when it loses contact with the primary SCC. Note that this requires that two or more SCC are operational at all times.

Thus, no further safety analysis will be done for the SCC. A special scenario will be added to handle the automatic transfer from primary to secondary SCC.

8. Security issues

8.1 Overview

This section contains material that has previously been published in the Flagship report /2/ Security is important in all communication. Insertion of wrong data in a communication stream may cause serious accidents as well as commercial, contractual or legal problems. Denial of service can inhibit critical information from reaching its destination and breach of confidentiality can likewise be used to cause accidents or for fraud. Three types of security issues will be discussed in the following:

- *Confidentiality:* This is the absence of unauthorized disclosure of information. For personal communication and business communications, confidentiality is of high importance.
- *Integrity:* This is the absence of improper system alteration. For communication systems, this may be malign or accidental insertion of false data or corruption of data.
- *Denial of service (DOS):* This is the possibility of an attack on components of the communication system that inhibits the use of the system to exchange data.

Wireless communication and communication over the Internet is particularly sensitive to security problems of the types mentioned above. Thus, this analysis will briefly point at some security issues that are related to these data carriers.

8.2 Overview of security level of some services

Table 9 lists a summary of security levels for some relevant carrier types. A brief discussion can be found below

Table 9 – Indicative security quality classification for the carriers

Carrier	Confidentiality	Integrity	Denial of service
Inmarsat	Medium	Medium	Medium
VSAT	Medium	Medium	Medium
Iridium OpenPort	High	High	High
AIS	Low	Low	Low
Digital VHF	Low	Low	Low
WiMAX/LTE	High	High	Medium
GSM 3G-4G	High	High	Medium

The security quality classification shown in Table 9 should be taken as indicative. Most of the carriers allow different protocols and access mechanisms to be used and by that impact the security level.

Briefly, the background for the classification is:

- *Inmarsat:* Ordinary Inmarsat transmissions are relatively easy to intercept, fake or jam. Inmarsat BGAN uses a combination of Time Division Multiple Access (TDMA) and Frequency Division Multiplexing (FDM). This allows hostile parties to intercept or influence transmission with relatively simple means. Use of encryption on the transmitted signal will overcome the first two issues, but the ground station and the signal up to the satellite can still be disturbed. Radio Technical Commission for Aeronautics (RTCA) does not currently accept Inmarsat for safety critical communication, but is working on certification /23/.
- *VSAT*: The same security issues as for Inmarsat apply. One may expect that newer solutions for satellite communication employ better security mechanisms, such as spread spectrum or frequency hopping, but this is still not the case for most commercial services.
- *Iridium OpenPort*: Iridium uses a very complex signalling mechanism as well as encryption and ground station authentication /7/. Also, the overall complexity of the system makes it difficult to manipulate.
- *AIS*: In its current implementation, AIS is open to all types of attacks. It also uses an omnidirectional antenna that is very easy to jam.
- *Digital VHF*: The transmission protocol is open and does not currently implement any security mechanisms. Thus, it is vulnerable to security attacks on the same level as AIS.
- *WiMAX*: This system has fairly advanced protocols with high security levels. However, common use of Internet as backhaul opens connections for hostile attacks on the land side. Omnidirectional antennas may also be susceptible to jamming attempts.
- *GSM networks, 3G and 4G*: These are difficult to eavesdrop or insert messages into, but the physical infrastructure may be attacked and destroyed. Some redundancy can be achieved by using different networks, but they may not be completely independent if they use some common infrastructure.

In general, this discussion only point at the fact that the user of such communication systems need to consider what attacks it is necessary to protect against, if any. Some mechanisms are already in place if implemented properly and others can be added on by using application layer mechanisms.

8.3 Possible remedial actions

Once the ship is connected to the shore, whatever technology or protocol is used, the ship has to be protected from potential attacks via the communication facilities. If this is not handled by the basic communication system as discussed in the previous section, one needs to install specific security systems that provide protection. While voice calls typically are connections switched via specialised data channels and do not generally represent a problem, this is different for data streams that go via the open Internet. In such cases one will typically provide a tired protection system as shown in Figure 7 /32/.

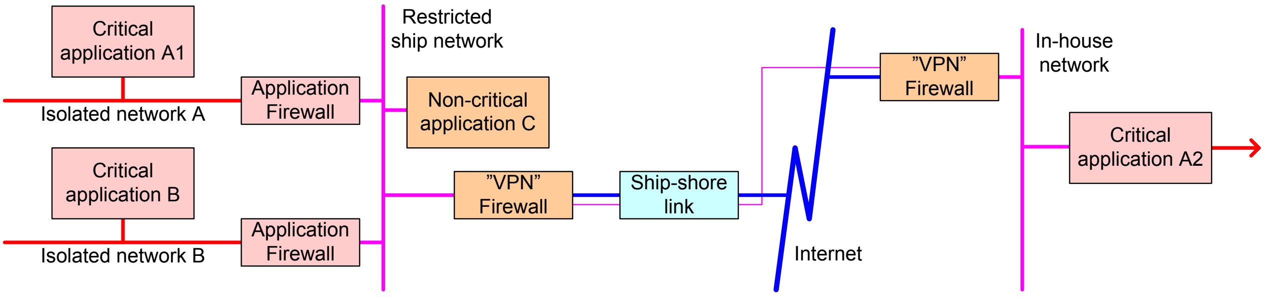


Figure 7 – Typical security implementation

Essential services (A or B) are directly connected to physically isolated networks, possibly with an application level firewall to the ship wide network. Only information that is explicitly made available by the application firewall can be reached from the restricted ship network. This is the first protection level.

Non-essential services are directly connected to the restricted ship wide network (C), servers as well clients, for performance reasons.

The second protection level is between the restricted ship network and the shore. Firewalls and gateways will be used to segregate these two worlds. These systems are confidential to each ship or fleet. In some cases, e.g. for maintenance, a pipe can be opened between the ship and the supplier who wants to access the system, but always for a small period and with login and password that are not reused afterwards.

The third protection level is between shore and shore. Ship owners request from their communication provider a private network (e.g. Virtual Private Network – VPN or a circuit switched line) between the ship and their shore office. It is not possible to access the ship directly through the general communication provider. Any supplier that need to access the ship shall connect first to the ship owner's shore office and only after that, the supplier can connect to the relevant application on the ship, normally through a dedicated VPN connection. The shore office has also, of course, firewall and gateways to protect them from outside intrusions.

This setup allows the owner easy access to the applications that export interfaces through the three levels of protection. However, this may reduce the available bandwidth in some cases. For third parties, e.g. equipment manufacturers, the access is significantly more cumbersome as several steps and possibly manual intervention is required. However, this depends on the level of trust between the third party and the owner. VPN access may in some cases be granted on a permanent basis.

8.4 Other security issues

As long as the on board systems and networks are dedicated to specific applications and are stand-alone, the only way to access them is locally on board the ship and normally only in controlled areas of the ship. With the progress of new technologies and in particular in networking, the systems now tend to be connected to or reside as part of a larger restricted network on the ship. This trend can be expected to continue with even more systems being connected to the restricted network and new links from the restricted network to shore.

Also, increasing levels of complexity and less crew on-board make more owners delegate the maintenance and management of networks and applications to third parties or to the manufacturers themselves. Consequently, systems that used to be stand alone and isolated inside the ship are now network based and are connected through the Internet to the shore. This opens up possibilities for hostile attacks, e.g. from hackers, but it also causes potential safety problems with regards to misunderstandings or bad decisions inside the owner's office or by other parties that have legal access to the systems.

Furthermore, ship systems and networks are normally not constructed by one party alone. On most ships, there is no IT department that manages network equipment and connections and the systems have in many cases been delivered and commissioned by different parties during the ship's building process. During the life time of the ship, systems and networks will be upgraded and exchanged several times. This adds to the problem of maintaining the complete network infrastructure. A virus or other mal-ware in the office is a great problem, on a ship it may lead to a serious accident.

On the other hand, developments on shore with respect to centralization and virtualization may also be implemented on ships. However, this causes new problems. Safety principles and also general business processes are currently based on each supplier having full responsibility for the delivery, including network, computers and software. With more distributed or integrated systems, this principle has to change and this will require updates in business practices as well as in rules and legislation. For the owner and yard it will also present new problems in terms of guarantees and maintenance.

8.5 Security of GNSS systems

A special warning should be made related to the availability of global navigation satellite systems such as GPS, GALILEO and GLONASS. As receivers are dependent on low signal levels and use omnidirectional antennas, it is relatively easy to jam reception of the satellite systems and possibly also inserting wrong data to the receiver /24/. Incidents where GPS reception has been inhibited in large areas have also been reported /25/ To address this, MUNIN will develop test scenarios where GNSS failures are included.

8.6 Summary of security requirements

Communication requirements are summarised in Table 3 in section 3.2. A brief conclusion is given below.

The rendezvous communication link is particularly sensitive and needs a high security level. This should include protection against jamming, but particularly against malicious insertion of control messages. This stream is particularly important as the connection probably needs to be based on unreliable message passing and cannot use low level connection oriented protocols.

The remote control stream is very critical and must have sufficient security measures in place. Most critical is also here the possibility of malicious insertion of control commands. Telemetry and radar and targets are also critical, but not to same degree. The use of secure and connection oriented communication lines should be a good solution. The use of Iridium as backup to a more conventional VSAT or Inmarsat system should provide a good solution.

9. Protocol impact on communication quality

9.1 Types of communication

Without going into details on all of the different available communication types, Table 10 lists five that can be said to be commonly used and their corresponding Internet Protocols (IP). Three of these types are expected to be made available to the MUNIN software modules as four different services (see Table 5 in section 3.5). The possible set of types represents permutations of the following properties of communication:

- *Reliable/unreliable*: This specifies if the data sent can be relied on being delivered to the recipient, without doing application level checking and retransmission. The protocol takes care of all aspects and will only notify sender if the delivery could not be completed.
- *Stream/message*: Stream data represent data streams, e.g. voice or video. It may also be the transfer of a large file, where the file itself does not contain records or other structures visible to the protocol layer. Messages are all other transfers, where each transmission is relatively short and consists of one record or block of data.
- *Uni-, multi- or broadcast*: This tells if there is one, a limited group of or many recipients to one data transmission.

Other permutations than the ones listed below are rarely used, either for practical or technical reasons.

Table 10 – Overview of common communication services

Service type	IP protocol	Description
Reliable stream	TCP/IP	Point to point data stream, e.g. file, sound, video.
Unreliable message	UDP unicast	Point to point delimited messages, not guaranteed delivery.
Reliable message	TCP/IP or UDP based	Point to point delimited messages with guaranteed delivery and sequencing.
Unreliable multicast message	UDP multi/broadcast	One-to-many unreliable distribution of messages.
Reliable multicast message	UDP or TCP/IP	One-to-many distribution of messages with guaranteed sequence and delivery.

The protocols that are listed are from the Internet Protocol (IP) suite and indicate what protocols are typically used to implement these services. Note that IP also includes other protocols that may more directly implement the services in question, but these are not commonly used in general purpose control applications. Thus, while an Internet protocol such as Pragmatic General Multicast (PGM) /3/ can implement reliable multicast messaging, in practice it is often implemented by a simpler application layer mechanism on top of UDP or TCP/IP.

Also, if one looks at special purpose protocols outside the IP suite, particularly in the real time or safety critical domains, there are wide selections of special protocols available, both for wired and wireless communication. For the purpose of MUNIN, we will need to rely on off-the-shelf computer systems and satellite communication services and the use of IP is in practical terms a necessity for many of these.

9.2 Remote state and distributed applications

A significant problem with distributed systems is to maintain correct information about the state of other units in the system. An example from an autonomous ship would be for the shore station to exactly know what state the ship is operating in, e.g. after a remote control command has been sent to the ship.

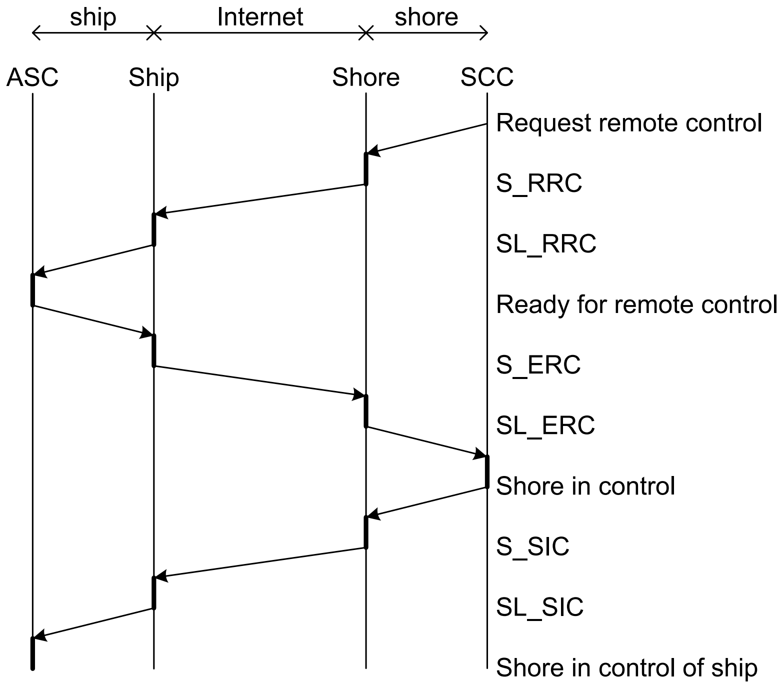


Figure 8 – Three way handshake for remote control

As can be seen in Figure 8, in general a three way handshake is necessary to ensure that the ship and the shore control centre is in agreement of who is in control. If any message is lost, either on shore, in the transmission through the networks or on the ship, the sender has to try again and retransmit from the last confirmed state. This retransmission principle effectively implements a guarantee for delivery of messages. If the link is reliable, i.e. the transmission system guarantees delivery of the messages, one will in most cases be able to drop the last third of the handshake. The second handshake is still necessary to ensure that the ship application layer responded correctly to the request for remote control. This is discussed further in the next section.

If retransmission fails to set or update the state, the two parties have to assume that there is no connection between the systems and that corresponding measures must be taken. This will typically be to enter some form of fail to safe mode or an increased level of autonomy.

The figure shows this exchange of messages where the parties to the communication are the ASC, the ship communication protocol layer, the shore communication services and the SCC. The link between ship and shore will look like an Internet connection and it will normally be operated over a satellite communication link.

For each data exchange of this type there are basically two different and generally independent problems:

1. Ensure that both sides are aware of the actual state of each other. This requires a three way handshake if the data link is unreliable and normally a two way handshake if the transmission is reliable.
2. Detect loss of communication between the two parties so that appropriate measures can be taken on both sides.

If unreliable communication is used, these two functions have to be catered for in all message exchanges. This is an argument for using a reliable communication paradigm and separating the two functions in the application layer (function 1) and in the communication layer (function 2).

9.3 Connection oriented or connection-less

If the transmission system is connection oriented, i.e. it keeps track of the liveness of the communication link and guarantees the delivery of messages as long as the link is active, the applications can be much simplified by monitoring link liveness separately from the details of message passing.

Table 11 – Main ship states

Connection	Application ack.	State	Action
Ok	Ok	On line and ok	Run normally
Ok	Not ok	Application dead	Restart
Not ok	n/a	Off line	Autonomous/FTS

This is summarized in Table 11. This is also the principle used in the MUNIN system software architecture described in section 10.1: The system level will keep track of communication status and the applications will normally use reliable and connection oriented messaging for exchanges between shore and ship.

9.4 Failure modes and connection oriented communication

Generally, failure modes in communication systems are as shown in Table 12 which is based on the general classification in EN 50159-1 /4/

Table 12 – General communication failure modes

Threat	**Explanation**	**Connection**
Repetition	Duplication, replication or babbling	Ok
Deletion	All or part of message	(Ok)
Insertion	Incorrect data, from other source	Ok
Wrong sequence	Switched order	Ok
Corruption	Wrong contents	Ok
Delay	Latency too long	
Masquerade	Wrong sender, authentication errors	(Ok)

A connection oriented protocol like TCP/IP will avoid most of these problems as the protocol itself makes sure that messages are correct and delivered in the correct order. This is done by using fairly solid check-summing and sequence numbering. While the TCP/IP checksum is only a 16 bit CRC, it also makes use of lower layer checksum mechanisms that together are strong enough for our purposes. There is obviously a small chance that the protocol software itself fails, but this is a standard and well proven protocol that is extremely unlikely to fail in any of these modes. The modes that remain relevant for a TCP/IP data link are the following:

- *Deletion:* A physical problem on the data link may cause the link to be broken and messages to be lost. However, the link break event can easily be detected and the application can do corrective actions. It is not possible that a part of the transmission disappears unnoticed, unless from a malicious intervention.
- *Delay:* This is a problem that cannot be avoided and will be discussed below. In addition to the transmission delays themselves, also packet loss will manifest itself as delays as retransmissions are necessary.
- *Masquerade:* This problem applies to link establishment, but can also be caused by malicious intervention in the communication system.

For UDP, most of the tabulated failure modes are possible. Corruption can be avoided by use of mandatory UDP checksums, but all other modes are relevant. UDP is defined as an unreliable protocol and these effects can be caused by protocol mechanisms as well as physical link layer issues.

9.5 Effect of link layer QoS on performance of TCP/IP

TCP/IP – Transmission Control Protocol/Internet Protocol – /16/ is probably the most common connection oriented protocol used in modern computing. This section will demonstrate with a few examples how changes in QoS attributes on the link layer impact the performance of TCP/IP. This analysis will also in general apply to other reliable transmission protocols, whether they are implemented in the application layer as a three way handshake or in the transmission protocol as in TCP/IP.

The main problem is that reliable protocols require a form of handshake between sender and receiver to verify that data have been received correctly. In TCP/IP this is done as illustrated in Figure 9.

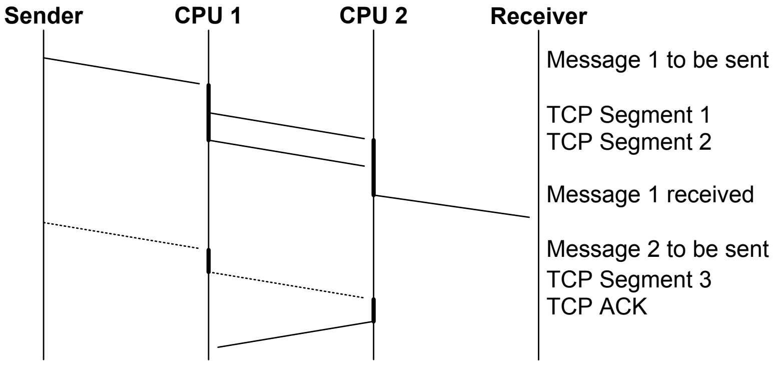


Figure 9 – TCP/IP Sequence diagram

When the sender requests the transmission of a message, this message will be divided into one or more segments and transmitted over the physical medium to the receiver computer. The physical medium will limit the size of each segment to the "maximum transmission unit" (MTU) and this may require the message to be divided into segments.

The TCP/IP protocol also operates with a transmission window that determines how many bytes can be sent before the receiver must acknowledge received data with an ACK message. This will also limit how much non-acknowledged data the sender will send before it will stop transmissions and wait for the ACK. This is illustrated in Figure 9 where the ACK is sent when a full window is received, after the third segment. Note that the messages sent by the sender may be shorter than the window size as in this case, but this will normally not impact response times in the system.

The window size will have an important effect on throughput on slow data transmission lines as shown in Eq. 2.

$$c_{eff}=c_{bps}\frac{8w_{byte}}{2t_{lat}c_{bps}+8w_{byte}} \qquad \text{(Eq. 2)}$$

The reason is that the round trip delay for the acknowledgement is dependent on the product of latency and bandwidth as well as the size of the window and that the latency dominates for small window sizes. As window size w_{byte} increases, the effective bit rate c_{eff} will go towards the nominal bitrate c_{bps} (bits per second here). This translates to the data listed in Table 13 when a latency of 0,6 seconds and a nominal bandwidth of 128 kbps is used, which has been reported for Iridium /15/

Table 13 – Effective bandwidth as function of window size in TCP/IP

Window size (byte)	Retransmit delay (s)	Effective bandwidth (kbps)
32000	5,8	80
16000	3,8	58
8000	2,8	38
4000	2,3	22

The retransmit delay column lists the worst case time it takes to transmit and retransmit a lost segment or message. It is the delay from sending a start of a window until the missing acknowledgement is detected and then for a new window of outstanding data to be sent. For normal transmissions without retransmissions this is of relatively little consequence as the delay experienced by the receiver is independent of this value: The receiver protocol stack will pass data from the receive buffer to the application as soon as it arrives. This gives a delay as described in Eq. 1, which is somewhat higher than the nominal latency.

For throughput, the higher retransmit delay for large windows will normally be less negative than the positive effect on increased bandwidths, except for very high bit error rates (BER). For the examples shown here, a BER of 10^{-6} or higher will make it necessary to reduce window sizes to below 16000 bytes to optimize bandwidth. In all other cases, the higher bandwidth achieved with larger windows will still make large windows more efficient.

Another and more severe problem occurs for time critical communication where occasional packet loss makes retransmission necessary. If this is common, longer windows will increase the maximum message transmission delay which may be critical for some applications.

The window size is also used for flow control in TCP/IP so there are also other mechanisms to consider when determining the best window size. Note also that the window is not normally changeable from software. Changing the protocol stack receive and send buffer sizes will normally also change the maximum window size.

A more relevant approach for MUNIN for time critical messaging is to consider using UDP with a simpler retransmit mechanism. This could, e.g. be to send immediate negative acknowledgements when missing messages are detected and send positive acknowledgements only each 5 seconds to verify that the data link is still open.

9.6 Other parameter setting in TCP/IP

When using TCP/IP for time critical communication one will normally want to turn buffering of outgoing messages off. Normally, TCP/IP will buffer data to get a better utilization of the bandwidth, but this introduces delays in time critical communication.

10. Outline of system service layer

10.1 General ship software architecture

The general software architecture is illustrated in Figure 10. This architecture is intended for use on board the ship. The shore side architecture will probably not provide the same services as discussed here (see next sub-section).

All application programs (Application 1 to N) will perform its part of the overall autonomous control and monitoring function in cooperation with each other, exchanging data as needed. Data exchanges may be done via direct calls, message passing or shared databases. These specifications must be agreed upon between the application programs themselves.

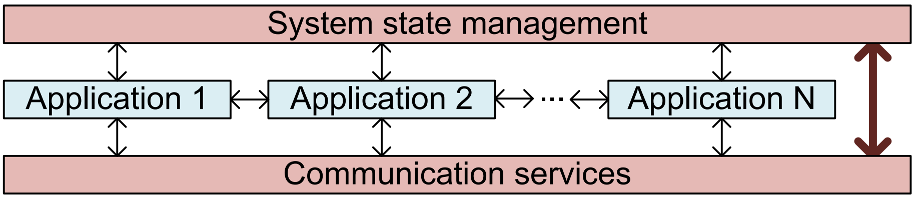


Figure 10 – System software architecture

The application program will also be interfaced to the system levels through the following services:

- *System state change:* The applications will be automatically notified by the system layer if the state of one of the application modules changes, i.e. that functionality provided by module is reduced or incremented. This may include going to a fail to safe mode or that the autonomous ship controller needs to reduce speed or engine power. The application modules must check the details of the reduced or increased functionality itself to determine if the change has any effect on own operations.

- *Communication state change:* Any change in communication capabilities will be immediately notified to the application programs. Details on available services and quality will be transmitted in the notification.

- *Application state change:* The application module must notify the system level of any changes in own capabilities. This will be used to update and transmit system status.

- *Data read and write:* Services will be available to send and receive data to and from other ships or shore. Different services may be implemented for the different communication types defined in section 3.5.

10.2 General shore software architecture

Currently, the assumption is that the shore system will be made more ad hoc than the ship system and that no specific architecture is needed there. This assumption will be revisited in deliverable D4.4, and if necessary, a similar structure will also be defined for the shore.

10.3 Application program identities

Each application program will be assigned an identity code that will be used in communication between application programs and between system and application modules. The number of modules and identity codes will be determined in D4.4.

10.4 Communication stream identities

Each application module may use one or more data streams to communicate with the shore system. Each stream will be assigned a priority, bandwidth and QoS requirement for normal and backup operation. This will be used by the communication services to prioritize and manage traffic.

References

/1/ ETSI (2010) European Standard (Telecommunications series), Intelligent Transport Systems (ITS); Communications Architecture. ETSI EN 302 665 V1.1.1 (2010-09).

/2/ Rødseth Ø.J., Kvamstad B., Tjora Å., Drezet F. (2009). Ship-shore communication requirements, Flagship Deliverable D-D1.3, 31st December 2009. EU Project contract number TIP5-CT-2006-031406. http://www.mits-forum.org/communication.html.

/3/ Speakman T. et al. Internet Society RFC 3208 (December 2001). Pragmatic General Multicast (PGM) - Reliable Transport Protocol.

/4/ EN 50159-1:2001, Railway applications - Communication, signalling and processing systems - Part 1: Safety-related communication in closed transmission systems.

/5/ ITU-T Recommendation G.1010, Series G: Transmission Systems and Media, Digital Systems and Networks, Quality of service and performance, End-user multimedia QoS categories, 2001.

/6/ ICAO Technical Manual for Iridium Aeronautical Mobile Satellite (Route) Service, Draft v1.1, 19 May 2006.

/7/ SATCOM Availability Analysis, ICAO Working Group M, Iridium Subgroup, August 23 2006 (Power point presentation).

/8/ CNS/MET SG/15 - WP/40, International Civil Aviation Organization, Fifteenth meeting of the communications/navigation/surveillance and meteorology sub-group (CNS/MET SG/15) of Apanpirg, Bangkok, Thailand, 25 – 29 July 2011.

/9/ Seo J., Walter T., Chiou T., Blanch J., Enge P. Evaluation of Deep Signal Fading Effects Due to Ionospheric Scintillation on GPS Aviation Receivers, Institute of Navigation GNSS 2008, 16-19 September 2008, Savannah, GA.

/10/ Raya S. and DasGupta A., Geostationary L-band signal scintillation observations near the crest of equatorial anomaly in the Indian zone, Journal of Atmospheric and Solar-Terrestrial Physics, Volume 69, Issues 4-5, April 2007.

/11/ Crowe K. E., A comparative analysis of the Iridium and Globalstar Satellite transmission paths, Thesis AFIT 1999.

/12/ Frost & Sullivan's February 2007 LEO Satellite Telephone Quality of Service Comparison.

/13/ Pratt T., Bostian C., Allnutt J., Satellite Communication, second edition, 2002.

/14/ Rødseth Ø.J., Christensen M.J.; Lee K., Design challenges and decisions for a new ship data network, ISIS 2011, Hamburg, 15th to 16th September 2011.

/15/ Stehle R., GPS Trackers & Iridium OpenPort, Polar Technology Conference, Boulder, CO, 25 & 26 March 2010.

/16/ IETF Network Working Group, Request for Comments 675: Specification of Internet Transmission Control Program, December 1974.

/17/ RTCA DO-270, Minimum Aviation System Performance Standards (MASPS) for the Aeronautical Mobile-Satellite (R) Service (AMS(R)S) as Used in Aeronautical Data Links, for requirement and specification for the data link.

/18/ IEEE Standard 521-2002 Standard Letter Designations for Radar-Frequency Bands.

/19/ Recommendation ITU-R M.1842, Characteristics of VHF radio systems and equipment for the exchange of data and electronic mail in the maritime mobile service RR Appendix 18 channels, January 2008.

/20/ Recommendation ITU-R M.493-11, Digital selective-calling system for use in the maritime mobile service, edition 2004.

/21/ Report ITU-R M.2171, Characteristics of unmanned aircraft systems and spectrum requirements to support their safe operation in non-segregated airspace, 12/2009.

/22/ Report ITU-R M.2233, Examples of technical characteristics for unmanned aircraft control and non-payload communications links, 11/2011.

/23/ RTCA 2011 Annual Report.

/24/ NAV 57/6/4, Resilient Position, Navigation and Timing (PNT), Submitted by IALA, 8 April 2011.

/25/ NAV 57/6/2, Need of reliable position-fixing system in view of GNSS signal failure case, Submitted by the Republic of Korea, 4 April 2011.

/26/ ITU series of reports and recommendations on the International Mobile Telecommunications-2000 (IMT-2000) system (see, e.g. www.imt-2000.org).

/27/ ITU series of reports and recommendations on IMT-Advanced: Mobile telecommunication services beyond IMT-2000 (see, e.g. www.imt-2000.org).

/28/ IEEE 802.16-2009, Air Interface for Fixed and Mobile Broadband Wireless Access System.

/29/ IEEE 802.15.4-2011, Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).

/30/ Annex 26 to Working Party 5B Chairman's Report, Working Document Toward a Preliminary Draft, New Report ITU-R M. [MAR-UMS], Characteristics of unmanned maritime systems.

/31/ ICAO DO-270, Minimum Aviation System Performance Standards (MASPS) for the Aeronautical Mobile-Satellite (R) Service (AMS(R)S) as Used in Aeronautical Data Links.

/32/ IEC 61162-450 ed1.0, Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 450: Multiple talkers and multiple listeners - Ethernet interconnection.