D2.10 Recommended on-board network Architecture

Project no.	636329
Project acronym:	EfficienSea2
	EFFICIENSEA2 – efficient, safe and sustainable traffic at sea
Funding scheme:	Innovation Action (IA)
Start date of project:	1 May 2015
End date of project:	30 April 2018
Duration:	36 months
Due date of deliverable:	25 April 2016
Actual submission date:	
Revised submission date:	-
Organisation in charge of deliverable:	Partner 21, DANELEC

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

DOCUMENT STATUS

Authors and contributors

Name	Organisation
Henrik Bech Helnæs (editor)	Danelec Marine
Erik Styhr Petersen	Wärtsilä
Anders Rydlinger	Transas
Timo Kostiainen	Furuno
Peter Andersen	Cobham

Document History

Version	Date	Initials	Description
0.1	2015-09-09	HBH	First Draft
0.2	2015-10-01	HBH	Second Draft
0.7	2015-12-01	HBH	Updated with 10% review changes
0.9	2016-03-18	HBH	Final Draft for review
0.91	2016-04-20	HBH	Final Draft for review meeting
1.0	2016-04-25	HBH	Final Report

Reviewers

Name	Organisation
Andy Winbow	CIRM
Hannu Peiponen	Furuno
Krzysztof Bronk	NIT
Jens Kristian Jensen	DMA

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

Contents

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

1 Summary

This report constitutes deliverable D2.10 in the EfficienSea2 project. It describes the on-board system integration architecture. The architecture is integrating the EfficienSea2 Task 2.3 Seamless Roaming function, the Maritime Cloud Client Component (MCC), the on-board part of the Maritime Cloud (MC), and the EfficienSea2 Task 2.1 VHF Data Exchange System (VDES).
The report use the user needs described in (E2-T3.1, Analysis report on communication and infrastructure, 2015) combined with analysis of the services specified in the Maritime Service Portfolio and proposes a set of requirements for the architecture.
Based on the proposed requirements, the report suggests an on-board architecture.
The methodology used, is the (ISO/IEC42010, 2011)

2 Introduction

Integration of equipment in on-board networks taking cyber security into account is a key element in providing the shipboard component of the maritime cloud. The scope of this report is to provide the first step in analysing the available on-board components, existing network standards, and installation trends, to form a recommendation on the network architecture to be used.

In collaboration with Work Package 3, input is provided towards the definition of a harmonized on-board architecture, which, while respecting the current type approval regime, whether by IMO and IEC instruments, or by Class, will promote the integration of interoperable radio communication devices with today's and tomorrow's navigation systems, automation systems and other electronic data processing systems in a reliable and safe manner, using intelligent network controllers to separate the networks.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

3 Definitions and Acronyms

AE	Architectural Element
AIS	Automatic Identification System (IEC 62320:2008)
ASM	Application Specific Messaging
DMZ	Demilitarised Zone
DOS	Denial Of Service
E2	EfficienSea2
ECDIS	Electronic Chart Display and Information System (IEC 61174:2015)
FW	Firewall
GPS	Global Positioning System
GW	Gateway
ICS	Integrated Communication System
LOS	Loss of Service
MC	Maritime Cloud
MCC	Maritime Cloud Client Component
MMS	Maritime Messaging Service
MSP	Maritime Service Portfolio
QoS	Quality of Service
RADAR	RAdio Detection And Ranging (IEC 62388:2013)
SOLAS	Safety of Life at Sea (SOLAS Convention, 1974, with amendments)
VDE	VHF Data Exchange
VDES	VHF Data Exchange System
VDR	Voyage Data Recorder (IEC 61996:2013)
VTS	Vessel Traffic Service
Wi-Fi	a trademark of the Wi-Fi alliance (WLAN or Wireless Local Area Network)

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

4 Methodology

Due to the rules and regulations in the maritime domain, one cannot immediately consider the entire electronic infrastructure of a ship to be a subsystem of the maritime cloud; this kind of thinking is required to be limited to the novel part of the shipboard architecture which binds the Maritime Cloud Client Component (MCC) to the existing type approved systems. This being stated, however, it is reasonable to suggest that the novel parts of the architecture must be proven (tested) to be a valid part of the architecture of the maritime cloud and as such support fulfilment of requirements to the maritime cloud.

To support future validation of the on-board MCC and to provide a description that is using a recognized way to describe the on-board architecture. This work producing this report has used the standard: (ISO/IEC42010, 2011) Systems and Software engineering – Architecture Description.

Literature supporting the standard is (Rozanski & Woods, 2013).

Grounded in this standard, the descriptions in this document make use of the concepts: Stakeholders, Concerns, Viewpoints and Perspectives.
The process to follow and the steps taken to provide a recommended architecture is illustrated in Figure 1.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

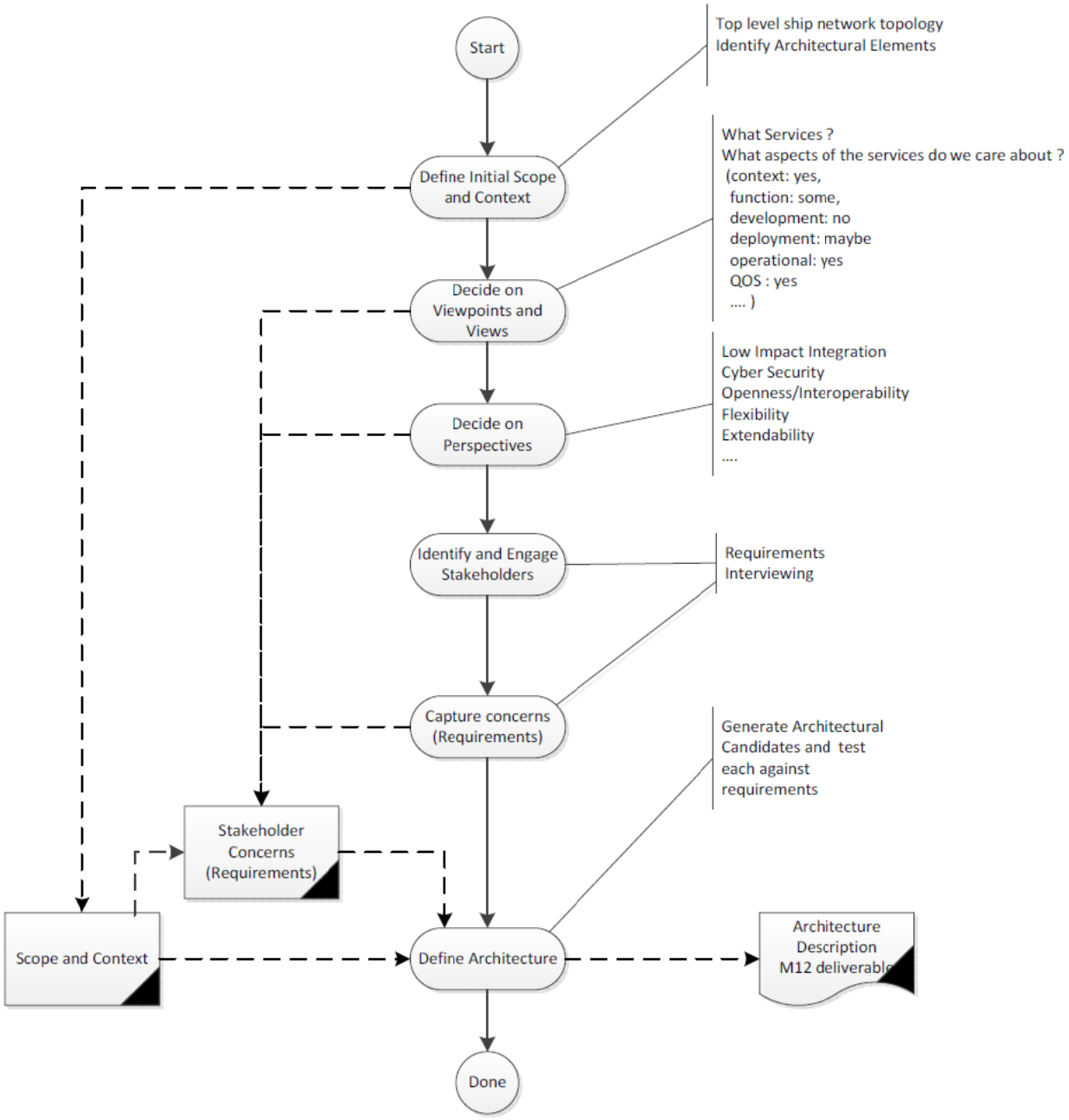

Figure 1 Process to follow to produce recommended architecture

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

5 Scope and Context

5.1 Introduction

By today (2015), in rough numbers, there are approximately 63.000 SOLAS ships in the global fleet. Commercial experts in the maritime domain expect a growth rate of 2% per annum. Assuming a service life of, say, 30 years, some 3.000 ships are being built every year to balance scrapping and to provide the expected growth. While some of these ships are small and intended for local trading, each of the remaining part of these new ships – perhaps 2.000 per year – is a potential target for the Maritime Cloud (MC). However, the MC should not be something which just new ships will benefit from; if that was the case, the MC implementation rate would be too low, and, correspondingly, the timespan to reach 'critical mass' would be too long, unnecessarily postponing the day where the maritime safety and efficiency would improve because of the MC. Thus, both conceptually and in practical terms, the MC must also apply to the existing fleet and future builds in order to fulfil its potential.

This real-world impact on the MC, its function, characteristics and architecture, should hence not be underestimated: unless the MC, and especially its on-board Maritime Cloud Component (MCC), from every relevant vantage point is fundamentally compatible with the existing rules, regulations, equipment and culture of commercial shipbuilding, ship operations and maritime equipment manufacturing, it is less likely to become the success it could be.
Lack of such compatibility could even turn out to be an unsurmountable barrier to implementation beyond limited testing in isolated geographical areas, causing the demise of the MC even before it goes beyond an embryonic state.

The approach chosen in the work reported in this document reflects this understanding, the fundamental thesis being that the MCC, as a result of the arguments presented, necessarily must be an add-on to existing ship systems and instrumentation infrastructure, in full respect of their present function and entirely aligned to the present set of relevant rules. While this may seem as a constraint from some perspectives, it however also has positive side-effects, one being that previous work on ship systems, ship infrastructures and integrated ship control system architectures is suitable as a foundation for the work with the MCC. Indeed, as a direct result of this line of thinking, it must be possible to describe the MCC within the framework of existing reference models of ships and ships equipment – if not, then the compatibility of the MCC to the present world is probably incomplete.

5.2 Background

5.2.1 The Heritage

From the early 1990s, to the middle of the first decade of 2000, two research projects in particular focused on on-board infrastructures and control systems, one being the

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

ATOMOS Consortium (ATOMOS, 1994; ATOMOS II, 2000; ATOMOS IV, 2002), and the other one being the MiTS Forum (The MiTS Forum, 2015). These two groups moreover cooperated on bringing forward a common suggested standard for Integrated Ship Control infrastructures and integration mechanisms, joining forces in the two DISC projects (DISC, 2001; DISC II). Directly applicable to the matter at hand, part of the work in the original DISC project aimed at providing a common understanding of integrated ship control systems – or, in other words, Architectural Descriptions (AD), as this term is used by (ISO/IEC42010, 2011).
One such AD is shown in Figure 2, which introduces a three-layer abstraction pyramid, grouping physical shipboard devices into (from bottom to top) sensors and actuators, components and a generic group, each being defined as follows (edited from (DISC, 1997)):

- The 'Generic' level contains information pertaining to the ship as an entity, e.g., position, speed, heading, destination, name of the ship, general machinery condition etc., but the generic layer also contains generic functions such as navigation and propulsion control etc.
- The 'Component' level contains ship specific details that are not possible to generalise, i.e. information that is defined by the specific configuration of the ship and the corresponding implementation of the systems being considered as part of the abstraction pyramid.
- At the lowest level, which is the 'Level of Sensors and Actuators', such devices are described with a relatively low number of variants, e.g., valves can be generalised into 5 to 10 groups. Therefore, similarly to what was the case at the generic level, standardized modelling is possible at this level.

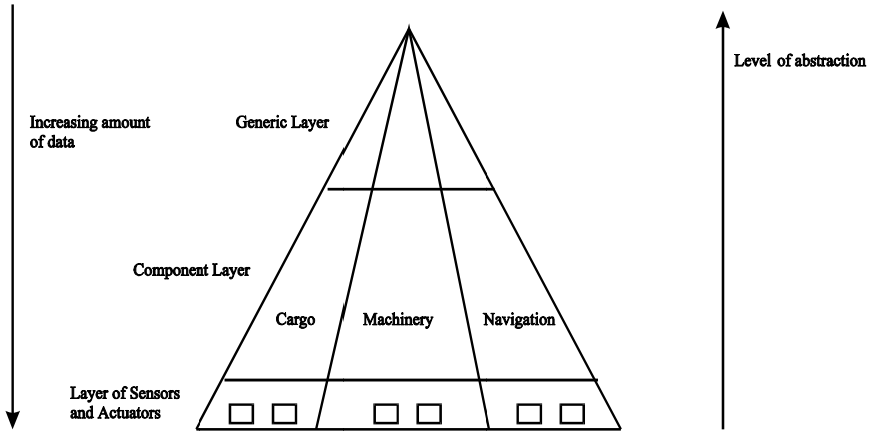

Figure 2 - Abstraction of the DISC ISC-System, from (DISC, 1997)

The thinking expressed in the original DISC ISC abstraction pyramid is reflected in later, and perhaps more refined and evolved Architectural Descriptions of Integrated Ship Control systems. One such example comes from (Rødseth, Christensen, & Lee), where the three original DISC layers are expanded to five. While the two concepts are quite

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

similar in many respects, it should however be noted that the latter AD focuses on interconnectivity; in the (Rødseth, Christensen, & Lee) terminology, 'Layer' thus means the interconnection between devices, rather than the DISC (1997) model definition, where 'Layer' is broader in its definition, and does not explicitly differ between devices and interconnections. The horizontal lines in the DISC AD however imply that there are electrical connections between the three layers.

With the definition above in mind, (Rødseth, Christensen, & Lee) describes five layers, from 'bottom' to 'top', as follows:

- 'Instrument Layer' – which defines the interconnection between sensors and the higher-level applications that utilizes the information provided, and in some cases commands devices at the bottom of the 'Instrument Layer', Conceptually, this layer seems to be close to, or even identical with, the DISC (1997) 'Layer of Sensors and Actuators';
- 'Process Layer' – which appears to be similar to the 'Component Layer' in the DISC (1997) abstraction pyramid, but where a closer scrutiny probably would reveal a divergence between the two mentioned models with respect to layers 2 and 3;
- 'Integrated Ship Control (ISC) Layer' – which is seen as being similar in purpose to the DISC (1997) 'Generic Layer';
- 'General Ship Layer' – which combines top-level, ship-wide functions with entities which are irrelevant to ISC, but which are sensible to consider in the context of the present work, like infotainment networks and shipboard administration;
- 'Off-ship Layer' – which, for all practical purposes, encompasses the functions one would come to consider as part of the ship-shore communications solutions of today, supplemented with the facilities and services offered by the MC.

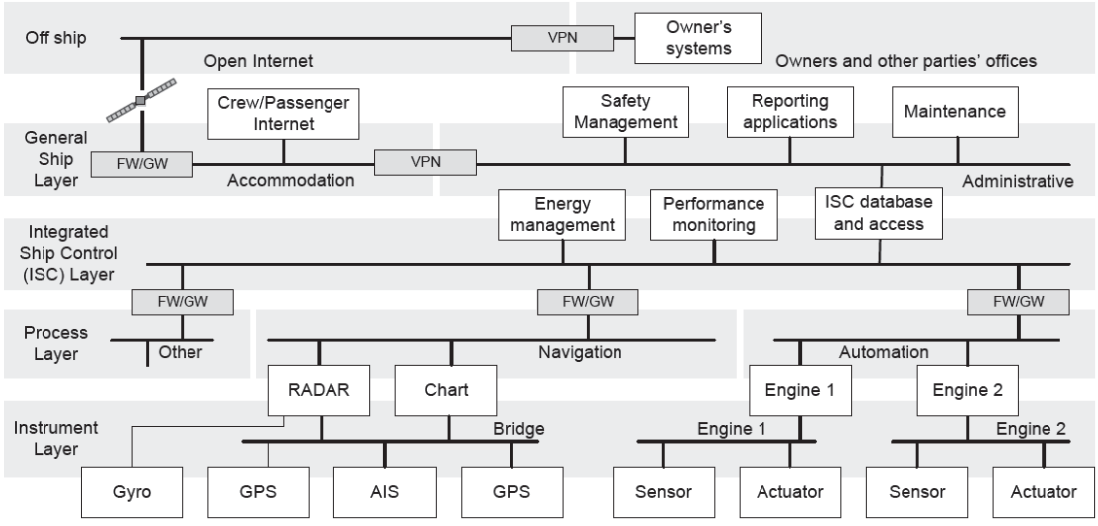

Figure 3 - Schematic Ship Network Architecture from (Rødseth, Christensen, & Lee)

Especially the more evolved ISC Ship Network Architecture from (Rødseth, Christensen, & Lee) is seen as useful in the context of this document since it has its focus on

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

interconnection, rather than on devices. As such, the (Rødseth, Christensen, & Lee) is providing an overview of the basic functions and/or devices in an ISC architecture, as well as their typical, immediate relationships, including also – importantly – how an ISC architecture could relate to ship – off-ship integration. It is also seen as worthwhile to note the extensive usage of security devices in the form of firewalls, gateways and VPN tunnels, to segregate network segments and to provide cyber-security isolation for mission critical devices and type approved entities.

In way of topology description, the work being reported on in the present document adopts the (Rødseth, Christensen, & Lee) five-layer AD, including the defined meaning of 'Layer'.

5.2.2 SOLAS, Carriage Requirements and IMO Type Approval

5.2.2.1 Navigation and Communications Equipment

The SOLAS convention dictates the minimum set of navigation and communication equipment that a ship must carry to fulfil the Convention – the carriage requirements. For each entity of such equipment, the IMO has moreover published a higher-level set of requirements, known as 'Performance Standards', and to make assessment of conformance against the Performance Standards operational and reproducible, the International Electro-technical Commission (IEC) publishes a corresponding set of 'Test Standards'.

As an illustration of this chain of requirements, SOLAS Ch. V, Reg. 19, Section 2.3.2 requires that all ships above 300 gross tons are to carry a 9 GHz RADAR, which, according to Section 2.7.1 of the same regulation, must be supplemented with an independent 3 GHz RADAR if the ship is above 3.000 gross tons. In turn, the properties and characteristics of these one or two RADARs are described in IMO Resolution MSC.192(79):2004, upon which the test specification IEC 62388:2013 builds. This means, in practice, that equipment suppliers who wishes to manufacture marine RADARs have to have their equipment 'Type Approved' in accordance with IEC 62388:2013 – which in turn cites a number of other IEC standards as being mandatory; fulfilment of the former ensures implicit fulfilment of also the latter. In addition to this complex of approval documents and processes, European ships – i.e. ships which flies a European flag – are required to use only equipment which has been approved according to the EC Maritime Equipment Directive (MED), for which equipment is rewarded the 'Wheelmark' upon passing the relevant tests.

One issue is in particular relevant for the present work: navigation and communications equipment is Type Approved according to its basic function, and is, as a starting point, seen as an independent island – so in the case described in the foregoing, a RADAR device is approved as a RADAR device - only.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

To ensure the integrity of navigation systems and subsystems, the IMO Type Approval standards often prescribes direct interfaces between systems, and almost always dictates the corresponding interface standards. In the latter context, the family of IEC 61162 serial communications standards are almost universally used. These interfaces are well understood in the maritime domain, and are characterized as being stable, effective and rugged – and, as a benefit to cyber security, they do not allow extraneous communications.

As touched upon briefly in the foregoing, the main functions/devices governed by carriage requirements and the IMO type approval regime fall in the spheres of navigation and communication equipment. Referring to the latter, the rules base is very similar to that in the realm of navigation: any seagoing ship above 300 gross tons has to comply with the overall rules set forth by SOLAS Ch. IV 'Radiocommunications', which in turn has spawned a set of Performance Standards and Test Standards, similarly to the world of navigation functions. This means that the primary functions of voice/data communications devices like VHF, MF, HF, Fleet broadband, Watch Receivers, and the other various members of the GMDSS clan, from a rules-based vantage point are comparable to RADAR, ECDIS, Heading Control (autopilot), to the sensor packages required to ensure the correct function of navigation systems (Gyro, GNSS, echo sounder(s), speed log(s)) as well as more general-purpose sensors like wind speed and direction, NAVTEX and AIS.

5.2.2.2 Equipment for Alert, Monitoring and Control (AMC)

The Classification Societies are to a great extent replicating the IMO Type Approval regime when it comes to equipment for ship-board Alert, Monitoring and Control (AMC) systems, and publish rules for their design, performance, response times, interconnections and segregation of function.

Where ships are quite generic when it comes to the navigation and communications requirements, they however differ much more in the AMC sphere: Ships are outfitted with different propulsion plants, auxiliary engines, valve systems, switchboards, tank gauging systems – the list is very long, and the number of variations very large. Moreover, in way of an example, while all ships have generic systems like a 'Ballast Water System', the features and automation level of individual instances are, again, varied in many respects.

From an architectural vantage point, AMC systems however follow the ideas in the AD described above, in the sense that at the lowest level they use relatively standard sensors and actuators, and the 'Instrument Layer' interfaces to such components tend to be standardized within three areas:

- Binary sensors which conceptually are contacts which can be either closed or open,
- Analogue sensors, which usually provide an industrial-standard interface where a voltage or a current is proportional with the measured value (0-10 VDC and 4-20 mA outputs being the most commonplace),

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

- Field-buses, most often using IEC 61162-type sentences or Modbus RTU telegrams for information more complex than what it is possible to convey with simple binary or analogue information, but also Canbus and Profibus are relatively often in use at this level.

Irrespectively, it should be noted that all hardware involved and/or connected to the instrument level, is required to be 'Type Approved'. This means that hardware is tested to comply with the environmental standards described in IACS E10 (IACS).
If the equipment is also be used in the ship's bridge, it has to fulfil (IEC 60945, 2002) instead; more often than not, suppliers choose to certify against both standards.

The consumers of data (and the corresponding providers of commands to devices in the lower levels of the AD) connected to the 'Instrument Layer' is usually process computers, which can be either PLC-types or PC-types of hardware – processors which more often than not are interconnected at the 'Process Level' using some kind of network. In older installations this could include HDLC, Arcnet and Ethernet, in newer installations this is almost exclusively Ethernet. Protocols vary at the 'Process Level', but are very often proprietary, since many suppliers believe that certain properties of TCP/IP are ill-suited for small-packet, near-real-time communications. Some suppliers are also using more than one protocol concurrently, providing data transmission which is optimized to the requirements from specific services and purposes, rather than one-size-fits-all.

AMC systems are going through an approval process which is comparable to the one described for navigation and communications equipment, but it is more individual than the one described above, driven by the nature of the beast: as described in the foregoing, AMC systems are much more varied than the latter two domains. In practice, the approval of AMC systems is based on the submission of drawings and functional descriptions of ship-specific configurations, and of tests of the individual systems, under the auspices of the Classification Society chosen by the ship owner for a particular ship. During this process, it is validated that the systems under scrutiny are composed entirely of type approved 'building blocks', and that the relevant rules and regulations in force for the particular ship and plant are adhered to, including the performance of the system in question, and, of particular relevance in this context, the segregation and isolation of interconnections and infrastructures.

5.2.3 Type Approved 'clusters'

Irrespectively of the rule and regulation base, i.e. whether the approval regime is grounded in the IMO type approval or the Class type approval domains, the rationale should not be ignored, however restrictive and rigid these processes may seem to be. As the name more than imply, the SOLAS convention is concerned with the safety of the crew/passengers, and the demands in SOLAS are set forth to ensure that a ship as a whole, as well as its individual components, do not exceed a given maximum level of acceptable risk. While ships are free to be more lavishly equipped than stated by the Convention, they will not get or be able to maintain the mandatory trading permits without being in compliance with

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

SOLAS, and the associated set of prescribed safety standards. Indeed, the IMO Performance Standards and the corresponding IEC Test Standards are formulated to ensure that capabilities which are deemed to be critical to life at sea are always available to the mariner.

Within the scope of machinery and automation systems, the Classification Societies have exactly the same mission as IMO, and their rules are formulated to ensure the safety, integrity, dependability and resilience of a ship and the ship systems which influences the safety and wellbeing of the crew, the protection of the environment and the preservation of valuables. The consequence of not meeting and remaining in compliance with the rules of an internationally recognized Classification Society is that such a ship, and its cargo, usually is unable to be insured by a recognized underwriter. This means, in practice, that financing for building or acquiring a non-conformant ship will not be available; in other words, any recognized ship owner does not have a choice but to be in compliance with Class rules – also considering that Class rule compliance implicitly ensures compliance with a long list of international rules and regulations besides IMO.

One practical result of the type approval regime, irrespectively of whether a particular ship-board system is governed by the IMO or by Class, is what could be called 'clusters': On-board systems are created out of type approved 'building blocks', but they are at the same time limited to integrate devices and to provide functions which, through the Rule base, are 'meant' to work together. For this reason, it is in many cases meaningful to subdivide ship-board systems like it has been done also in the foregoing (see Figure 4): The navigation system represents one such cluster, the communications system and the automation (AMC) systems are two other archetypical clusters. Following the arguments presented, it will also be clear that these systems essentially are meant to be kept apart, as well as being 'closed worlds': one cannot directly add components or devices to either type of system that is not type approved for the purpose as appropriate, and one cannot add functions which compromise the type approved functionality of such an entity, cluster, or both.

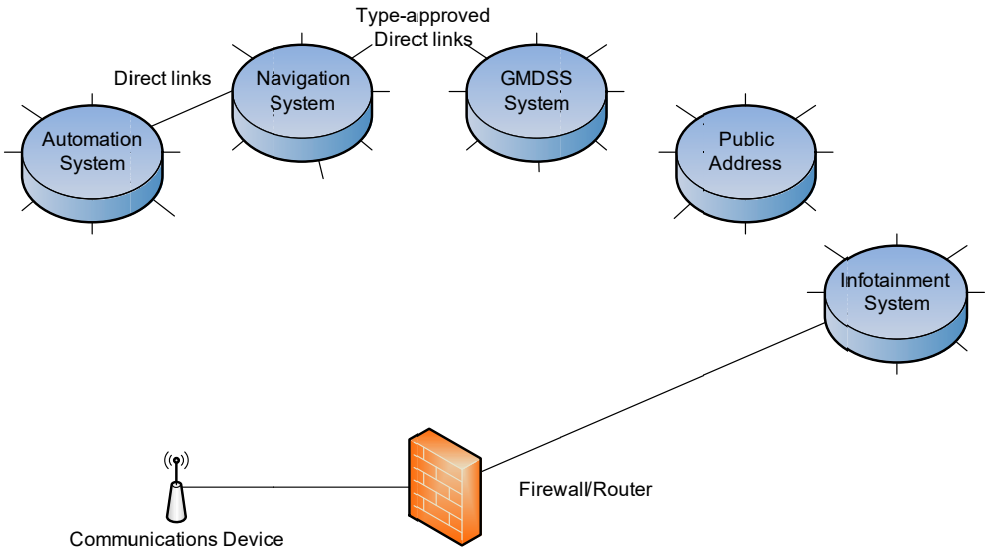

Figure 4 – Conventional (2016) topology showing clusters of type approved equipment

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

The exception for this practice is usually tied to being able to demonstrate that such additional devices and/or functions do not violate the type approved nature of the host device or application, while observing that the add-ons are to be compliant to any relevant rule and regulations in force. When it comes to networked systems, best practice does also seem to involve the extensive use of gateways and firewalls, not only between layers, but also between entities at each layer, as well as the usage of multiple networks dedicated for particular purposes (see Figure 5). As an example of this, operator workstations can conceivably be connected to one network for alert, monitoring and control, one network for administration, and one network for CCTV; the important issue here is segregation and the ensuring that no data flows from one domain to the next, with the risk of corruption of essential services.

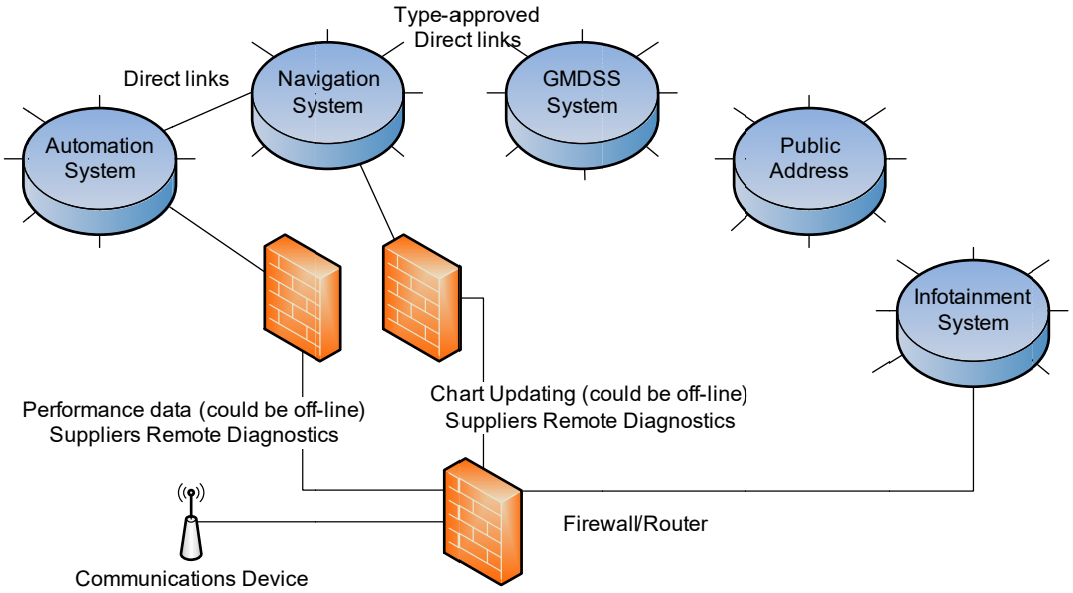

Figure 5 - State-of-the-art topology (2016) showing a higher level of integration

5.3 The MC and MCC in Context

The argument that it is necessary for the MC and MCC to be fitted not only on new ships but also on the existing fleet is a primary dimension of the context. Within that, it is however also clear from the foregoing that it is insufficient that the MCC is simply able to co-exist with type approved clusters, the architecture must be so that the MCC can provide the upcoming MC services to the mariner:

- The on-board architecture must support that eNavigation functions and services can be provided to the mariner;
- The on-board architecture has to be so that it does not compromise type-approved systems and clusters of systems;
- The on-board architecture has to ensure that the loss of connectivity to the MC/MCC does not violate mandatory functions;

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

- The topology of the on-board architecture has to be in compliance with the industry best practice for security, protection and segregation of infrastructure.

5.4 Architectural Elements (AE)

To be able to produce candidate architectures, the essential elements, i.e. elements that have a need for communication with the MC through the MCC, are to be identified and described from a number of architectural views, as set forth by (ISO/IEC42010, 2011). One such view, which is well represented in the above, is the physical – topological – view; another, which is more implicit, is the functional view: because the functionality of type approved navigation and communications devices and components are inherent in the IMO Performance Standards and the IEC Test Standards, these are seldom explicit, but they nevertheless have to be known to, appreciated and understood by the systems architect.

Figure 6 show a potential conceptual model of the architecture. Some architectural elements are clearly visible:

- e-Navigation Services
- Automation System
- Navigation System
- GMDSS System
- Infotainment system
- IEC61162-460
- Public Address
- T2.3 Roaming

The MCC as well as the elements providing the various communication services, such as VSAT, T2.1 VDES are clearly also an AE

Elements that can be identified from e.g.
Figure 3, such as ECDIS, RADAR, AIS may not need to be items in the architecture, since each represent a certain function within the Navigation System.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

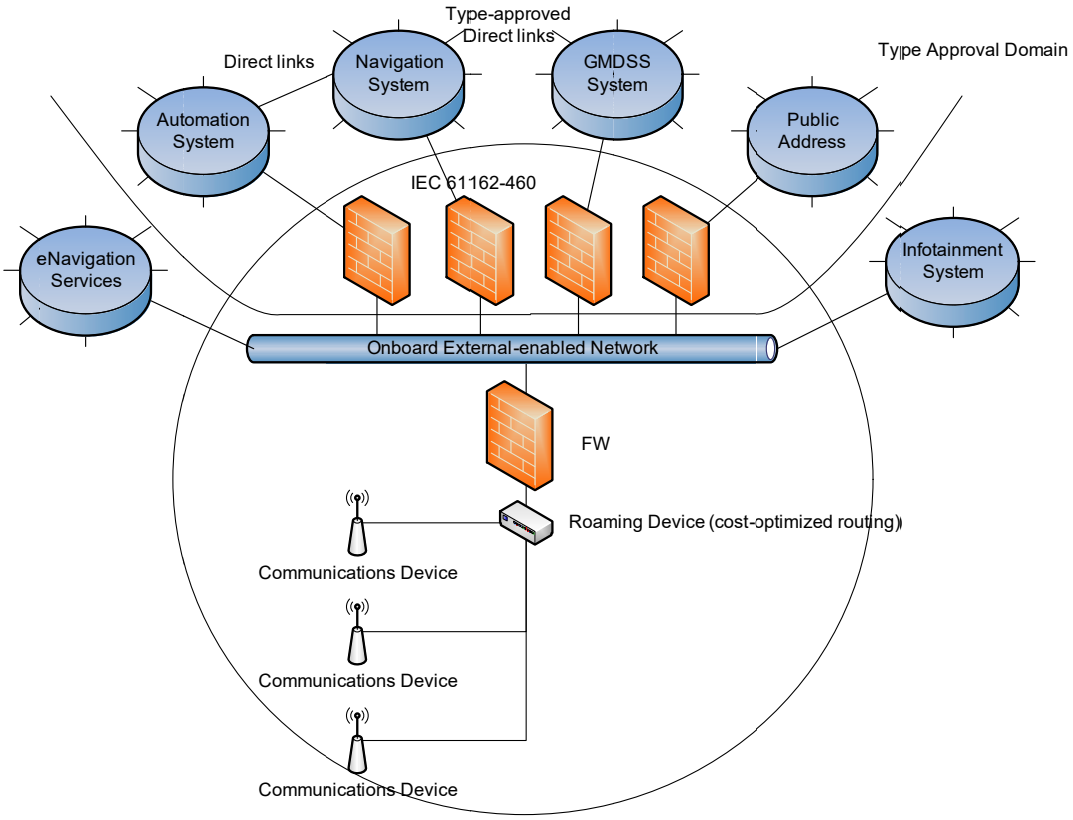

Figure 6 – Potential/conceptual ship-board eNavigation topology

For clarity, it should be noted that the three individual communications" devices shown in the lower half of
Figure 6 not necessarily are type approved according to an IMO/IEC set of performance standards and test standards. Indeed, while such devices have to conform to either IACS E10 or IEC 60945 for shipboard use, the relevant standard being dependent on the physical proximity to the ship's navigation bridge, they are seen here as fulfilling a communications requirement which is not mandated by rules and regulations. For this reason, there may not be a relevant set of performance standards available, which, for example, would be the case for a WiFi device, certain kinds of satellite communications and certain kinds of terrestrial communications networks, such as mobile phone technology.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

6 Viewpoints

This chapter identifies the viewpoints important for the on-board architecture within the defined scope for Task 2.4.
Experience from use of the (ISO/IEC42010, 2011) methodology is that the following viewpoints are recommended for consideration:

- Context
- Functional
- Informational
- Concurrency
- Development
- Deployment
- Operational

In WP2, Task 2.4 we have not identified further viewpoints.

6.1 Context Viewpoint

The context viewpoint describes the relationships, dependencies and interactions between the on-board systems and their environment.
The context viewpoint is considered to be fully relevant since the architecture in scope is involved in various service contexts i.e. all services that involve communication to and from the ship.
Concerns/requirements seen from all relevant types/classes of services must be included.

6.2 Functional Viewpoint

The functional viewpoint describes the system's runtime functional elements, their responsibilities, interfaces and primary interactions.

6.3 Informational Viewpoint

The informational viewpoint describes the way the architecture stores, manipulates, manages and distributes information.

6.4 Concurrency Viewpoint

The concurrency viewpoint basically describes the architectural behaviour when operating/servicing in multiple contexts.
Since the architecture in scope is central in communication to/from the ship and services and functionality relying on this communication needs to operate concurrently, the viewpoint is a given to consider.
However, the viewpoint may be simplified to requirements related to communication prioritization and the architecture behaviour in special situations e.g. in distress.

6.5 Development Viewpoint

The development viewpoint describes the architecture that supports the development process.
The architecture and the data communication protocols and data structures should support easy development of services.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

6.6 Deployment Viewpoint

The deployment viewpoint describes the environment into which the system will be deployed.
Since we have the overall goal of recommending architecture in our defined scope that takes the existing infrastructure into consideration and identifies the gap between the recommendation and the existing infrastructure, a *perspective* dealing with deployment will be defined.

6.7 Operational Viewpoint

The operational viewpoint describes how the architecture will be operated, administered and supported when active.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

7 Views

This chapter describes the operational needs/views that shall be considered as prerequisites and /or requirements for the design of the on-board architecture for the integrated ships network.

Efficient communication solutions and enhanced ability to integrate information from different systems provides new way of doing “old stuff” - all the way from planning via operation and monitoring to reporting or analytics of historical data. The possibility to use, share, store and transfer data is the key to success. In the table below we have prepared a matrix outlining the user need, services in use, data type and data needed including the time aspect.
The table does not include what is required by and fulfilled by the installed GMDSS.

The e-Navigation strategy has been developed by IMO (NSCR-1/28) with contributions from member states of IMO and a number of Intergovernmental and non-governmental organizations, including the International Hydrographic Organization (IHO), Comité International Radio-Maritime (CIRM),the International Association of Lighthouse Authorities (IALA), the International Chamber of Shipping (ICS), the Baltic and International Maritime Council (BIMCO) and the International Electro technical Commission (IEC).
In defining the current and future maritime communication needs, a set of maritime services has been defined, namely: The Maritime Service Portfolio (MSP).
Various other works, MarNIS, Flagship, EfficienSea, Monalisa, ACCSEAS and MonaLisa2 have further refined the services defined by MSP.

The Task 2.4 analysis work to produce Views has resulted in combining several of the viewpoints described in chapter 6, and basing the views on the MSP.
At this time of writing (April 2016), there is a bit of confusing numbering of the MSP’s, since this is work ongoing. E2 Task 2.2 has produced the overview of current definitions of MSP shown in Figure 7. This numbering is also used in the work of Task 2.4.

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

MSP reference	Maritime Service (IALA WG3)	EfficienSea 2 Selected & ref Use Cases	EfficienSea 2 MSP use cases (WP2.2)
MSP 1	VTS Information Service (IS);	MSP 1	VTS (task 6.2)
MSP 2	VTS Navigation Assistance Service (NAS)	MSP 2	task 6.2
MSP 3	VTS Traffic Organization Service (TOS)	MSP 3	task 6.2
MSP 4	Local Port Service (LPS)	MSP 4	Port information (task 5.2)
MSP 5	Maritime Safety Information (MSI) service	MSP 5	MSI & NM (task 4.2)
MSP 6	Pilotage Service	MSP 6	
MSP 7	Tugs Service	MSP 7	
MSP 8	Vessel Shore Reporting	MSP 8	Port reporting (task 5.2) SRS reporting (task 6.2)
MSP 9	Telemedical Maritime Assistance Service (TMAS)	MSP 9	Self-organising emergency (task 6.1)
MSP 10	Maritime Assistance Service (MAS)	MSP 10	Sea charts (task 4.4)
MSP 11	Nautical Chart Service	MSP 11	
MSP 12	Nautical Publications Service	MSP 12	
MSP 13	Ice Navigation Service	MSP 13	Ice Cat Service - charts & forecast (task 4.7)
MSP 14	Meteorological information service	MSP 14	METOC (task 4.3)
MSP 15	real-time hydrographic and environmental information services	MSP 15	
MSP 16	Search and Rescue (SAR) Service	MSP 16	Self-organising emergency (task 6.1)
-	Remote monitoring of ships systems	MSP 17	
-	Offshore activities	MSP 18	
-	Fishing activities	MSP 19	
-	Leisure boating	MSP 20	
-	Coastal surveillance	MSP 21	

Figure 7 Maritime Service Portfolio (MSP) as defined by IALA and E2

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

				Data to be available electronically	
Category	**MSP**	**UseCase**		**Data Source**	**Usage (what equipment) (what endpoint)**
Task 5.1	MSP 8	Port Reporting	Port Reporting (prior to port entry)	on-board admin	Shore Authorities
			Port Reporting (prior to port departure)	on-board admin	Shore Authorities
Task 4.2	MSP 5	MSI & NM	MSI & NM	Shore Authorities	Ships
			MSI & NM (Hydro data)	Shore Authorities	Ships
Task 4.3	MSP 14	Weather	Real time Metoc Data	Shore Authorities	Ships
			METOC	Commercial entity	Ships
Task 4.4	MSP 11	Sea Charts	Sea Charts (authorities)	Shore Authorities	Ships
			Sea Charts (commercial serv.)	Commercial entity	Ships
Task 4.5	MSP 5/14/15/18	Smart buoys	Smart buoy Broadcast Service	Smart Buoy	Ships Off-shore installations
Task 4.5	MSP 3/18/(others?)		Smart Buoy Management Service (AtoN)	Off-shore installations	AtoN
Task 4.6	MSP 1/8	Route data	Route plan Active route	Ship	Shore Authorities VTS centers Ship
Task 4.6 Task 6.1	MSP 1/2/3/4/6/13/14		Route check Route info's - suggestion - alerts Route optimisation & negocation (Ex. Arctic nav: ice + shallow waters)	Shore Authorities VTS services Commercial Provider Pilot	Ship
	MSP 1/2/3		Route information (optimization, revision, incident, hazard)	VTS services	Ship
Task 4.6	MSP 1		Route exchange	Ship	Ship
Task 4.7	MSP 13	Ice Charts Services	Ice Chart Service - charts	Shore Authorities	Ships
			Ice Chart Service - charts	Commercial Provider	Ships
			Ice Chart Service - forecasts	Shore Authorities	Ships
			Ice Chart Service - forecasts	Commercial Provider	Ships
Task 5.2	MSP 4	Port Information	Port Information	Port authorities (not in Effic.2) Port organisations	Ships
			Port Information Commercial services	Commercial entities Port organisations	Ships
Task 5.3	MSP 8	Emission Monitoring		Ships sensors/devices Smart Buoys sensors/devices Shore control stations	Shore Authorities Shipping Companies
Task 6.2	MSP1	VTS & SRS	VTS Reporting (see also Route info task 4.6)	Shore Authorities	Ships
Task 6.2	MSP8		SRS Reporting	Ships	Shore
Task 6.3	MSP 10/16	Self-organizing emergency (Arctic area)		Ships	Ships Shore

Figure 8 MSP Use cases and relation to E2 Tasks

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

Task 2.2 and Task 2.4 have in co-operation worked out a list of MSP's, their use cases and relation to work on-going in various E2 tasks. This list is show in Figure 8.
Since the on-board architecture also have to support other types of communication/services, Task 2.4 have produced an additional set of use cases, shown in Figure 9.

				Data to be available electronically	
Category	**MSP**	**UseCase**		**Data Source**	**Usage (what equipment) (what endpoint)**
Task 2.4	Public but regionally constrained Text Chat	Text Communication	Ship to Ship	Ships	Ships
			Ship to Shore Ship to Ship	Ship/Shore	Ship/Shore
Task 2.4	MSP 21	Vessel tracking	Sattelite	Ship	Shore
			AIS	Ship	Shore
			MC	Ship	Shore
Task 2.4	MSP17	Voyage Safety monitoring	Route + Tracking + Safety alarms + loading conditions and stability	Ship	Shore
		Voyage efficiency monitoring	Tracking + Nav Data + Fuel + static and dynamic vessel data	Ship	Shore
		Vessel Performance analysis	Consolidated data package needed for shore based performance analysis and planning	Ship	Shore
		Ship's system performance	Monitoring of vessel system performance and alarms	Ship	Shore
		Ship's system performance and maintenance analysis	Consolidated data package needed for analysis of vessels system performance and maintenance planning	Ship	Shore
		Cargo monitoring	Volumes/weight, environmental conditions etc.	Ship	Shore
Tasl 2.4		Ship's spares and logistics		Shore	Ship

Figure 9 E2 Task 2.4 added Services and their use cases

For each of the use-cases in this larger table, E2 Task 2.2 and Task 2.4 have defined a set of characteristics of the communication involved in the service (described in the following sub-chapters)
In the tables in the following chapters there are question marks several places. This is to denote that further investigation has to be made to achieve better guess than what is possible at this time of writing (April 2016).

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

7.1 Interaction Type

There are three interaction/communication types:

- Point to Point (P2P)
- Multicast
- Broadcast

The table in Figure 10 shows the interaction types involved in the various MSP use cases and the following sub-chapters describes the interaction types in more detail.

7.1.1 Point to Point (P2P)

We have defined the P2P communication so that the destination end-point is known and the source of communication is sure that information is transferred, since the destination is providing acknowledgement of reception. TCP is one type of protocol used in P2P communication.

7.1.2 Multicast

Multicast is defined as a “one to many” communication, where all destination endpoints are known and the source of communication is sure that information is transferred, since the destination is providing acknowledgement of reception

7.1.3 Broadcast

Broadcast is defined as “one to many” communication, where the destination endpoints are not known by the source and are not providing acknowledgement of reception. Therefore there are not guarantee that information is transferred.
There are several subsets of broadcasts. E.g. geocasts used in literature for MSP denoting messages distributed to a geographical limited area.
Geocasts can be based on multicasts or broadcasts, all depending if the receivers are known or not.
Since broadcasts can be “filtered” by various constraints, where geography is just one, this report will use the term broadcast.

7.2 Cyber Security

To indicate the level of cyber security in the communication, the following characteristics are used.

- Authentication of information, including data integrity (Digital signing)
- Confidentiality (Encryption)
- Client Authentication

The table in Figure 10 shows cyber security characteristics for the various MSP use cases. Note that MSP design is still work on-going and hence information is subject to change.

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

UseCase		Interaction Type			Cyber Security		
		P2P	Multicast, Point to many, with ack.	Broadcast, Point to many, No ack.	Authentication (digital signing)	Confidential (Encrypted)	Client Authentication
Port Reporting	Port Reporting (prior to port entry)	x			x	x	
	Port Reporting (prior to port departure)	x			x	x	
MSI & NM	MSI & NM	x			x	x	
	MSI & NM (Hydro data)	x			x	x	
Weather	Real time Metoc Data			x	x		
	METOC	x			x	x	x
Sea Charts	Sea Charts (authorities)	x		x	x		
	Sea Charts (commercial serv.)	x	x	x	x	x	x
Smart buoys	Smart buoy Broadcast Service			x	x		
	Smart Buoy Management Service (AtoN)	x			x	X (?)	
Route data	Route plan Active route			x	x		
	Route check Route info's - suggestion - alerts Route optimisation & negocation (Ex. Arctic nav: ice + shallow waters)	x			x	x	(X)
	Route information (optimization, revision, incident, hazard)	x		x	x	x	x
	Route exchange		x	x	x		
Ice Charts Services	Ice Chart Service - charts	x			x		x
	Ice Chart Service - charts	x	x		x	x	x
	Ice Chart Service - forecasts			x			
	Ice Chart Service - forecasts	x	x		x	x	x
Port Information	Port Information			x	x		
	Port Information Commercial services	x			x	x	
Emission Monitoring							
VTS & SRS	VTS Reporting (see also Route info task 4.6)	x		x	x	x	
	SRS Reporting	x			x	x	
Self-organizing emergency (Arctic area)		x		x	x	x	

Figure 10 Use Case Interaction Type and Cyber Security

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

7.3 Link Requirements

The Link requirements are split into the following:

- Transaction Frequency
- Information size per transaction
- Transfer per day, per site
- Latency

This is basically to provide some estimates on required bandwidth and accepted latency in the communication.
The link requirements are not as important in relation to developing architecture as it is for E2 Task 2.2, evaluating communication technologies, but will provide an understanding of options for communication in various scenarios.
The table in Figure 11 shows the Link requirements for the various MSP use cases.
Note that MSP design is still work on-going and hence information is subject to change.

7.4 Priority

For use when prioritizing traffic, we have used the same definitions as in GMDSS DSC calling.

- Distress
- Urgent
- Safety
- Routine
- General

The table in Figure 11 shows the priority for the communication in the various MSP use cases.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

UseCase		Link Requirements				Priority
		Transaction Frequency	Information Size (per transaction) (maximum)	Transfer per day per site kB	Latency	Priority (Distress, Urgent, Safety, Routine General)
Port Reporting	Port Reporting (prior to port entry)	Depend of Type of Operation 1 per day ?	32 x 1 K Byte	32 x 1 K Byte		Routine
	Port Reporting (prior to port departure)	Depend of Type of Operation 1 per day ?	32 x 1 K Byte	32 x 1 K Byte		Routine
MSI & NM	MSI & NM	Depend on info type & priority	1-10 kByte	?		Safety
	MSI & NM (Hydro data)	Depend on info type & priority	High data volumes > 1 Mb			Safety
Weather	Real time Metoc Data	Depend on info type & priority				Routine
	METOC	On request	?		1-4 hours (?)	Routine Urgent (on event)
Sea Charts	Sea Charts (authorities)	On request On event (change)	< 1-10 kBytes (images ?)	< 1-10 kBytes	few hrs to several weeks	Routine Urgent (on event)
	Sea Charts (commercial serv.)	On request On event (change)	<150 MB ?	<20 MB	few hrs to several weeks	Routine Urgent (on event)
Smart buoys	Smart buoy Broadcast Service	1 h On event (alert)			1 h	Routine Safety (alert)
	Smart Buoy Management Service (AtoN)	On event	?		Days	Safety
Route data	Route plan Active route	before leave berth on change on demand	< 1 kbytes	< 10 kB		Routine
	Route check Route info's - suggestion - alerts Route optimisation & negocation (Ex. Arctic nav: ice + shallow waters)					
	Route information (optimization, revision, incident, hazard)	On event On request	< 10 Kbytes	10 Kbytes	Few mn to few hours	Routine Urgent (on event)
	Route exchange					
Ice Charts Services	Ice Chart Service - charts	1h	250 bytes	1200		Routine
	Ice Chart Service - charts	1h	1 Kbytes (may be more, images ?)	?		Routine
	Ice Chart Service - forecasts	1h	1 KBytes	4800		Routine
	Ice Chart Service - forecasts	1h	1 Kbytes (may be more, images ?)	?		Routine
Port Information	Port Information	On request	?	?		Routine
	Port Information Commercial services	On request	?	?		Routine
Emission Monitoring						
VTS & SRS	VTS Reporting (see also Route info task 4.6)	On event On request	< 10 Kbytes	10 Kbytes	Few mn to few hours	Routine Urgent (on event)
	SRS Reporting	Depend on type of operation 1 per day?	32x 1K Byte	32x 1K Byte		Routine
Self-organizing emergency (Arctic area)		On event On request	< 1 kByte	< 1 kByte	Few mn to few hours	Urgent

Figure 11 Use Case Link Requirements and Priority

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

7.5 Candidate Carriers

The candidate carriers for the communication to support the various services, identified by E2 Task 2.2 are:

- Wi-Fi
- WiMax
- Cellular networks (2G, 3G, LTE)
- AIS/ASM
- VDE-TERR
- MF/HF NBDP
- MF/HF digital data service (NAVDAT)
- Inmarsat
- Iridium
- VSAT
- VDE-SAT

For description of these, please refer to (E2-T2.2, 2016) Analysis report on available and emerging communications technologies.

Figure 12 show candidate carriers for some MSP use cases. The full list is available in a larger excel sheet not suitable to include in this report.

		Candidate Carriers										
UseCase		Wi-Fi	WiMAX	Cellular networks (2G, 3G, LTE)	AIS/ASM	VDE-TERR	MF/HF NBDP	MF/HF digital data service (NAVDAT)	Inmarsat (also C)	Iridium	VSAT	VDE-SAT
Port Reporting	Port Reporting (prior to port entry)	x	x	x		x			x	x	x	x
	Port Reporting (prior to port departure)	x	x	x		x			x	x	x	
MSI & NM	MSI & NM	x	x	x	ASM	x			x	x	x	x
	MSI & NM (Hydro data)	x	x	x		x			x	x	x	x
Weather	Real time Metoc Data				ASM	x						
	METOC	x	x	x		x			x	x	x	x
Sea Charts	Sea Charts (authorities)	x	x	x		x			x	x	x	x
	Sea Charts (commercial serv.)	x	x	x					x	x	x	
Smart buoys	Smart buoy Broadcast Service				ASM	x						x
	Smart Buoy Management Service (AtoN)				ASM	x						x

Figure 12 Example Candidate Carriers for some MSP Use Cases

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

7.6 Basic Communication Services

This chapter makes an attempt to break down the services from the MSP and the future envisioned services by T2.4 in to basic communication services, that single handed or in combination can be used to create the complete service in the Maritime Cloud (MC).

The actual design of the various services obviously cannot be predicted in the scope of this report, however, analysis of various service descriptions, such as:

- (ACCSEAS, Service Description: Maritime Safety Information and Notice to Mariners Service, 2015)
- (ACCSEAS, Service Description: Maritime Cloud, 2015)
- (E2-T3.1, Analysis report on communication and infrastructure, 2015),
- (E2-T3.1, D3.2 Conceptual Model, 2015)

show a set of basic elements in the MCC:

- Maritime Messaging
- Almanac
- Local Data Service
- Local Lookup Service

It is judged that the on-board components for many of the use cases can be based on the service elements of the MCC. Others will require further tailored web service components that cannot be standardized in a similar manner as done for the MC and MCC.
In some of the use-cases, the specific services may be implemented as a combination of MCC and tailored components.
With a few exceptions (AIS through VHF), it is assumed that all of the services are built on top of the IP layer (RFC1122, 1989).

Figure 13 and Figure 14 show how the various services in the MSP are anticipated to make use of the basic services, partly offered by the MCC and partly by tailored Web services.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

UseCase		Data to be available electronically		Base Communication Service					
		Data Source	Usage (what equipment) (what endpoint)	MMS	Almanac	LLS	LDS	WEB	AIS
Port Reporting	Port Reporting (prior to port entry)	on-board admin	Shore Authorities	x	x	x			
	Port Reporting (prior to port departure)	on-board admin	Shore Authorities	x	x	x			
MSI & NM	MSI & NM	Shore Authorities	Ships	x			x		
	MSI & NM (Hydro data)	Shore Authorities	Ships	x			x		
Weather	Real time Metoc Data	Shore Authorities	Ships	x	x	x			
	METOC	Commercial entity	Ships	x	x	x			
Sea Charts	Sea Charts	Shore Authorities	Ships		x	x	x		
	Sea Charts (commercial serv.)	Commercial entity	Ships		x	x	x		
Smart buoys	Smart buoy Broadcast Service	Smart Buoy	Ships Off-shore installations	x					
	Smart Buoy Management Service (AtoN)	Off-shore installations	AtoN	x					
Route data	Route plan Active route	Ship	Shore Authorities VTS centers Ship	x	x	x			
	Route check Route info's - suggestion - alerts Route optimisation & negocation (Ex. Arctic nav: ice + shallow waters)	Shore Authorities VTS services Commercial Provider Pilot	Ship	x	x	x			
	Route information (optimization, revision, incident, hazard)	VTS services	Ship	x	x	x			
	Route exchange	Ship	Ship	x					
Ice Charts Services	Ice Chart Service - charts	Shore Authorities	Ships	x	x	x	x		
	Ice Chart Service - charts	Commercial Provider	Ships	x	x	x	x		
	Ice Chart Service - forecasts	Shore Authorities	Ships	x	x	x	x		
	Ice Chart Service - forecasts	Commercial Provider	Ships	x	x	x	x		
Port Information	Port Information	Port authorities (not in Effic.2) Port organisations	Ships		x	x			
	Port Information Commercial services	Commercial entities Port organisations	Ships		x	x			
Emission Monitoring		Ships sensors/devices Smart Buoys sensors/devices Shore control stations	Shore Authorities Shipping Companies						
VTS & SRS	VTS Reporting (see also Route info task 4.6)	Shore Authorities	Ships	x	x	x			
	SRS Reporting	Ships	Shore	x	x	x			
Self-organizing emergency (Arctic area)		Ships	Ships Shore			?			

Figure 13 Basic Communication Services for the MSP

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

UseCase		Data to be available electronically		Base Communication Service					
		Data Source	Usage (what equipment) (what endpoint)	MMS	Almanac	LLS	LDS	WEB	AIS
Text Communication	Ship to Ship	Ships	Ships	x					
	Ship to Shore Ship to Ship	Ship/Shore	Ship/Shore	x					
Vessel tracking	AIS	Ship	Shore						x
Voyage Safety monitoring	Route + Tracking + Safety alarms + loading conditions and stability	Ship	Shore					x	
Voyage efficiency monitoring	Tracking + Nav Data + Fuel + static and dynamic vessel data	Ship	Shore					x	
Vessel Performance analysis	Consolidated data package needed for shore based performance analysis and planning	Ship	Shore					x	
Ship's system performance	Monitoring of vessel system performance and alarms	Ship	Shore					x	
Ship's system performance and maintenance analysis	Consolidated data package needed for analysis of vessels system performance and maintenance planning	Ship	Shore					x	
Cargo monitoring	Volumes/weight, environmental conditions etc.	Ship	Shore					x	
Ship's spares and logistics		Shore	Ship					x	

Figure 14 Basic Communication Services for MSP

7.6.1 Generic Web Service

A web service is as defined by W3C Web Service Architecture Working Group, and therefore a basic service implemented using standards such as HTTP, HTML, XML and JSON. The service can be REST compliant or not.
The term "Web service" as generally understood, describes a standardized way of integrating Web-based applications using the XML, SOAP, WSDL and UDDI open standards over an Internet protocol backbone. XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available and UDDI lists what services are available.

7.6.2 Data Service

The Data/File Service is a basic service that is able to transport larger content from ship to shore or from shore to ship. The term larger content is a semi-undefined measure. It simply means that the size of the data to be transported is of a size that is too big to be handled by a basic request/response web service in a robust manner due to the nature of the quality of service provided by e.g. VSAT, VDES.
The Data/File service is envisioned to be of a "background" nature in the sense that a data/file transport can be initiated by specification of content identification, source and destination endpoints as well as other requirements to the particular transport in a request

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

to the Data/File Service, and then the service will take care of the transport and notify the client when the transport has completed.
Both source and destination endpoints that support this service must of course contain a certain amount of storage capacity, enough to support the providers and consumers of the content.
The simplest implementation of such a service could contain a FTP server and a FTP client plus a service that enables clients to request files to be transferred from the source to the FTP server and the FTP client to "get" the file from the server and when done, notify the client of completion and location of the transported file.

Several SATCOM providers are offering file transport/synchronisation services as means for transporting larger data amounts to/from the ship. The value added that these services provide are that the methods used are overcoming the problems with latency and drop-outs when transporting larger data amounts, especially in areas of poorer link quality. The services typically make use of advanced TCP spoofing and various types of compression. Similar methods should be considered with respect to the MC data service, especially if it is to work across VDES.

7.6.3 Broadcast Message Service

We have defined broadcasting as a distribution of information to multiple clients without acknowledgement of reception. The service type is similar to an automated weather station transmitting voiced forecasts via VHF radio. The new element here is that it is the broadcast of data information via available data exchange communications channels.
It is envisioned that for receivers to be able to receive broadcast information, they will have to "subscribe" to the broadcast stations, similar to tuning into the specific VHF radio channel.
For inspiration to architectural design of a Broadcast Message Service, it is worth to make a reference to similar broadcast services that have been developed for the W3C, namely the Really Simple Syndication (RSS), also called Web Feeds.

In (ACCSEAS, Service Description: Maritime Cloud, 2015), a Maritime Messaging Service (MMS) is described using geo-casting, a broadcasting method addressing receivers within a certain geographical area. The basic Broadcast Message Service with geographic filtering applied on messages broadcast could also be a solution here.

7.7 Data Formats

Since the first version of the (IHO, 2009) S100 standard was published, several works on MSP mentioned in chapter 7.6 and the work in e-Navigation projects like the Monalisa 1&2 have provided several additions/extensions to S100. S100 defines a conceptual schema language and allows for encoding languages such as XML, GML, HDF-5, ISO 8211 and JPEG2000.
Other works, such as (ACCSEAS, Service Description: Maritime Safety Information and Notice to Mariners Service, 2015) and (ACCSEAS, S-100 Product Description: Maritime

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

Safety Information / Notice to Mariners Service, 2015) base the data formats developed, on the S100 standard.
In general, the XML schemas are the dominant web service data formats although formats such as JSON and BISON are becoming increasingly used on the basis of claimed enhanced efficiency.
It is not in the scope of this document to define data formats further. It can be concluded that the architecture must support any of the data formats used in the definition of web-services.

7.8 Viewpoints for the different services

To be sure that all aspects are considered for the services defined in MSP, they have to be analysed from the viewpoints as set out in chapter 6.

- Context
- Functional
- Informational
- Concurrency
- Development
- Deployment
- Operational

With the current state of the definitions of the various services, it is too early to conduct that analysis. Therefore a more intuitive approach needs to be applied when deducing stakeholder concerns as given in chapter 10.

8 Stakeholder Identification

The EfficienSea2 project has been setup in such a way, that WP3 develops the communication framework for the maritime cloud, and as such the on-board architecture is a sub-component supporting that framework. Since WP3 must collect input and develop requirements for the framework, the work of WP3 will also provide requirements for the on-board architecture.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

9 Perspectives

An architectural perspective is a collection of architectural activities, tactics and guidelines that are used to ensure that a system exhibits a particular set of related quality properties that require consideration across a number of the systems architectural views.

The following perspectives have been identified to be relevant for E2 Task 2.4:

- Low impact Integration with existing infrastructure and architecture
- Requirement of an "open" and harmonized architecture
- Cyber Security Considerations.

9.1 Low impact Integration with existing infrastructure and architecture

Presently, the standardization of the on-board data infrastructure is mostly in areas such as navigation sensors in the IEC61162 series of standards, that cover serial and network based communication between sensors and data users, such as RADAR, ECDIS, VDR and AIS.
Within both the navigation, automation and communication domains on ships, proprietary solutions are still dominant.

Furthermore, it is not expected that the advent of the Maritime Cloud will change this substantially, considering both the magnitude of the installed base, which it in any case should be possible to integrate into the Maritime Cloud, but also the very substantial effort which has been put into establishing and maintaining the present effective, efficient and safe data platforms.

With the existing magnitude of the installed base of on-board data infrastructures with very little standardization, it is important to understand the gap between suggested candidate architectures and the existing installed base.
To validate the candidate architectures using this perspective, it is important to produce a map of the existing installed base to at least a top level topology and data communications overview.

9.2 Requirement of an "open" and harmonized architecture

Many discussions can be initiated on what the requirement of an open and harmonized architecture means. This chapter describes the assumptions made in Task 2.4.

An Open architecture means:

- The architecture supports easy expansion with and implementation of additional functionality
- The architecture is based on functional elements with interfaces that are publicly defined and preferably have open source implementation examples.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

Harmonized architecture means that its context, functional, informational and operational properties are defined by existing and / or upcoming areas for standardisation.

Context properties describe how architectural elements interact.
Harmonized context properties then mean: use of standardised protocols.
Functional properties describe the function of architectural elements.
Harmonized functional properties then mean: requirement of standardised functionality.
Informational properties describe what information is exchanged between architectural elements.
Harmonized informational properties then mean: standardised data formats.
Operational properties describe how the architecture will be operated when active.

Note, that the above does not mean that e.g. all functionality of the architecture needs to be standardised.

9.3 Cyber Security Considerations

The Cyber Security standards area is complex and growing, and will probably continue to do so, as the world of interconnected IT systems and devices are developing. The history of security breaches and their effects are continuing to provide a source of risks to our society on land, sea, air and space.

The only standards found, that relate directly to cyber security on-board are the (IEC61162-450, 2011) and (IEC61162-460, 2015).

European Network and Information Security Agency (ENISA) has produced a report on analysis of cyber security aspects in the maritime sector, clearly identifying the need for policies and recommendations in the Maritime Sector. (ENISA, 2011)

Currently, there are suggestions to IMO and work initiated for producing recommendations on the area.

BIMCO has in January 2016 published Guidelines on Cyber Security On-board Ships (BIMCO, 2016). The guidelines are produced and supported by BIMCO, CLIA, ICS, Intercargo and Intertanko, and several other organisations and companies.

American Bureau of Shipping (ABS) has February 2016 published a guidance note on the application of cyber security principles to marine and offshore operations (ABS, 2016). This note is indicated to be the first in a series.

Both BIMCO and ABS are referencing the NIST series of standards related to cyber security, as well as the ISO/IEC 27000 standards.

The original and ongoing work of the ISA99 committee is being utilized by the International Electrotechnical Commission in producing the multi-standard IEC 62443 series. Although

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

not a specific maritime standard, the ISA/IEC 62443 series addresses Industrial Automation and Control Systems (IACS) Security and complements ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements, both of which are relevant to the response to potential cyber security threats in the maritime context.

IHO has created and maintains the baseline S-100 standard which is selected by IMO to be the baseline for all IMO e-Navigation. Within IHO two workgroups (S100WG and DPSWG) are drafting cyber security to be included into the S-100 baseline most probably for 2018 publishing. The S-100 metadata will already amended for edition 2.1.0 publishing to include placeholders for digital signatures.

Since the work on cyber security will be on-going in the timeframe of EfficienSea2, the strategy for Task 2.4 is to base the cyber security considerations on the above mentioned standards and recommendations, as well as standards applied in the IT and Control systems areas along with common IT practices for implementation of risk mitigation controls, like use of firewalls, gateways, authentication, authorization and encrypted communication.

The required security levels depend on the on-board functional areas.

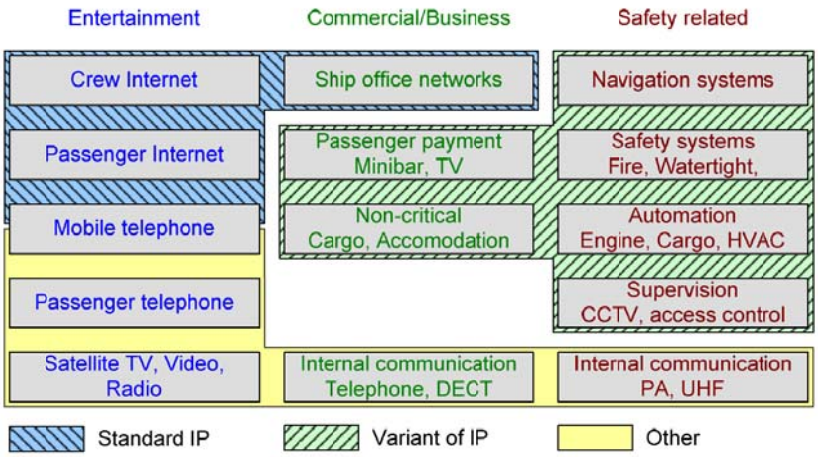

Figure 15 Three areas with different Security requirements (SINTEF, 2005)

In Figure 15 the three areas, Safety related, Commercial/Business and Entertainment have different requirements for control of cyber security and similarly different stakeholders.

In (MARINTECH, 2009) security issues related to ship to shore communication is discussed. Partly as a summary classification of different type of satellite communication carriers and partly a discussion of some remedial actions that can be taken.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

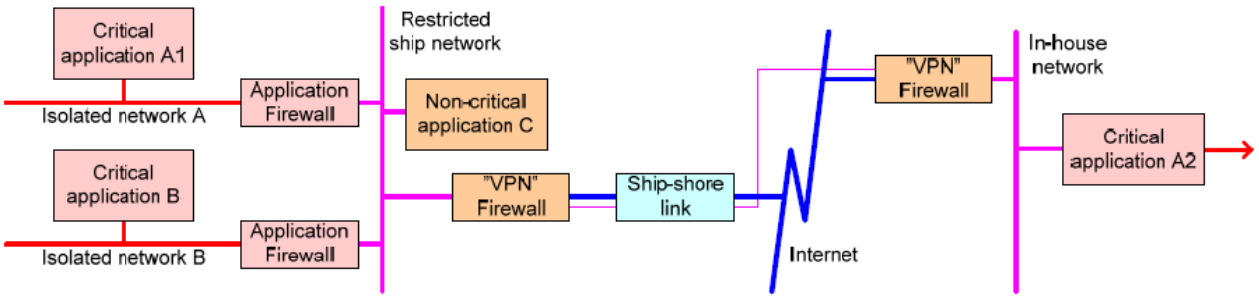

Figure 16 Typical Security Implementation (MARINTECH, 2009)

In Figure 16 a typical security implementation is shown. The different sections with different levels of security requirements are separated using firewalls. Since 2009, a new standard that specifies a firewall to use for on-board security control has emerged, namely the (IEC61162-460, 2015) where the firewall functionality is combined with a gateway functionality and is then called a 460-Gateway.

9.3.1 User Needs described by E2, WP3

The direct requirements extracted from the conclusion in (E2-T3.1, Analysis report on communication and infrastructure, 2015) are the following:

- Disruption of infrastructure functions due to hacking or other types of cyber-attacks could affect a large population of users, and thus such services should be protected against Cyber Security risks
- The level of protection should be at least equivalent to the level of protection required for those systems that depend on the infrastructural functions.

However, the consolidated list of user needs in (E2-T3.1, Analysis report on communication and infrastructure, 2015) has the following cyber security related needs:

- Role based access control (authentication and authorisation)
- Standardized function(s) for validation of authenticity and integrity of transferred information are needed
- The infrastructure must provide standardized means to support encryption of data
- Ownership of information elements, and authorization to pass it on must be managed

9.3.2 Using the NIST Framework for Improving Critical Infrastructure Cybersecurity

Both ABS and BIMCO discuss the use of the NIST framework for cyber security risk management.
The framework amongst others contains the four elements:

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

9.3.3 Cyber Security Risk Identification

Risk identification is the process of determining risks that could potentially impact system operations and data and the possible outcomes
It is important to add that the process includes understanding vulnerabilities and to understand what threats that is relevant.

Many different Cyber Security threats exist and new are appearing. A few relevant to an on-board architecture are listed here.

- Backdoors
- Denial-of-Service
- Direct-access
- Eavesdropping
- Spoofing
- Tampering
- Information Disclosure
- Privilege Escalation
- Exploits
- Social Engineering
- Malware
- Identity Theft
- Password Attacks

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

It is advisable to use Threat Intelligence (ABS, 2016) by consulting and monitor the various sources of threat information:

- United States National Institute of Standards and Technology (NIST), *Guide to Cyber Threat Information Sharing, SP 800-150*, Draft, Oct 2014.
- http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf
- *ii)* United States Department of Homeland Security, "Information Sharing," current.
- http://www.dhs.gov/topic/information-sharing
- http://www.dhs.gov/topic/cybersecurity-information-sharing
- *iii)* United States National Institute of Standards and Technology (NIST), *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, SP 800-171*, Jun 2015.
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
- *iv)* European Union Agency for Network and Information Security (ENISA), *ENISA Threat Landscape 2014*, Jan 2015.
- https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport

9.3.4 Mitigation of Cyber Security Risks using 460-Gateways

9.3.4.1 Mission critical equipment

Some equipment within the navigation system, for example, will require access to data provided by the Maritime Cloud. IEC-61162-460 defines a standardized solution for communicating with such equipment.

Here we can identify two extremes in the range of available equipment:

- 61162-460 compliant equipment inside a fully compliant 460-network. Such equipment is very rare today due to the fact that the -460 standard has been published recently.
- "Legacy" equipment connected in legacy networks. It should be possible to make the Maritime Cloud available for this equipment without degrading their current status of safety and security. A firewall device like the 460-Gateway could be configured for this purpose.

9.3.4.2 Uncontrolled equipment

The 460 network provides security but also places many restrictions. In some cases it may be preferable to allow the connection of some non-critical equipment directly with the cloud. The Maritime Cloud is supposed to provide cybersecurity, so it can be safely accessed from an uncontrolled network. Examples of applications that could be used in uncontrolled networks include

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

- e-Navigation prototype display terminal
- Application for browsing Maritime Service Portfolio Registry
- Application for managing subscriptions to services of the Maritime Cloud

Uncontrolled equipment may use the DMZ inside 460-gateway, but they could also use direct connections such as HTTPS.

From the point of view of 61162-460, the maritime cloud is an uncontrolled network. Connection between such a network and 460 networks is possible through the 460-Gateway, by setting up an application server within the gateway's demilitarized zone (DMZ) to transfer data files.

The use cases are basically reception of data (e.g. chart updates, MSI) and sending of data (e.g. automated reports). Interactive communication needs can perhaps be left to equipment in uncontrolled networks.

Two ways to use the files inside 460-network:

- Move files received from the Cloud manually into the DMZ, and then access them from equipment inside the 460 network. This can be done by network access or even by means of removable media. It will work, but it will not reduce the workload of the mariner compared with current practices.
- Set up automatic transfer of data from the Cloud to the DMZ through network. Define a method or convention to organize data in the DMZ such that it can be easily (or automatically) found and accessed from the equipment inside 460 networks.

The latter method is preferable, and not difficult to do if the data to be transferred is well defined in advance. It is more difficult to make it extensible for new services. On the other hand, the former method will always be available as a fall-back.

9.3.5 Detect and Respond to Cyber Security Breaches

The on-board architecture needs to enable functions to detect cyber security breaches. The only available building blocks are the (IEC61162-450, 2011) and the (IEC61162-460, 2015) standards. These, amongst others, contain requirements for equipment to provide system log information. To support detecting breaches, the architecture must then support the mentioned standards.

The architecture must provide means for responding to security breaches. One cannot predict the nature of the required responses. Short term responses would e.g. include temporary isolation of safety critical networks.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

In many cases, the long term responses require configuration updates of the network components and especially the Firewall/Gateway components. In other cases, it is required to update the software/firmware of the components.

In summary, the architecture must allow for efficient and safe update of component configuration and software/firmware.

9.3.6 Cyber Security Conclusion

Given, the perspective “Requirement of an “open” and harmonized architecture” , the user needs identified in (E2-T3.1, Analysis report on communication and infrastructure, 2015), the available standards for security risk mitigation, such as (IEC61162-460, 2015), The Architectural Candidates needs to be validated against Cyber Security threats and must contain sufficient Security control mechanisms to enable mitigation of the risks.

This could be achieved by:

- Placing (IEC61162-460, 2015) Firewall/Gateways at strategic places in the topology
- Describing Gateway functionality that enables use of role based access control
- Describing standardized methods to encrypt communication between architectural elements and between architectural elements and the off-board elements in the maritime cloud.

Making use of the NIST approached described in chapter 9.3.2 in the validation.

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

10 Stakeholder Concerns (Requirements)

This chapter describes the result of analysis of Stakeholder input to develop a set of requirements for the recommended on-board architecture.

10.1 WP3 User Need analysis

Analysing (E2-T3.1, Analysis report on communication and infrastructure, 2015) reveals that it contains a set of consolidated list of user needs. See

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

Appendix A.

The following list is the set of deduced requirements for the on-board architecture:

- The Architecture must be able to support standardized encryption protocols
- MCC must be present as AE
- T2.3 Roaming must be present as AE
- Architecture must support distribution of broadcasts made by Maritime Messaging Service
- Message Transport Protocol must support reception of acknowledge (Maritime Messaging Service)
- Message Transport Protocol must support compression and continue after LOS (Loss of Service)
- Message Transport Protocol must support encryption
- Architecture topology must not by method or implementation change state of SPOF (single point of failure) areas.
- Architecture must support offline or "silent mode" required functionality. I.e. Inter AE communication must not be affected by on-line/off-line state

10.2 Requirements deduced from Analysis of typical network topology

This chapter analyses a typical network structure on-board a ship, and proposes requirements that will enable proper cyber security risk mitigations as well as allow for implementation of the required classes of services from the maritime service portfolio. Please note that throughout this chapter, when the term REQUIREMENT is noted, it does not mean requirement originating from a resolution or standard, but a notation used to mark a requirement for the recommended architecture to be proposed by this report.

The segmentation of the on-board network is steered by requirements for:

- Prioritisation of traffic according to importance
- Avoidance of congestion (overloading)
- Cyber Security risk mitigations
- Allowing different levels of security

In (Rødseth, Christensen, & Lee) layered network architecture is being presented (Figure 17). The following chapters and network segmentation, does not contradict the general description of the layered abstraction. However, the specific use of VPN and Gateways and the segmentation on each layer are being disregarded due to above mentioned segmentation requirements.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

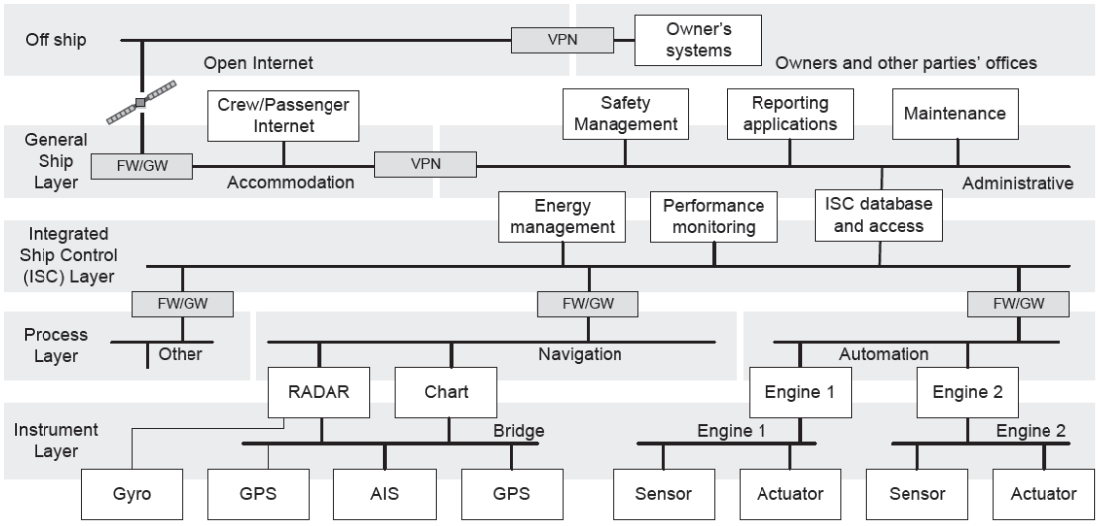

Figure 17 Layered network architecture (Rødset, Christensen, & Lee)

In this analysis, the following domains will be used:

- Accommodation (Crew, Passenger and Infotainment)
- Administration
- Ship Operation

In (SINTEF, 2005), Security requirements are being discussed (**Error! Reference source not found.**)

The Navigation and Automation systems are required to be separate domains where full control of each domain's internal network is crucial - both for security reasons and to ensure the networks are not congested. Typically there are interconnections between e.g. navigation system and automation system (engine) sometimes by using -450 and -460 Gateways – or by dedicated serial lines 62162-1 and -2

10.2.1 Traffic Segmentation

Controlling segmentation of traffic to/from the different domains is vital – both to ensure that e.g. safety related traffic is not suffering from network congestion due to lower priority administrative traffic – or passenger traffic and to reduce security risk of Denial of Service Attacks.
For the part of the traffic that is to be routed to/from shore, the T2.3 roaming needs to be able to distinguish the origin/destination of the traffic to be able to make the right roaming decisions. Separating the network domains by using VLAN is often mistakenly being used as mitigation. If VLAN's are using the same physical connection, it will not mitigate risk of Denial of Service Attacks with origin from e.g. Passenger net.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

Due to this, there is a REQUIREMENT that the EfficienSea2 Task 2.3 roaming must have separate physical ports and network segments for:

- Accommodation (Crew, Passenger and Infotainment)
- Administrative networks
- Ship operation networks (Safety related)

10.2.2 Control of Quality of Service

Quality of Service (QoS) for communication to/from the MSP services needs to be controlled.
Chapter 7.3 Link Requirements and 7.4 Priority provide an indication of the quality of service requirements to the communication links for the various services. For some of the services, in the domain of vessel monitoring and VTS services, adaption to the actual quality of service that can be provided by the communication links, will be required.

Today, the SatCom providers offer services that have user and machine2machine accounting, where management can control allocation of bandwidth, priority and data quotas for users and for M2M communications. In this scenario, the clients (users) of the communication links, if we focus on M2M accounts, are not provided with information of available quota, bandwidth and priority. The M2M clients need to attempt connection and transfer of data and then just get the actual quality of service that can be provided for the specific account in the given communication scenario.

To be able to control and provide the appropriate quality of service in the communication scenarios varying from poor quality in the arctic areas to high quality areas with good VSAT coverage and all the way to excellent quality with very low latency and low bandwidth constraints with Wi-Fi and GSM 3G/LTE, it is envisioned that it is not only the T2.3 Roaming functionality that can implement this on its own. The elements of the Service applications need to have knowledge of the available quality of service at any given time, to be able to make the right decisions when communication is required.

An idea originating from SatCom providers, having M2M accounts to which Quality of Service attributes can be assigned, accompanied with a QoS management functionality, could be utilized.
It could partly be implemented by T2.3 Roaming and partly by the applications (M2M users).
It might also be anticipated that the MC/MCC could centralize functionality that could ease implementation in many of the MSP applications in the M2M mode

It can be concluded that it is REQUIRED that the architecture supports implementation of control of Quality of Service.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

10.2.3 Ship Operation networks

The ship operation networks can be divided into classes, such as:

- Automation Networks
- Navigation
- Safety, Security and Supervision

10.2.3.1 Automation Networks

There may be multiple Automation Networks on-board a vessel, such as:

- Engine Automation
- Energy Automation
- Cargo Automation

In many cases, e.g. these automation networks are part of a closed system where the suppliers of the systems only guarantee functionality with the supplier delivered equipment connected to that network. The supplier may specify and deliver Interfaces (Gateways) to other systems as the means of communicating with the system. Sometimes the network follows (IEC61162-450, 2011).

The operation networks are REQUIRED to be separated using IEC61162-460 Gateway/Firewalls, thus protecting each network from unwanted access and against Denial of Service Attacks.
Further it is REQUIRED to implement interface to the network functions via the Gateway functionality specified by the standard.

It is REQUIRED that the architecture allows for use of proxy services as part of the IEC61162-460 Gateway, to avoid direct communication to endpoints at entities inside the automation network.
This is due to the perspective of easy integration of the recommended architecture that will require allowing endpoints for communication to be inside the protected network.

10.2.3.2 Navigation Network

The navigation network is governed by the IMO Resolution (MSC.252(83), 2007) The Revised Performance Standards for Integrated Navigation System, the original (MSC.86(70), 1998)
and the IEC standards covering the Integrated Navigation System.

Most navigation networks are proprietary solutions, normally based on Ethernet. However, the (IEC61162-450, 2011) forms the base and direction for the network used in new Integrated Navigation Systems.

The (MSC.252(83), 2007) require interfacing to the Central Alert Management system.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

To protect the Navigation Network and the Integrated Navigation System from Cyber Security Threats, and to ensure conformance to the performance standards, it is REQUIRED that the network is protected by (IEC61162-460, 2015) Gateway(s).

10.2.3.3 Safety, Security and Supervision Networks

Safety, Security and Supervision Networks are implementing communication needed to obtain Safety and Security on-board the vessel.
These networks are assumed to be protected from cyber security threats on the highest level. This means that any risk assessment of the ship network should result in mitigations leading to a very low level of risk for these networks.
These networks are REQUIRED to be kept separate from all other networks.
Access to and from these are REQUIRED to be kept under strict control using (IEC61162-460, 2015) Gateway/Firewalls ensuring conformance to the IMO Resolution (MSC.147(77), 2003) Revised Performance Standards for a Ship Security System.

10.2.3.4 Firmware/Software update of equipment on the operative networks

For type approved equipment, the standards define the procedures and methods to follow. Usually update on this type of equipment cannot be done without human interaction and the appropriate verification of functionality after update.

For other types of equipment, various methods of firmware/software deployment exist.
It is REQUIRED that the architecture supports easy and rapid deployment of configuration and firmware/software on certain types of equipment. Especially an organisation should be able to deploy Gateway/Firewall configurations rapidly and in a completely safe manner, to allow for fast reaction to security threats.
Of course, the connections, and the items provided in the update must be secure using encryption, authorisation and authentication using digital signatures.

It is REQUIRED that the architecture must allow for implementation of services for automated deployment of configuration/firmware and software.

10.2.4 Administrative Networks

The ship administrative network is REQUIRED to be a separate domain – both from crew and passenger internet and from Safety related domains. The administration network typically has ability to connect to shore office network. It is REQUIRED that this be done using dedicated VPN connection and that on-board administrative network considered as remote office to the shore based network.

It is REQUIRED that the on-board administrative network only has connection to the public internet via VPN to shore and through shore based company firewall.
This prevents need to manage a multitude of mobile (on-board) firewall entries to the company network.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

Few gateways/firewalls between the secure and non-secure domains are easier to maintain and control and thus less prone to risks due to mistakes.

One can think of examples of multiple operators (companies) with separate responsibilities on one vessel and each requiring an administrative network on-board separated from the others.
In this case, the same principle of separation and remote office is required. I.e. multiple dedicated VPN connections to respective shore networks are required.

In cases where it is needed that equipment on the administrative network has ability to collect information from the Ship operation network. It is REQUIRED that this is done using IEC61162-460 Gateway/Firewalls configured to allow for controlled connections from the administrative network.

10.2.5 Accommodation (Infotainment, Passenger and Crew network)

Infotainment, Passenger and crew network provides connection to the internet and may provide on-board services such as e-mail and media streaming. Compared to the other networks on a vessel, the traffic to/from this network are required to be given the lowest priority.
Since the type of traffic that is generated by the equipment connected to the passenger network are not controlled, it is REQUIRED to be completely separate from other networks on the vessel.
Seen from other networks on the vessel, the passenger network is to be considered as the domain of the public internet.

To protect the T2.3 roaming and the rest of the ship network from Denial of Service Attacks originated from the Passenger/Crew network, it is REQUIRED that either, the roaming device implements detection and protection against such attacks, or the Passenger network is isolated using a IEC 61162-460 Gateway / Firewall. The -460 standard specifies the requirements needed for protection against Denial of Service Attacks.

The Passenger/Crew network cannot be implemented as an IEC61162-450 network, since often there is a need to allow for BYOD (Bring Your Own Device).
BYOD requires DHCP (Dynamic IP Address allocation) – which is not allowed in 61162-450 networks.

The Passenger/Crew network may be implemented as wireless 802.11 networks.

10.3 Deduced, Assumed and/or obvious Requirements

For completeness of the set of requirements, this chapter states a set of assumed and/or obvious requirements.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

- E2 Task 2.1 VDES Communication Functionality must be present as AE
- SAT Broadband must be present as AE
- E2 Task 2.3 Roaming must be present as AE

10.3.1 Concurrency

Architecture must support concurrent provision of services according to SLA given by configured prioritisation and allocated bandwidth for the associated communication to/from ship.

10.3.2 Opening discussion on how AIS functionality is implemented

Regulation 19 of SOLAS Chapter V - Carriage requirements for shipborne navigational systems and equipment - sets out navigational equipment to be carried on board ships, according to ship type. Resolution A.917(22) provide guidelines for the on-board operational use of shipborne automatic identification systems (AIS)

The function of the AIS can be split in several parts. One way is to have a transponder part and a communication of AIS data part. This chapter provides the rationale for doing that.

Imagine if the architecture and network infrastructure, as purely TCP/UDP/IP based, was in place. Then implementation AIS functionality would be different from what we see today.
The AIS function would quickly be split in two parts. One the transponder functionality (or service) and the other would be the function of communication of AIS data.

Since the (RFC1122, 1989) is already in place and most of the worlds internet services and data formats are being specified as WEB services, it would be natural to define the AIS functionality with the standards, tools and methods available in that domain.
It would also very quickly become obvious that communication of AIS data could not only happen via VHF channels, but also via broadband satellite channels.

With the current suggestions of the MC and the MCC messaging service, the ASM part of AIS would very quickly be functionality implemented using MCC messaging services.

With the current suggestions in the standardisation work of VDES, combining IP data exchange on some VHF channels and AIS and ASM data exchange on other channels, and implementing both parts in one physical unit leads to a concern for cyber security risks. It should be noted that, at this time of writing (April 2016), the role of VDES is uncertain and clarification could change above statement.

Since the IP data exchange part would have some connection to the public internet, the unit would be prone to cyber security threats originating from the internet domain.
With connections on the AIS part, directly into the Bridge navigation system, the navigation system would be in risk.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

Therefore one would implement the AIS function so that AIS data would be routed and handled the same way as other traffic, ensuring security using -460 gateways.

In the suggested architecture, the AIS function has been split in the above mentioned parts and the T2.3 roaming is expected to handle the appropriate routing and prioritisation of AIS traffic.

This discussion and the architecture proposal, does not prevent implementations where AIS/ASM function is kept the way that legacy provides – namely using the products available today and then implementing the VHF data exchange (of IP based data) using a VDES modem.

The E2 T2.3 has developed a model as shown in
Figure 18.

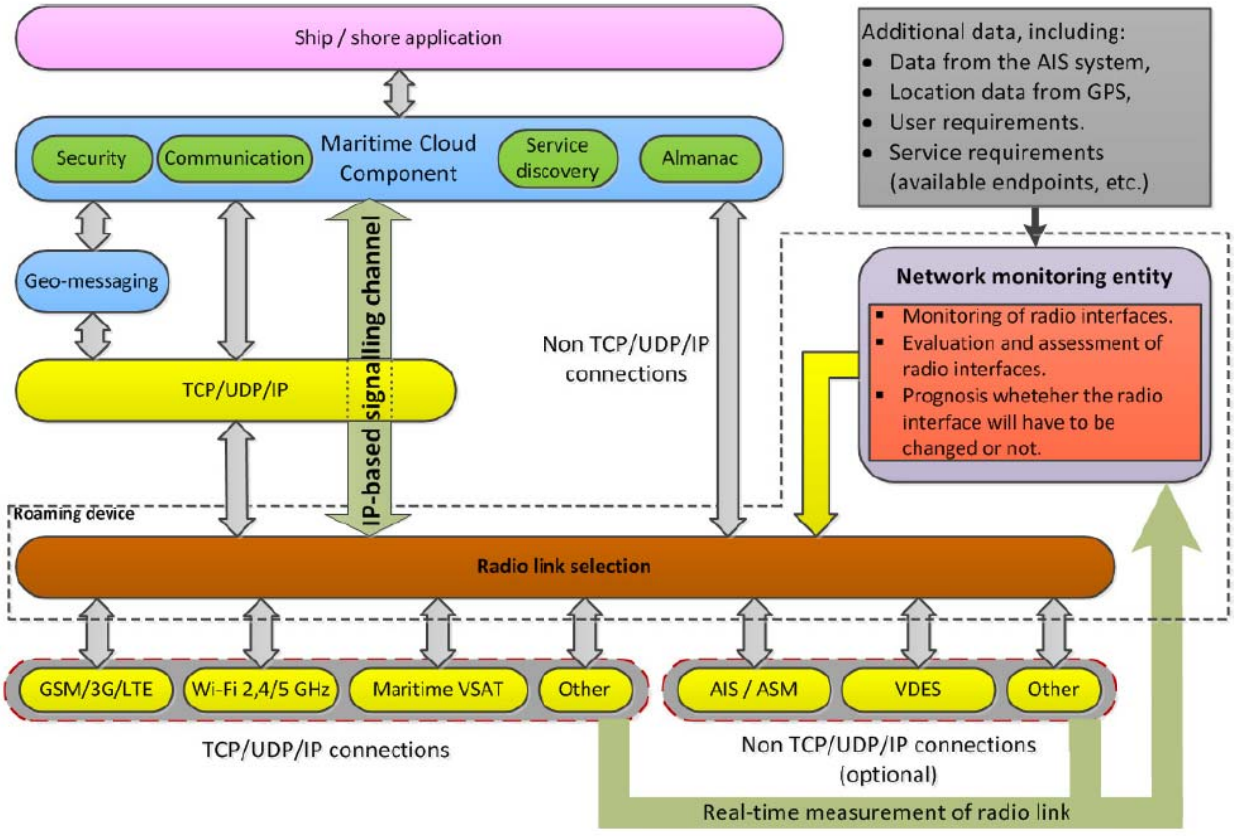

Figure 18 The E2 T2.3 architecture of the Maritime Cloud client connected with the components of the hybrid

With the discussion opened here and the suggestions in 7.6.3 Broadcast Message Service, the Network protocol model simplifies as shown in
Figure 19 Network Protocol Model.
Hence, this model has no “Non TCP/UDP/IP” path.

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

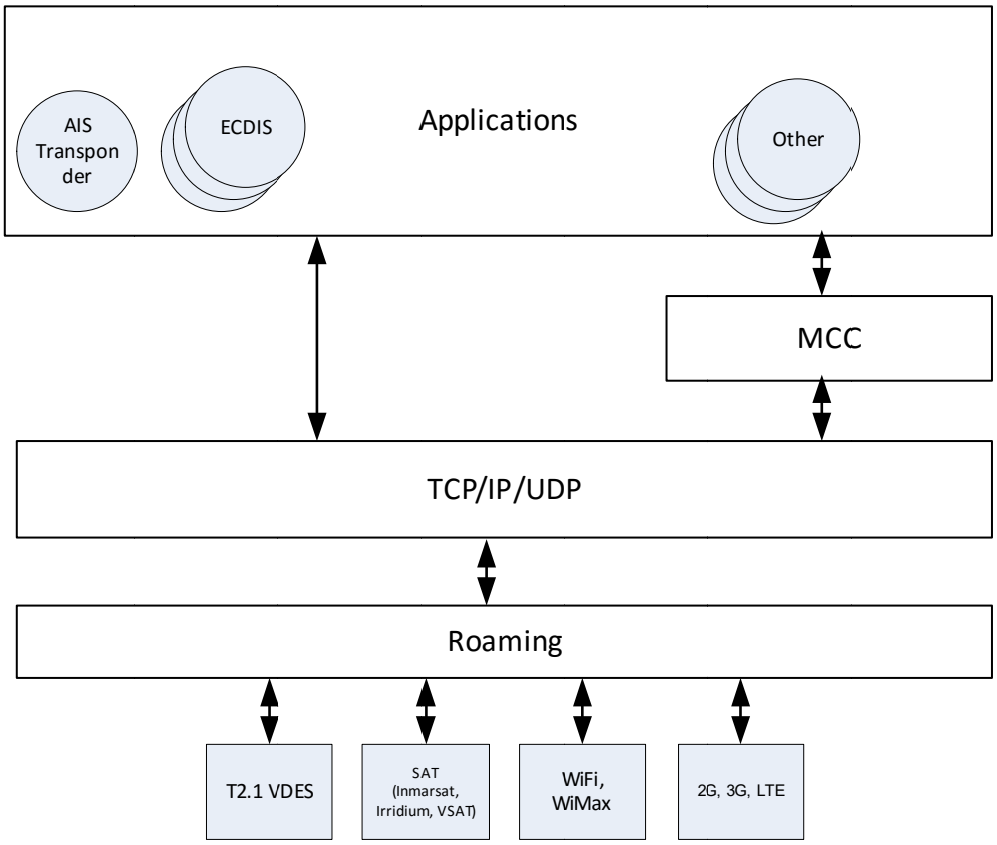

Figure 19 Network Protocol Model

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

11 Architectural Candidates

This chapter describes one architectural candidate that has been developed during the work of T2.4 until this moment of writing.
To ease the reading, the chapter starts to describe the most simple implementation as a before implementation and after implementation example and then a description of the full network topology.

11.1 Simplest Implementation

Figure 20 and
Figure 21 illustrate before and after implementation done e.g. on a ship with low maturity with respect to on-board network and ship/shore data communication. In this example, the ship, before implementation has one Ethernet network segment that may not even have elements like ECDIS attached to it.

The automation systems are connected to bridge control panels via either serial lines or on the same network segment. The rest of on-board communication is done via serial lines IEC61162-1 and -2.

In this example, it is imagined that the argumentation for doing the installation is to implement e-navigation and Vessel monitoring, hence IEC61162-450 connectivity to ECDIS and VDR.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

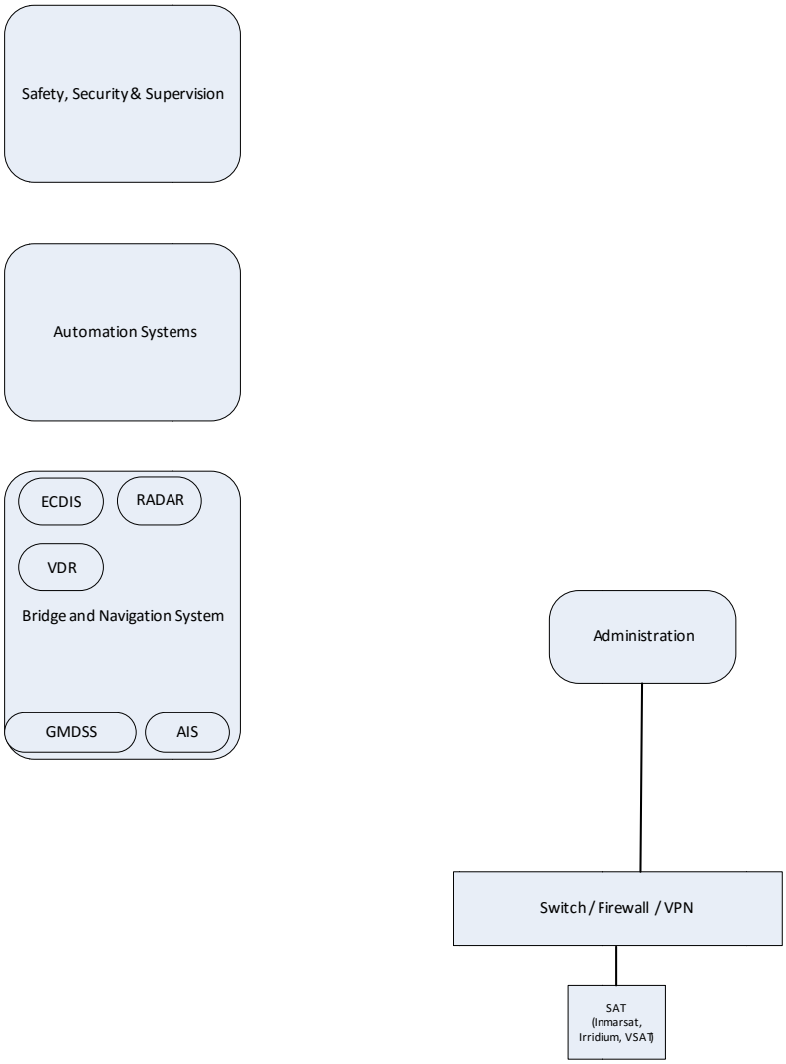

Figure 20 Simplest Situation – Before Implementation

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

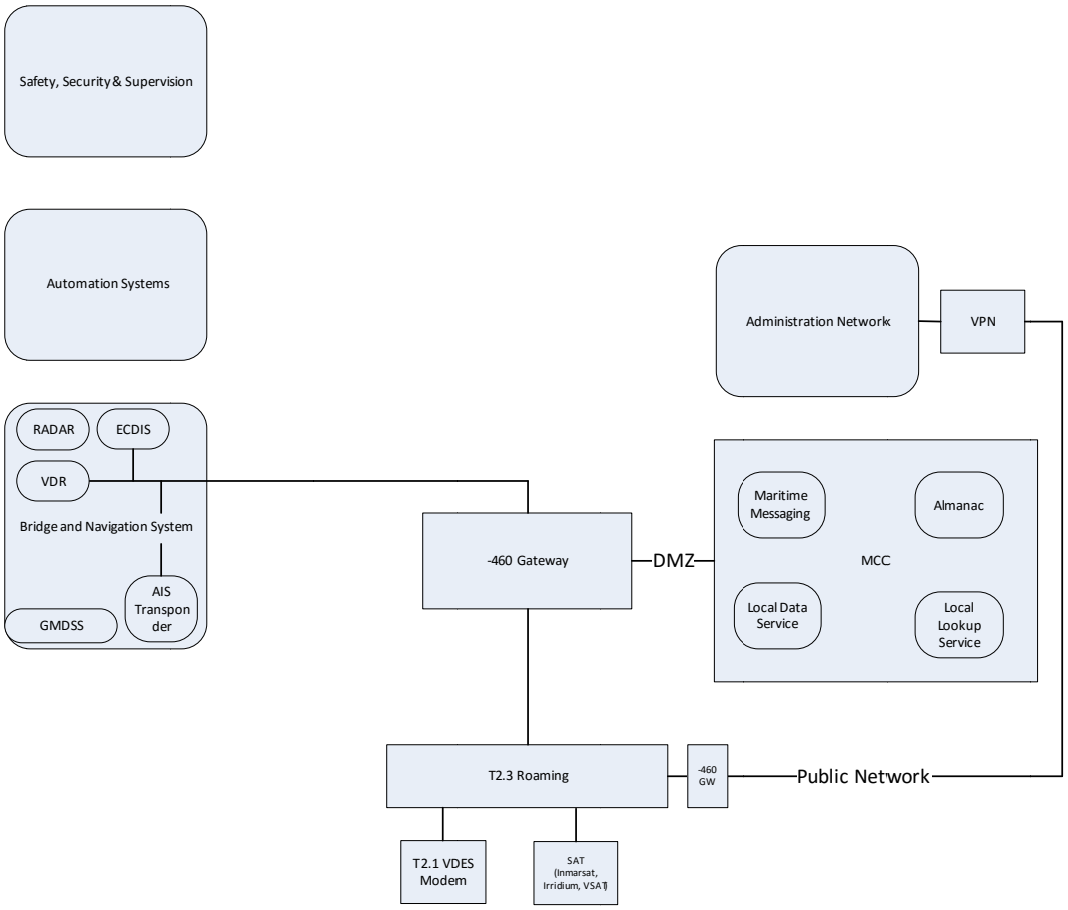

Figure 21 Simplest Situation – After Implementation

11.2 Network Topology

Figure 22 Network Topology shows the top level network topology of the suggested architecture. The required architectural elements are included in the drawing.

The MCC is in the figure, placed as a part of the main -460 Gateway. It should be noted that it is still a discussion if MCC exist on-board in multiple instances. I.e. in every -460 gateway. It is, at this point in time (April 2016), unclear how multiple MCC instances would work together and how to avoid duplicate information to be communicated over the sparse communication channels.

It is uncertain, at this point in time (2016-04), what VDES is going to provide on IP side. Therefore the VDES, as used in the architecture, is assumed to provide IP connectivity only.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

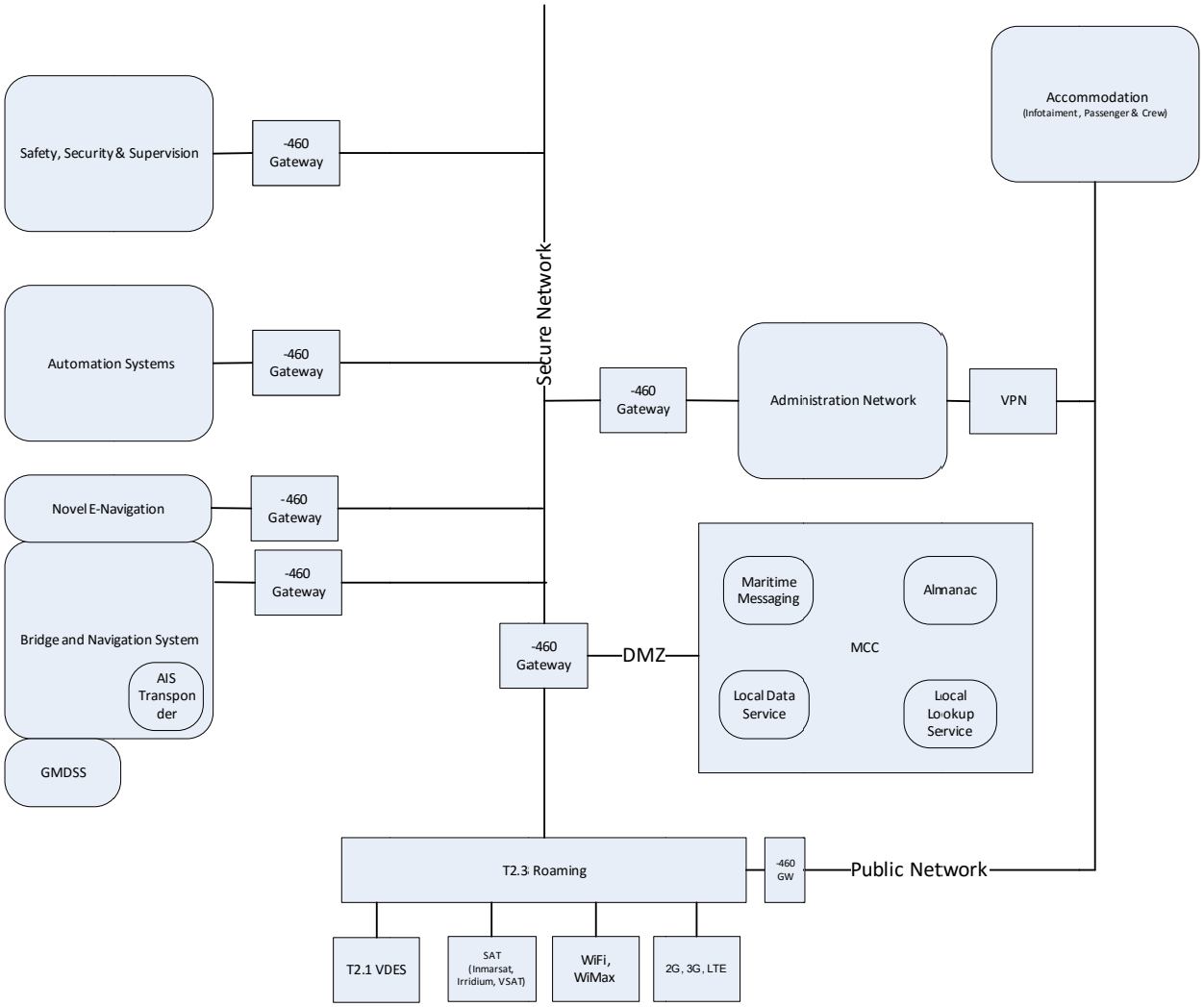

Figure 22 Network Topology

11.3 Integrated Communication System

The shipborne integrated communication system (ICS) is designed to perform ship external communication and distress and safety communications (GMDSS) and the functions of onboard routeing of this communication.

The design requirements to an Integrated Communication System are based on the of the IMO performance standards for integrated Radiocommunication Systems, and other relevant IMO resolutions and circulars. For interconnection of the elements of the ICS, the solution is based on applicable requirements for Ethernet interconnection in IEC 61162-450.

The ICS is a system in which individual radiocommunication equipment and installations are used as subsystems, i.e. without the need for their own control units, providing outputs to and accepting inputs from a communications human machine interface (COM HMI). Each subsystem is in compliance with the IMO type approval requirements for that subsystem where applicable, An ICS consists of at least two individual GMDSS subsystems.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

The COM-HMI is designed so that it can be made available on a bridge workstation either dedicated to communications or as part of a multi-function display.

Figure 23 illustrates the relation to this up-coming IEC standard on Integrated Communication System (IEC62940-ICS, 2016).

The domain of the ICS has been marked with red and yellow dashed lines. The yellow one shows how the gateway and MCC can be included in the ICS.
The “yellow” integration needs to be amended with a note that to mitigate cyber security risk, the implementation should be done on separate autonomous units.

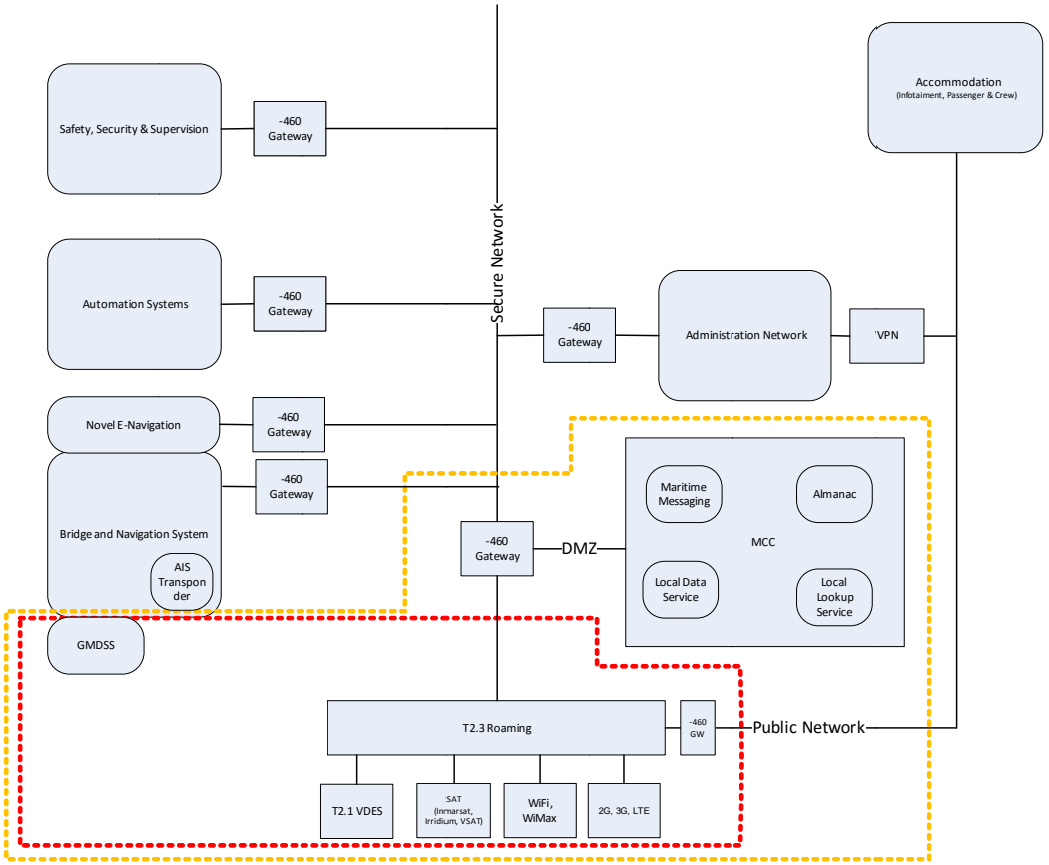

Figure 23 The integrated Communication System

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

11.4 Integrated Gateways

In case where the Automation System and the Bridge and Navigation System components conforms to the Service standards offered by the MC and MCC, the role of the -460 Gateway is simplified by the fact that no translation between proprietary protocols is needed. Hence the gateways can be integrated into one. See Figure 24.

Figure 24 Integrated Gateways

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

11.5 Quality of Service

To allow the service clients to make intelligent decisions on how to use the available quality of service that the communication links allow in certain situations, it is suggested that service clients have the option of implementing a QoS client that can interface with a QoS server implemented in the T2.3 roaming.

Figure 25 illustrates suggested architecture for QoS implementation.

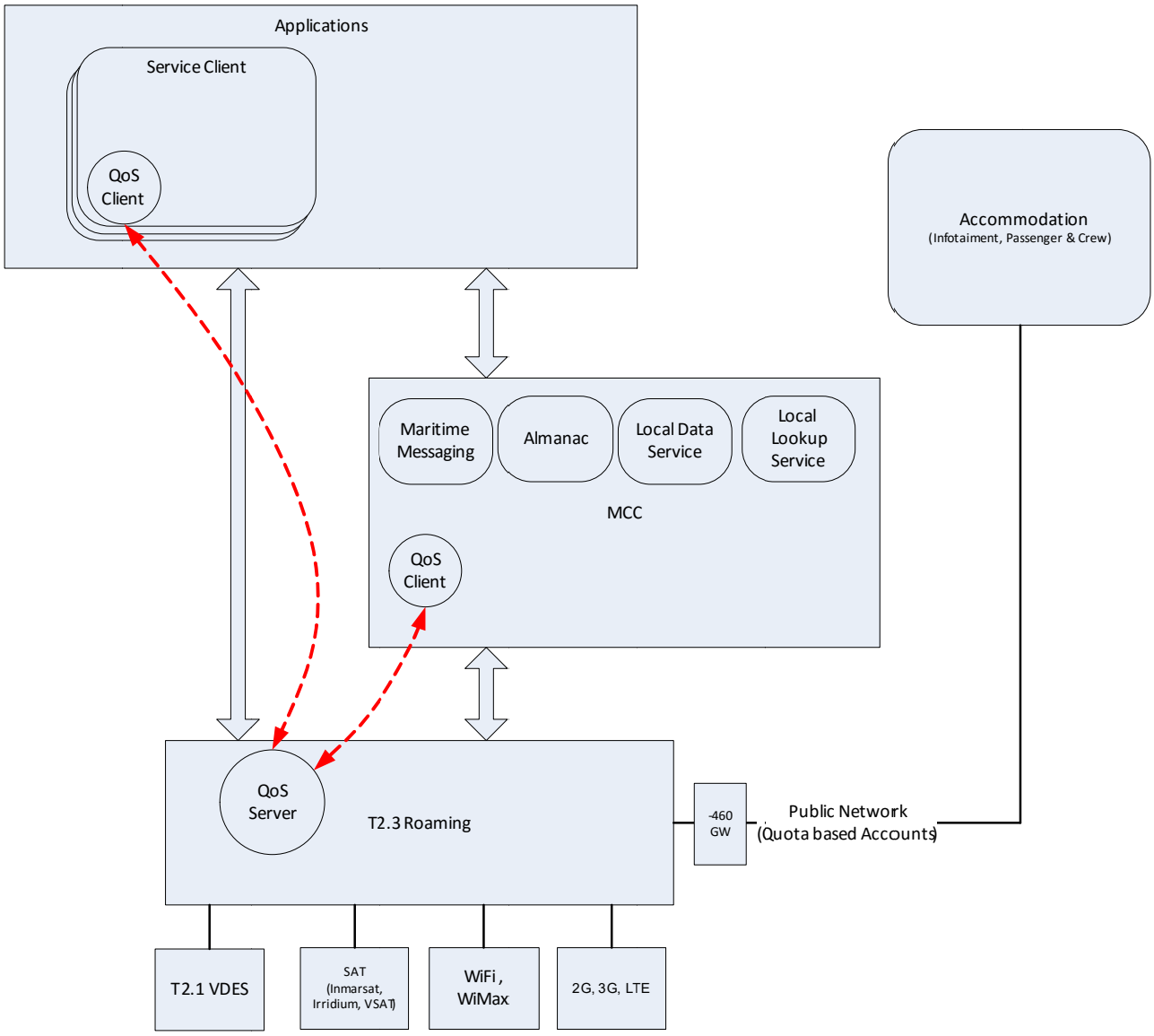

Figure 25 QoS Client/Server Architecture

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

12 Architectural Candidate Test Results

It is suggested that the proposed architecture fulfils the requirements as described in chapter 9 Perspectives and chapter 10 Stakeholder Concerns (Requirements).

13 Identification of potential Areas for standardization

This chapter is included to provide input to E2 WP1.

During the work of T2.4 producing this document, the following have been identified as potential areas for standardization.

- Inclusion and standardisation of MCC as extension/addition to the (IEC62940-ICS, 2016)
- Data formats and protocols used for the defined services in MSP, several of these can be extensions in the S100 framework.
- Quality of Service Control for the ship/ship and ship/shore communication

14 Conclusion

Proposed architecture is believed to fulfil the user needs as described by WP3.
Since the stakeholder input is described as user needs on a rather high level, the proposed architecture is not based on a full and reviewed set of requirements from the stakeholders, the architecture is, therefore, likely to be modified or extended in the next phase of the E2 Task 2.4 work.

Based on Cyber Security Perspectives, a set of requirements have been developed and it is believed that the proposed architecture provides sufficient means for security risk mitigation, partly in the structure and suggestions for network separation, and partly by the use of (IEC61162-460, 2015) gateways.
Cyber Security Perspective needs to be included in the further work for T2.4, since the choices of communication protocols to be used are to be done there.

Considerations on the impact when implementing the recommended architecture have been discussed and it is suggested that the architecture provides a framework that allows for gradual implementation. Also it is suggested that “transformation” to the architecture can be done with installation of few components in existing on-board infrastructures.

The perspective of providing an open and harmonized architecture has been defined, and it is suggested that the proposed architecture is delivering the basis for exactly that.
One of the consequences is the fact that it is proposed that all communication to/from the ship (except GMDSS), is centralized through the T2.3 Roaming function and that it is to be based on standardized network, using standardized protocols and data formats.

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

Bibliography

ABS. (2016). *The Application of Cybersecurity principles to marine and offshore operations.* Houston: American Bureau of Shipping.

ACCSEAS. (2015). *S-100 Product Description: Maritime Safety Information / Notice to Mariners Service.* ACCSEAS.

ACCSEAS. (2015). *Service Description: Maritime Cloud.* ACCSEAS.

ACCSEAS. (2015). *Service Description: Maritime Safety Information and Notice to Mariners Service.* ACCSEAS.

ATOMOS. (1994). Retrieved 01 22, 2016, from CORDIS: http://cordis.europa.eu/project/rcn/17378_en.html

ATOMOS II. (2000). Retrieved 01 16, 2016, from CORDIS: http://cordis.europa.eu/result/rcn/23723_en.html

ATOMOS IV. (2002). Retrieved 01 16, 2016, from CORDIS: http://cordis.europa.eu/project/rcn/52030_en.html

BIMCO. (2016). *The Guidelines on Cyber Security Onboard Ships.* BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO.

DISC. (1997). *Brief Summary of Final Report, DISC Document ID D101.00.01.047.005B.* The DISC Consortium.

DISC. (2001). Retrieved 01 16, 2016, from CORDIS: http://cordis.europa.eu/project/rcn/44674_en.html

DISC II. (n.d.). Retrieved 01 16, 2016, from TRIP - Transport Research and Innovation Portal: http://www.transport-research.info/project/integrated-ship-control-system-practical-demonstration

E2-T2.2. (2016). *E2 Task 2.2 Analysis report on available and emerging communications technologies.* EfficienSea2.

E2-T3.1. (2015). *Analysis report on communication and infrastructure.* Jens K. Jensen, DMA - Peter Petersen, GateHouse.

E2-T3.1. (2015). *D3.2 Conceptual Model.* EfficienSea2.

ENISA. (2011). *ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR.* European Network and Information Security Agency (ENISA).

IACS. (n.d.). *IACS.* Retrieved 01 29, 2016, from IACS: http://www.iacs.org.uk/document/public/Publications/Unified_requirements/PDF/UR_E_pdf150.PDF

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

IEC 60945. (2002). *IEC 60945 - Maritime Navigation and Radiocommunication Equipment and Systems - General Requirements - Methods of Testing and Required Test Reaults.* Geneva: IEC.

IEC61162-450. (2011). *Multiple talkers and multiple listeners - Ethernet interconnection.*

IEC61162-460. (2015). *Multiple talkers and multiple listeners - Ethernet interconnection - Safety and Security.*

IEC62940-ICS. (2016). *IEC62940 - Integrated Communication System.* IEC.

IHO. (2009). *S100 - HYDROGRAPHIC GEOSPATIAL STANDARD FOR MARINE DATA AND INFORMATION.* International Hydrographic Bureau.

ISO/IEC42010. (2011). *Systems and Software Engineering - Architectural Description.*

MARINTECH. (2009). *European Framework for Safe, Efficient and Environmentally-friendly, D-D1.3 Ship-shore communication.* FLAGSHIP.

MSC.147(77), I. (2003). *REVISED PERFORMANCE STANDARDS FOR A SHIP SECURITY ALERT SYSTEM.* IMO.

MSC.252(83), I. R. (2007). *ADOPTION OF THE REVISED PERFORMANCE STANDARDS FOR INTEGRATED NAVIGATION SYSTEMS (INS).* IMO.

MSC.86(70), I. (1998). *Adoption of new and amended performance standards for navigation equipment.* IMO.

NSCR-1/28. (n.d.). *E-NAVIGATION STRATEGY IMPLEMENTATION PLAN.* IMO.

RFC1122. (1989). *Requirements for Internet Hosts -- Communication Layers.* IETF.

Rødseth, Ø. J., Christensen, M. J., & Lee, K. (n.d.). *Design Challenges and decisions for a new ship data network.*

Rozanski, N., & Woods, E. (2013). *Software Systems Architecture, Working with Stakeholders Using Viewpoints and Perspectives.* ISBN-13> 987-0-321-71833-4.

SINTEF. (2005). *Marnis, WP2.2 Broadband Communication - State of the Art.*

The MiTS Forum. (2015). Retrieved 01 16, 2016, from The MiTS Forum: http://www.mits-forum.org/

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

15 Appendix A – Consolidated User Needs

This chapter list the consolidated user needs, extracted from (E2-T3.1, Analysis report on communication and infrastructure, 2015). The list is amended with an extra column stating the deduced requirements to the T2.4 on-board architecture.
The user need “No” column tags are shortcuts:

- ID is about Identity management and role based access control
- SD is about Service definition and discoverability
- SR is about Seamless roaming
- MS is Miscellaneous

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

No.	Need	Notes	Task 2.4 Requirement
ID#1	All types of Ships as well as a multitude of shore based or Off Shore entities must be able to interact, and Digital Identity of interacting actors must be manageable	See Wikipedia for an overview of definitions related to digital Identity Management. https://en.wikipedia.org/wiki/Identity_management In the maritime domain entities such as companies, authorities, ports, ships as well as employees or operators with assigned roles/responsibilities (such as ships' captain, VTS operator or harbour master) must be identifiable.	
ID#2	A digital UID (Universal Identifier) concept must be defined for the Maritime Domain, which is flexible, decentralized and forward compatible, yet provide unique identifiers for different actors.	An Identity concept that can provide one binding, unique identifier that can cover the Maritime Domain must be The identifier concept could be a maritime adoption of the URI (Universal Resource Identifier) https://en.wikipedia.org/wiki/Uniform_Resource_Identifier	
ID#3	A UID registry is needed, which can uniquely identify an actor, and facilitate lookup of secondary identifying attributes	Not all actors have MMSI numbers, however MMSI numbers play a significant role in several existing GMDSS and dedicated maritime communication systems In other cases identifiers such as terminal numbers, or e-mail addresses could be used to identify an actor The UID registry must enable binding (lookup) between existing identifiers and a unique UID It must be possible to decentralize the process of assigning identities As such, the UID registry may be decentralized, but lookup of identities and associated identifiers must be possible across the Maritime Domain.	
ID#4	It must be possible to associate identities with roles The role concept should be flexible, decentralized and forward compatible, allowing unique role definitions for different responsibility domains	Standardized roles may be defined by certain stakeholder groups to manage which identities are associated with certain responsibilities and entitled to which level of access In using role based access management, a role belongs to a responsibility domain, where a specific responsibility belongs to one role, eg. IMO could define the roles of a 'Flagstate', 'Coaststate' or 'Portstate', and delegate authority to competent authorities of its member states to assign such roles to identities executing tasks related to those responsibilities EU could most likely reuse roles already defined relevant to information sharing within the e-maritime concept An actor/identity may be assigned more than one role	
ID#5	Unique Identifiers for virtual objects (such as information objects) are paramount for some use cases and should be considered in relation to developing a maritime UID concept	Example: A Voyage_IDs identifying a particular voyage of a particular ship, or a Persistent Universal Identifier for an Aid to Navigation Identities related to objects that are not actors and need authentication may belong to other registers, than the Identity register related to actors that need authentication.	
ID#6	Standardized function(s) for Authentication of identities is needed	The ability to validate the identity of an actor requesting access to restricted information or a resource is needed by many use cases to facilitate access control Common authentication function(s) is(are) needed, to avoid all services implementing their own authentication function, requiring actors to maintain password lists for all systems they need to access	
ID#7	Standardized function(s) for validation of authenticity and integrity of transferred information are needed	It must be possible to 'sign' a digital document in such a way, that the recipient can validate the origin of the information and detect if it has been modified Certificates may need to be part of some data transfers.	
ID#8	The infrastructure must provide standardized means to support encryption of data	In order to support transfer of confidential information	The Architecture must be able to support standardized encryption protocols
ID#9	Ownership of information elements, and authorization to pass it on must be managed	The infrastructure must not pass on information to unauthorized parties Privacy of confidential information transfer must be addressed – technically as well as legally, including requirements for legal interception (law enforcement). A digital service provided based on this infrastructure must be explicit about ownership of information and authorization to pass on information Standardized functions supporting Nomination of collaborators (roles or specific identities who are entitled to access my information) could ease implementation of many information services	N/A
ID#10	Vetting of identities would increase the credibility of identities and facilitate a higher degree of trust in online business relationships or sharing of information within the industry	Vetting: Validation of relationship between legal entity and digital identity – for instance a flag state validating the relationship between a ship and an associated digital identity (identified by UID, IMO number or MMSI number, etc.)	N/A

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

No.	Need	Notes	Task 2.4 Requirement
SD#1	The infrastructure should provide a Service Registry / lookup function		MCC must be present as AE
SD#2	A standardized description of a digital service should include a functional description, user presentation issues (where relevant), operational context and definition of data formats	Geographic context and level of criticality of a service could be part of the operational context	
SD#3	A standardized service description language could facilitate service implementation		
SD#4	A standardized description of a digital service must describe how privacy of information is ensured, if confidential information is exchanged with the service	Technical as well as legal aspects must be covered including stating which national (or international) legislative regime cover the provider of the service	
SD#6	Standardized methods for setting up subscriptions to a service should be developed		MCC must be present as AE
SR#1	Actors should be able to interact without using the same point-2-point radio link or the same satellite system (seamless roaming)	Seamless roaming - i.e. a carrier agnostic or cross carrier communication service - should be available (The proposed Maritime Messaging Service) This will require a shipboard messaging application, which can offer other shipboard applications a connection to a shore based messaging service, while automatically switching between a number of different communication links, based on availability, capacity, cost or other	Roaming must be present as AE
SR#2	A Messaging Service should support the capability to broadcast information to actors inside an area (or actors subscribing to information in an area or along a route)	Geocasting (broadcasting to an area) will require the roaming service to be aware of mobile actors location or the 'listening area' of fixed actors Precision and timing requirements for updating the location of mobile actors has not been determined	MCC must be present as AE Architecture must support distribution of broacasts
SR#3	Support for setting up dynamic multicast groups for multicasting information only to actors related to a particular operation is requested	(like subscribing to a chat room for sharing certain operational information related to an operation)	MCC must be present as AE
SR#4	Although not part of the GMDSS, any roaming capability should be designed to support the operational priorities defined for GMDSS (Distress, Urgency, Safety, Routine) in executing queues of information transfer	Based on advice from the High Level User Group, the infrastructure functions should *not* initially aim for supporting safety critical applications, but its inherent design should not prevent upgrading the operational status at a later stage, if the functions prove successful and become widely used.	Covered by the Open and Harmonized Perspective
SR#5	A Messaging Service should support requesting acknowledge of information delivery	Acknowledge mechanisms could exist at different levels - a communication link level acknowledge of information delivery, an application level acknowledge of information received at a relevant application, or a user acknowledge	Message Transport Protocol must support reception acknowledge
SR#6	Legal implications of the components of a Messaging Service must be considered – including requirements in national or international law related to lawful interception.		
SR#7	A Messaging Service should support the ability to distribute messages to ships outside range of stable connectivity	May require store-and-forward queuing capabilities, and ability to provide 'delivery delayed' or 'not connected' statuses in relation to requirement for delivery acknowledge.	
SR#8	A Messaging Service should support methods for bandwidth efficient transfer of data	Efficient methods for encoding or compression of data should be applied In case of a temporarily lost connection during an ongoing transfer of a large data block, the process should be able to continue after a reconnect, rather than starting the transfer over.	Message Transport Protocol must support compression and continue after LOS (Loss of Service)
SR#9	A Messaging Service should support encryption for confidential transfer of data		Message Transport Protocol must support encryption
SR#10	A Messaging Service should support text messages with non-standardised content The text-chat function could be used to clarify other standardised information exchange e.g. explain reason for changed time of arrival	Standardized expressions, such as Maritime Standard Phrases, could be supported.	
MS#1	Introduction of the infrastructure should not require major modifications of existing systems	The infrastructure functions should rather allow a gradual transition towards better service designs, providing improved and unified access control mechanisms, enabling automation of interactions with minimal user attention	Covered by the Low Impact Integration with existing infrastructure perspective
MS#2	Introduction of the infrastructure should not introduce single points of failure, which may prevent interactions between maritime stakeholders due to disrupted operation	Infrastructure functions should as far as possible not require online access to centralized systems, but should be able to be replicated and function offline or in a decentralized manner	Architecture topology must not by method or implementation change state of SPOF areas. Architecture must support offline or "silent mode" required functionality. I.e. Inter AE communication must not be affected by on-line/off-line state
MS#3	A business case for operating the infrastructure functions should be identified	Supported by comments from HLUG	
MS#4	Legal implications of establishing the infrastructure functions should be analysed and addressed	Supported by comments from HLUG	
MS#5	The roadmap towards establishing infrastructure functions should include establishing test beds and developer forums, where technologies can be tested and validated, and allow room for agile adaptation of technology developments	HLUG also requested a roadmap	
MS#6	The level of criticality of the infrastructure functions must be defined		

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

16 Appendix B – Final Review Report

This chapter list the review comments received and action on comments from the final review of this report.

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
1	NIT	page 42, par.10.2.1	formulation	The sentence: „*Due to this, there is a REQUIREMENT that the EfficienSea2 Task 2.3 roaming device must have separate physical ports and network segments for (…)"* is not compliant with the results and outcome of Task 2.3. The roaming device from the EfficienSea 2 Task 2.3 will not be equipped with several separate physical ports – there will be only one physical port. Network segments will be separated logically.	After correspondence with NIT and input from review meeting 2016-04-16, editor has decided to stick with requirement for two physical ports in the report. The means of witch this is achieved are to be discussed and decided in the next phase of E2 T2.4 and T2.3
2	NIT	page 42, Par. 10.2.2	formulation	Comment refers to the sentence: „*The elements of the Service applications need to have knowledge of the available quality of service at any given time, to be able to make the right decisions when communication is required."* The services are performed via Maritime Cloud and it is in Maritime Cloud where the required QoS and necessary endpoints are determined. The EfficienSea 2 Task 2.3 roaming device will select the most suitable transmission link which will depend on the required QoS and endpoint. The information about the QoS that is currently available in the link may be logically distributed to relevant network components but cannot be modified by them – such a modification can only be performed by the Maritime Cloud.	… stick to QoS way of drawing

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
3	NIT	page 45, par. 10.2.5	formulation	Comment refers to the sentence: „ *To protect the T2.3 roaming and the rest of the ship network from Denial of Service Attacks originated from the Passenger/Crew network, it is REQUIRED that either, the roaming device implements detection and protection against such attacks, or the Passenger network is isolated using a IEC 61162-460 Gateway / Firewall.*" To clarify the matter: the EfficienSea2 Task 2.3 roaming device will not be equipped with ANY modules detecting attacks and/or protecting against them. Passenger network must be isolated using a IEC 61162-460 Gateway / Firewall. So, out of the two possibilities included in the cited sentence from D.2.10, the second one is true.	The sentence has been extended to note that -460 gateway/firewall is required in E2.
4	NIT	Fig. 22/23/24/ 25/26	formulation	The EfficienSea2 Task 2.3 roaming device will not be equipped with separate physical ports. Public Network should be separated using the Gateway / Firewall.	Figures updated to show GW
5	NIT	Fig. 26	formulation	The EfficienSea2 Task 2.3 roaming device might send the QoS information logically to relevant network components, but it will not be equipped with the QoS Server.	Definition of the QoS functionality in T2.3 roaming and the service clients are to be discussed and decided in the next phase of E2
6	NIT	Par. 7.1.3	structural	In par. 7.1.3 a definition of broadcast communication is given. In many documents regarding the Maritime Cloud, the terms "geocast" and "broadcast" are used interchangeably. We acknowledge, that this fact was observed by the authors later in paragraph 7.6.3, but to avoid possible confusion, we believe a similar statement should be included in paragraph 7.1.3 as well.	Formulation of definition expanded. Geocast can be a special case of broadcast. Geocast could also be distributed using multicast.
7	NIT	General	editorial	To mention Quality of Service, the authors use the acronym 'QOS', instead of the most common form – 'QoS'. It should be corrected, since 'QOS' usually refers to „Quality Operating System" - http://www.acronymfinder.com/Quality-Operating-System-(QOS).html	Fixed.
8	NIT	General	editorial	There is a relatively big number of spelling and punctuation mistakes. A few examples below:	Fixed (I hope)
8a	NIT	Page 49	editorial	It is: "*Figure 22 and Figure 22 illustrates*…"	Fixed

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
		Par. 11.1		It should be: "*Figure 21 and Figure 22 illustrate*…"	
8b	NIT	Fig. 8	editorial	It is: "Shios" It should be: "Ships"	Fixed (I hope)
8c	NIT	Fig. 8	editorial	It is: "Shpis" (x2) It should be: "Ships"	Fixed (I hope)
8d	NIT	Fig. 9	editorial	It is: "Tasl 2.4" It should be: "Task 2.4"	Fixed (I hope)
8e	NIT	Fig. 13	editorial	It is: "Shios" It should be: "Ships"	Fixed (I hope)
8f	NIT	Fig. 13	editorial	It is: "Shpis" (x2) It should be: "Ships"	Fixed (I hope)
8g	NIT	Page 40, 1st sent. in par. 10.2	editorial	It is: "*This chapter analyse a typical network structures on-board a ship, and propose requirements*(…)" It should be "*This chapter analyses a typical network structures on-board a ship, and proposes requirements*(…)"	Fixed
8h	KB (NIT)	Page 43, Par. 10.2.2	editorial	It is: "*The idea from the SatCom providers, of having M2M accounts to witch Quality of Service attributes (…)*" It should be: "*The idea from the SatCom providers, of having M2M accounts to which Quality of Service attributes (…)*"	The paragraph was confusing. It has been Reformulated.
9	AW	Ch 2 para 1 sentence 2	Editorial	The scope **of** …[not for]	Fixed
10	AW	Ch 3	Ditto …	Definition of MCC – Maritime Cloud Client Component?	Fixed
11	AW	Ch 4 para 1	…	Possible redraft: the concept of considering the entire electronic infrastructure of a ship as a sub-system of the maritime cloud is not possible due to the rules and regulations that apply to equipment in the maritime domain. However, a limited application of the concept is	Found both formulations hard to read, so stayed on existing one.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				possible on novel parts of those parts of the shipboard architecture that bind the maritime cloud client component (MCC) to existing type approved systems.	
12	AW	Ch 4 para 2	…	Redraft? ....on board MCC and to identify and describe a suitable on-board architecture a recognized standard has been used (the ISO/IEC…) in this report.	Paragraph reformulated.
13	AW	Ch 4 para 4	…	The process to follow and the steps taken to provide a recommended architecture is illustrated in Figure 1.	Suggested formulation used.
14	AW	Ch 4 para 5.1	Formulation	Reviewer Comment: EQUASIS 2014 figures are 85,094 ships in world fleet (over 100 GT) of which 31,240 were less than 500 GT – so taking one from the other the number of SOLAS ships (generally taken to be those of over 500 GT notwithstanding the fact that some provisions are for ships of over 300 GT) is 53,854 in 2014. The UNCTAD Review of Maritime Transport 2015 has a higher figure for the total of 89,464. The ICS website quotes a figure of approx. 50,000 ships trading internationally. The text referring to SOLAS ships and small ships and replacement rates is therefore a bit confusing so I suggest deleting the second sentence altogether and just making a comment on the size of the current fleet and the fact that it will be 20 to 30 years before the majority are replaced.	Reformulated a bit and added a "rough numbers" attribute. Left most of the text the same, since point is to make clear that the MC and the on-board architecture is not only intended for new builds.
15	AW	Ch 5.1	Editorial	….**potential** improvements…	Could not find, assume fixed
16	AW	Ch 5.1 para 1 last sentence	…	….and in practical terms the NC must apply to the existing fleet and future builds in order to fulfil its potential.	Used suggestion and simplified formulation.
17	AW	Para 2	…	On board [not on ship]	Fixed
18	AW		…	Suggest delete text: ….and which it is considered to deserve.	Deleted.
19	AW	Ch 5.2.1	…	….2000, two research projects in particular focused on on-board infrastructure….	Used suggestion.
20	AW	After Fig. 2, 3rd	…	While the two concepts….	Fixed

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
		sentence			
21	AW	Last para	…	…adopts the (…) five-layer AD, including the definition of 'layer'	Fixed
22	AW	5.2.2.1 First sentence	…	Comment: Actually owners do have a choice of equipment (manufacturer, model, spec, etc) so the text is a bit odd, particularly the Conversely bit so I suggest delete the first 1.5 sentences and start the rest with: The SOLAS Convention establishes the minimum set of…….	Used suggestion.
23	AW	Para 4, 2nd sentence	…	…are almost universally used.	Used suggestion
24	AW	3rd sentence	…	…to be discussed below, they do not allow extraneous communications.	Used suggestion
25	AW	Ch 5.2.2.2 para 1	…	…publish… [not publishes]	Fixed
26	AW	Para 2	…	…ballast **water** system….	Fixed
27	AW	Para 3	…	…tend… [not tends]	Fixed
28	AW		…	The first sentence is very long and complicated and might be better edited or split into shorter sentences.	Edited and split…
29	AW	Ch 5.2.3 para 2 2nd sentence	…	The consequence of not meeting and remaining in compliance with the rules….	Used suggestion.
30	AW	Ch 5.2.3 para 3	…	..components… (s added) …compromise…(s deleted)	Fixed
31	AW		Structure	There are no references in the text to figures 4 or 5	Fixed
32	AW	Para 4	Editorial	…also seem **to** involve…	Fixed
33	AW	Ch 5.3	…	…..argument that it is necessary for the MC and MCC to be fitted not only on new ships but also the existing fleet…	Used suggestion.
34	AW			…architecture must be such that the MCC: .1 supports… .2 does not compromise…	Kept existing formulation.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				.3 ensures that… .4 is in compliance…	
35	AW	Ch 5.4	General	The list of items is in a different font to the rest of the text and this is the same in other lists – the font might be the same throughout the text	Fixed fonts
36	AW	Ch 5.4 near end	Editorial	..nevertheless **have** to be known, ….	fixed
37	AW	Para 1	…	The MCC….. [no need to spell out as abbreviation used many times before in text]	fixed
38	AW	Para 3	…	…VSAT, T2.1 VDES are clearly also AE.	fixed
39	AW	Para 4	…	…..may not need to be separate items…	fixed
40	AW	Ch 6	General	Although Viewpoints is a part of the ISO/IEC 42010 standard this chapter and its concepts do not seem to add much (for me at least). Font in list is as in previous general comment	Kept chapter. Important for further work. Font fixed.
41	AW		Editorial	Experience… [no s]…for consideration…	Fixed, used
42	AW	Ch 6.1	…	…and **their** environment	fixed
43	AW	2nd sentence	...	….context viewpoint is considered to be fully relevant since the….	Used suggestion
44	AW	Ch 6.3	…	…informational…[**al** added]	fixed
45	AW	Ch 7 1st sentence	…	…requirements …[**s** added]	fixed
46	AW	2nd sentence	…	….communication solutions and enhanced ability to integrate…	Used suggestion
47	AW			…via operation and monitoring to reporting….	Used
48	AW	Para 2	…	….strategy has been developed by IMO…	Used
49	AW	Para 2 2nd sentence	Editorial	….maritime communication needs, a set of…	Fixed
50	AW	Para 2 3rd sentence	…	…other projects and research including: [list..] have further refined…	Fixed

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
51	AW	Para 3	…	….in previous chapters [**s** added]	Reference to the specific chapter added
52	AW			At the time of writing [enter a date] the numbering of MSPs is confusing….	fixed
53	AW	Figure 8	…	This table is basically ordered according to Task number so on that basis Task 5.1 should be moved accordingly	Table is ordered from an original list of use cases. Kept it that way.
54	AW	Last sentence	…	….to be made to make a better estimate than is possible at the time of writing [enter a date]	Fixed
55	AW	Ch 7.1	…	Font in list as before…	fixed
56	AW		…	There are three interaction/comms types [delete types of]	fixed
57	AW	Ch 7.1.1	…	….destination end point is known and the source of communication is sure that…….providing acknowledgement of reception.	fixed
58	AW	Ch 7.1.2	…	Defined as a one-to-many communication…..and the source of communication is sure that acknowledgement…	fixed
59	AW	Ch 7.1.3	…	…is also a one-to-many communication but where the destination end point….., no acknowledgement is given therefore there is no guaranteed that the information is transferred.	reformulated
60	AW	Ch 7.2	…	Font in list as before….	fixed
61	AW		…	…..the level of….	fixed
62	AW	Figure 10	Error???	Aren't MSI and NM generally broadcast rather than P2P?	Good question. We discussed this and came to the conclusion that the service would be implemented as a "client request available MSI and NM's and server will send to client". Hence P2P. This might change with completion of the service description. For now, no change made.
63	AW	Figures 8,10 & 11	Editorial	The word **chart** has been misspelt as cart in the tables	Fixed

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
64	AW	Ch 7.3	…	Font in list as before…	Fixed
65	AW		…	….estimation of the…[not guesstimate]	Changed. However, we really guessed more than estimated…
66	AW	Ch 7.4, 7.5, 7.6	…	Font in list….	Fixed
67	AW	Ch 7.6 para 3	…	…..it is assumed that all of the services are built on top of….	Used suggestion
68	AW	Ch 7.6 para 4	Editorial	Figure 14 shows how the various services in the MSP are anticipated to make use of the basic….	fixed
69	AW	Ch 7.6.1	…	A web service is the standard defined by the W3C….	Reformulated.
70	AW	Ch 7.6.2	…	Both source and destination end points that support [s deleted] the….	fixed
71	AW	Final para second sentence	…	The value-added that these…	fixed
72	AW	Final para last sentence	…	Similar methods should be considered with respect to the MC data service, especially if it is to work across VDES	Used suggestion
73	AW	Ch 7.6.3	…	…acknowledgement…	fixed
74	AW		…	The new element here is that it is the broadcast of data information via available data exchange communications channels	Used suggestion
75	AW		…	…..they will have to 'subscribe'….	fixed
76	AW		…	With respect to architectural design of a Broadcast Message Service, the broadcast services that have been developed for the W3C, particularly the RSS (Web feeds) are a possible example to follow.	Reformulated.
77	AW	2nd para	…	….also be a solution here.	fixed
78	AW	Ch 7.7	…	…**have** provided several additions….	fixed

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
79	AW		…	In general, the XML schemas are the dominant web service data formats although formats such as JSON and BISON are becoming increasingly used on the basis of claimed enhanced efficiency.	Used suggestion.
80	AW	Ch 7.8	…	…set out in chapter 6	Fixed
81	AW		…	Font in list as before	fixed
82	AW		…	….as given in chapter 10.	fixed
83	AW	Ch 8	…	…..set up in such a way that the communication framework is developed in WP3 and the on-board architecture… [delete: of..]	reformulated
84	AW		…	Since WP3…[delete: in the work]	fixed
85	AW		…	…..will also provide requirements forming the basis…	reformulated
86	AW	Ch 9	…	Font in list…s	fixed
87	AW	C 9.1 1st para	Editorial	…..standardization of the on-board data infrastructure is…	fixed
88	AW		…	….series of standards that cover serial and network-based…	fixed
89	AW		…	Delete the '' at the end	fixed
90	AW	Ch 9.2	…	….mean**s**	Fixed
91	AW		…	Font in list…	fixed
92	AW	Para 2	…	Delete it's and replace with **its**	Fixed
93	AW	Functional sub heading	…	…requirement for [not of] standardization	fixed
94	AW	Ch 9.3	Error???	Should reference also be made to ETSI Cyber Security Technical Committee and the IEC 62443 series	Reference and description made
95	AW	Figure 15	Editorial	No reference in the text to this figure	fixed
96	AW		…	ENISA and ABS might be better in ( ) and the full name in text – and the	Fixed

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				same format used throughout (i.e. acronym in ( ) to follow full text)	
97	AW	Ch 9.1 and 9.2	Structure	These two chapters are very brief compared to 9.3 on cyber security – I appreciate that cyber security is a hot issue but should more elaboration be given (if possible) to integration and open, harmonized architecture???	Input from review meeting 2016-04-21: The level of information in 9.1 and 9.2 is accepted at this point in time
98	AW	Ch 9.3 2nd para	Editorial	…type**s..**	Could not find – hence assume fixed
99	AW		…	…action that can be taken.	fixed
100	AW	Last para	…	…**has** emerged..	fixed
101	AW	General	…	As a general comment…the various lists in the report are in various formats: bullet points, numbering, use of a), b) etc… they might be standardized.	Fixed … only one required numbering.
102	AW	Ch 9.3.1	…	Font in list…	fixed
103	AW	Ch 9.3.3	…	Risk identification is the process of determining risks that could potentially impact system operations and data and the possible outcomes.	Reformulated.
104	AW	Ch 9.3.4	…	Such equipment **is** very rare today…	fixed
105	AW	2)	…	….it may be preferable to allow the connection of some…	fixed
106	AW	Penultimate para	…	…the 460 gateway is..	fixed
107	AW		Editorial	… responsibility for [not **of]**	Fixed
108	AW		…	… recommendations for [not **of**]	fixed
109	AW	Ch 9.3.5	…	…to enable [delete for] functions that	fixed
110	AW	Ch 9.3.6	…	Given the perspective requirement (para 9.2 above) for an open…… and the user needs identified in (E2-T3.1…etc) and the available standards for mitigating security risks (IEC…), any candidate architecture needs to be validated…… of the risks. This might be achieved by: .1 placing…	Reformulated and used part of suggestion.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				.2 describing… .3 describing… Making full use of the NIST approach (para 9.3.2) [and delete the list as it duplicates 9.2.3]	
111	AW	Ch 10.1	…	Some explanation of ID, SD, SR and MS in the table in Appendix required (email exchange of 7 April refers)	Added into description in Appendix.
112	AW		General	Is the list here a summary? If so it might say so…	Added description for list
113	AW		Editorial	Font in list…	fixed
114	AW	Ch 10.2	…	…. analyses a typical network structure….and proposes…. required classes of services	fixed
115	AW		…	Font in list…	fixed
116	AW		…	In (SINTEF)… each domain**'s** internal….there are interconnection**s**….	fixed
117	AW	Ch 10.2.1	…	….**is** vital…traffic **is**…administrative or passenger traffic and to reduce…. VLAN **is**…	
118	AW	Ch 10.2.2	…	….7.4 priority provide an indication of..	fixed
119	AW		…	Which at the top of page 43 ..not witch!	fixed
120	AW		…	The text starting One could also imagine…could say: It might also be anticipated that the MC/MCC could centralize functionality that could ease implementation in many of the MSP applications in the M2M mode.	Used suggestion
121	AW	Ch 10.2.3.1	…	…suppliers of the system**s**….implement interface**s**…	fixed
122	AW	Ch 10.2.4	…	Examples can be envisaged of multiple operations	Not changed, suggestion would change meaning.
123	AW		…	In this case the same principle…. In cases…..	fixed
124	AW	Ch 10.3.2	…	Delete: …one would very quickly…	reformulated
125	AW	Ch 11	…	…up until the date of this report [date to add]	Date on front page.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
126	AW	Ch 11	Editorial	Figures should be 21 and 22	fixed
127	AW	Ch 11.3	…	….illustrates the relation….	fixed
128	AW	Ch 12	…	It is suggested that…	Changed.
129	AW	Ch 14	…	WP3. [full stop to add]	fixed
130	AW		…	….is, therefore, likely….	fixed
131	AW				
132	PAN	Page 10	edit	While to two concepts are quite similar in many respects Change to to the	fixed
133	PAN	Figure 6	structural	With reference to the listing on the previous page I miss an indication of the intelligent roaming device described in T2.3. the parts I miss are shown in figure 19 Either add some text explaining the implementation of intelligent roaming, or adopt it into the drawing.	List show the roaming device and figure 6 does show the roaming device.
134	PAN	7-1-1 and 7.1.2	edit	And the source of communication are sure that And the source of communication is sure that	fixed
135	PAN	10.2.3	structural	Description of the communication network based on IEC 62940 Consider adding a description in this chapter	Rejected. The 62940 network is not seen as a ship operation network. Traditionally the communication components are considered part of the navigation and hence one could say that ICS is part of the Navigation network. Later in doc, however – it is shown how the ICS is binding it all together.
136	PAN	Figure 20	structural	Figure 20 is in contradiction to figure 19 in relation to placing the VDES. In figure 19 VDES is a non LAN item, in figure 20 it is a LAN item	I think you hit the spot of the main problem in our work. As it looks, VDES is offering both AIS/ASM as non lan and data

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
					exchange via the IP network. By nature, VDES is an interface between VHF (non-lan) and the on-board networks. As noted later, it is suggested to move away from the non-lan area and move the communication to an IP based. In the proposed architecture, it is assumed that VDES is providing nothing but IP connectivity. A note of that has been added to chapter 11.2.
137	PAN	11.3	edit	The latter "yellow" integration needs to be amended with a note I think the sentence should be, the latter "red" integration needs….	Reformulated.
138	PAN	Figure 24	edit	It is not possible to follow the yellow line all the way on the figure Update the figure to make both yellow and red lines fully visible.	Fixed
139	JKJ	P12,40	formulation	Unclear. I don't see how this is discussed in the section below.	Reformulated, refer to cyber security
140	JKJ	P13,5	formulation	Replace GPS-type with GNSS	fixed
141	JKJ	P13, 5.2.2.2	formulation	Should BAM not be mentioned in this context?	BAM is part of CAM and part of IMO type approval regime
142	JKJ	P14,13	editorial	Passengers are relevant for Safety of Life At Sea as well…	fixed
143	JKJ	P14,20	formulation	'Never' is a strong word… We frequently need to send test standards into a maintenance cycle, to take into account creative solution which no one had imagined.	Deleted last sentence.
144	JKJ	P14,37	editorial	Propose to delete "entities and"	fixed
145	JKJ	Fig. 4	structural	I miss the administration (office) network – which is mentioned in the text	The figure show clusters of type approved equipment.. .that is not in

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
					the office network.
146	JKJ	P15,7	editorial	Add 'to'	fixed
147	JKJ	P15,8	structural	Don't understand "between entities between layers"…	Reformulated
148	JKJ	Figure 5	structural	Miss the admin network. Administrative reporting formalities and associated communication needs play a significant role	The figure show clusters of type approved equipment.. .that is not in the office/admin network.
149	JKJ	P16	formulation	I'm not sure what is meant here. Is it administrative systems? Many of the services (MSP's) discussed in e-Navigation are related to the NAVIGATION system?	No .. it is not administrative systems. It is the process of identifying architectural elements that must present in the proposed architecture. Why e-navigation services are included separately is because it is new.
150	JKJ	Figure 6		What is meant by the separate network for e-Navigation? Where is the administrative network?	Separate network for e-navigation is because it is new. Are reverting to definition and use of administrative network later in report.
151	JKJ	Figure 10		*Why are several Use Cases duplicated – Port Reporting for instance? What is the difference between MSI&NM and the version with (hydro data)? RE MSI&NM, I think the P2P interaction would be an exception, while the Multi- or broadcast are the typical – and I see no need for Confidentiality/encryption for this use case. These informations are typically publicly available . RE the broadcast of ROUTE PLAN / active route – I think it should read 'route segment'. It is unlikely that the entire route plan will be broadcast.	All very good and relevant comments. Will not change for this report since changes will not influence proposed architecture. The list/overview of MSP and service communication requirements needs to undergo much more work during E2.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				RE ROUTE EXCHANGE I think the 'broadcast' is covered by the Route plan segment broadcast. The EXCHANGE of route will typically be a P2P or multicast operation which would require authentication and encryption. RE ICE CHARTS – I don't understand why a broadcast interaction without requiring client authentication is not mentioned. ICE charts are likely to be public information just like weather forecasts. RE Emission monitoring I think the typical communication interaction will be P2P requiring encryption and client authentication	
152	JKJ	Figure 11		MSI&NM: I would expect Priority to be 'SAFETY (URGENT on event) SeaCHARTS: The indicated information sizes must be updates or overlays only. Base chart ENC data magnitudes are larger in my experience. SMART BOUY MANAGEMENT SERVICE: I would consider Priority to be ROUTINE (SAFETY on event) ICE CHART service: I would expect Priority to be 'SAFETY' EMISSION MONITORING: I would expect latency to be 'Days' and priority to be 'ROUTINE'. (No idea of the magnitude or frequency).	All very good and relevant comments. Will not change for this report since changes will not influence proposed architecture. The list/overview of MSP and service communication requirements needs to undergo much more work during E2.
153	JKJ	Figure 12		I would consider it unlikely to fit much SeaChart data into AIS/ASM – and I would disapprove of utilization of AIS/ASM for a commercial sea chart service. That would overload the AIS with data transfers irrelevant to the function of AIS. Re Snart bouy Management Service I see no reason why Wi-fi, WiMax, Cellular or even commercial satellite services are not candidate carriers. Many AtoN are today equipped with 3G or similar for remove management.	All very good and relevant comments. Will not change for this report since changes will not influence proposed architecture. The list/overview of MSP and service communication requirements needs to undergo much more work during E2.
154	JKJ	Page 28,		VDES, NAVDAT, NBDP…?	VDES not a service.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
		27			NAVDAT and NBDP stay as they are … They are to be replaced by new services in the MSP.
155	JKJ	Page 28, 13		I think Web services can and will play a significant role – much more than figure 13/14 seem to indicate, for several reasons: Introducing a MCC with MMS capabilities, almanac, etc. will be a long haul. In the mean time, a lot of web services may be exposed more easily, although not benefitting from the ease of authentication and other capabilities provided by the MCC. I think the 'web' is a candidate for most use cases.	Don't understand. Does this not undermine the whole work and idea behind MC ? No change made .. to be discussed at next E2 conf.
156	JKJ	9.1 2nd para		Delete "	fixed
157	JKJ	Figure 15		Identical to figure 18. Is it needed twice?	It is included twice for readability.
158	JKJ	Page 36,5		Also?	Deleted.
159	JKJ	P38,36		Is it the primary role? I thought the role of the 460-gateway was segregation of controlled networks from uncontrolled. The Gateway may contain a DMZ area, and functionality in that zone *could* be related to storage of data made accessible by several networks?	Deleted paragraph.
160	JKJ	P39,7		A foreseeable emergency response procedure might include temporary isolation of safety critical networks – i.e. consider the effects of disabling or manually disconnecting gateways to controlled networks, to prevent an observed anomaly from affecting safety critical functions.	Reformulated, however I think the short term response: isolation is part of gateway re-configuration.
161	JKJ	Figure 17		Identical to figure 3. Propose to delete here and refer to figure 3. An alternative would be to extend the figure. In this figure I lack the GMDSS network. Although probably not included due to complete isolation, this could be indicated explicitly by adding the GMDSS network as an isolated network connecting radio comms on the Instrument layer with ICS Workstations on the process layer.	Kept the figure to ease readability.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
162	JKJ	Figure 18		Identical to figure 15. Propose to delete and refer to figure 15 instead.	Figure 18 deleted and reference to figure 15.
163	JKJ	P45,27		reformulate	Fixed.
164	JKJ	P46,22		Interesting discussion. I think this chapter should however touch upon the real time need of the AIS service in order to correlate well with e.g. RADAR, which results in a requirement for Point-2-point communication – IP or other protocol. Routing via different commercial SATCOM without QoS and a well known latency would not be useful.	Uncertainty of VDES role statement has been added to chapter.
165	JKJ	P46,39		Would it necessarily? Just because IP is chosen as a protocol, it doesn't mean you cannot create a maritime radio network which is not connected to the public internet. But agreed – the VDES network must be treated as 'dangerous' because it is an open radio network – a bit like the AIS is a door into the IEC 61162 network, but it only allows certain data structures to pass… VDES could be designed to utilize the IP protocol, but I think VDES should remain a strictly maritime professional radio network. VDES gateways (shore stations) could be allowed to connect to the MMS (Maritime Messaging Service) – which in turn would also be allowed to accept connections via internet, providing the cross network messaging capability, based on priority. VDES stations should however just like the MMS only allow traffic with priority Routine, Safety, Urgency or Distress – NOT General.	Uncertainty of VDES role statement has been added to chapter.
166	JKJ	P49,5		Before and after what?	reformulated
167	JKJ	P49,10		Figure 21	fixed
168	JKJ	11.3		Don't quite understand this – please explain.	Added description of ICS standard work.
169	HP	Figure 3	structural	The figure 3 might be a "copy-paste" from the declared source (Rödseth,	The figure is not supposed to

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				Christensen & Lee), but it gives wrong impression of the reality onboard. For many years there has been online delivery of many of the IMO e-Navigation services. Many of them are off course today by private arrangement, although there was a time when online delivery of ENC charts and updates was available by methods established by EU-project ECHO. I propose that the figure 3 is modified or if that is not acceptable, then a new alternative figure is added. The new key points of the new or additional figure is in "picture 1" (see end of this review comment document). Use case "a)" in the picture 1 has been provided ENC chart and updates for over 5 years by companies such as Furuno, Transas, Navtor, etc. Use case "b)" in the picture 1 has been provided weather, weather routing, Ice-breaker assistance, Route exchange, etc. in addition to ENC chart and updates. This use case has even longer history of use than the use case "a)".	illustrate reality onboard, but merely a view of how we could organize architecture into a layered model. Further into the document, this architecture model is challenged, especially around cyber security. End of report suggest a slightly different topology, much more looking as you have shown on picture 1 and usecase a) Even though usecase b) has a long history and will probably be used quite some time into the future as well, the purpose of this project is to propose architecture for the on-line and connected ship. This means that manual transport of data is not included.
170	HP	Figure 3	structural	The figure 3 should be clearer about what is the scope or focus area of the EfficienSea2. The EfficienSea2 has focus to provide platform to implement infrastructure for IMO e-Navigation. The platform might be used also for other purposes than IMO e-Navigation, but such things should be distinguished clearly from the main focus. IMO e-Navigation include 16 MSPs. MSP8 (Vessel Shore Reporting) is an administrative task to fill and submit IMO FAL-forms. All other IMO MSPs are related to Navigation. The body text and/or Figure 3 should make the focus of the EfficienSea2 clear. See also picture 2 provided in the end of this review document	Figure 3 is not supposed to illustrate scope of E2. It is part of background and discussion, leading to figure 6 which illustrate the scope. The objective of E2 is not only to advice infrastructure for e-navigation. That is only part of the objective.
171	HP	Clause 5.2.2.1 3rd para	structural	The 3rd paragraph talks about navigation and communication equipment living in isolation. I fully agree this for the most of the current existing installation. However the wording gives reader wrong impression about the real	3rd para deleted

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				situation. IMO - as rule setting organization - has been pro-active in specifying integration. IMO published Performance Standard for Integrated Radio Communication System (IRCS) already in 1995 and Performance Standard for Integrated Navigation System (INS) in 1998. However neither of these integrated solution is part of mandatory carriage requirement. We can claim both manufacturers and ship owners being slow to understand benefits and proceeding into this direction. Anyhow IMO still strongly believes in the integration as part of IMO e-Navigation. One part of the SIP (Strategy Implementation Plan) of IMO e-Navigation is to specify additional modules to the IMO INS to provide mandatory integration between communication and navigation. For IMO the whole e-Navigation is a voluntary arrangement available for interested parties to adopt. IMO has clearly stated that there is no plan to make e-Navigation as mandatory carriage requirement. On the other hand IMO has a clear rule that if an IMO Performance Standard exist for a voluntary instrument, then, if installed onboard, such instrument must be type approved. Conclusion is that the INS is seen to be the instrument to implement the navigation side of the IMO e-Navigation. The 3rd paragraph is talking about combination of Radar and ECDIS. It is true that today such devices exist, but their legal use cases are extremely limited and it is already looking like that the class societies will have a very strong opinion about their use. The basic issue is that by reading IMO Performance Standard of the INS, one understand that a combination of Radar and ECDIS functions is actually covered by the INS. Therefore this means that such combined devices should be type approved of being INS. The result of this would be that there can exist "only Radar", "only ECDIS" and INS. About the legal side of use of "non-INS" combined Radar+ECDIS. IMO carriage requirement is clear: 1 or 2 radars depending of the size of the vessel + ECDIS and his backup arrangement. A combined unit without	

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				being an INS does not fulfill the carriage requirement. Therefore they can be legally used only as an additional device in addition to carriage requirement (although recently interpretation of the authorities are getting tougher toward a direction that any combined equipment shall be type approved as INS). The practical reason for still today existing combined units is the fact that manufacturers have had not enough interest to provide real type approved INS for the market. In practice there were no type approved INS available in the market before 2012 and still today very few manufacturer has it available. But as insider I know that all major manufacturers are now in a process to type approve their combined units as a consequence of tightening of the following of the rules by the authorities. Therefore it is already foreseen that within the project time of the EfficienSea2 combined Radar+ECDIS will disappear as being legal for SOLAS vessels.	
172	HP	Clause 5.2.2.2	structural	This clause explain that Classification Societies go beyond IMO rules for their "Alert, Monitoring and Control (ACM)" system. That is true, but it that relevant for the EfficienSea2 project? IMO has published Performance Standard only for Radio Communication and Navigation instruments. Typical for Radio Communication and Navigation instruments is that they are installed in the bridge of the vessel. Obviously vessels have a lot of system installed outside the bridge. Very often these outside the bridge devices are called as "below deck". IMO has not implemented similar type approval regime to below deck than for Bridge. Below deck is mainly controlled and polices by the Classification Societies. The AMC is for below deck purposes. For bridge purpose IMO has published a Performance Standard called Bridge Alert Management (BAM). My opinion is that for the scope of EfficienSea2 the issue is BAM and not AMC. My opinion is that the title of 5.2.2.2 should be "Alert management" and the text within it should explain that for bridge this is specified by IMO BAM for below deck this is specified largely individual Class Society rules Basic idea of BAM is that either all alerts are by individual equipment only	Text updated to clarify difference between IMO type approval and Classification type approval.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				or all alert are centralized - partial implementation is not acceptable. Consequence is that many vessel have IMO BAM which also show alerts from below deck sources IEC has already specified how to implement the Alert communication (IEC 61924-2 INS) Further IEC is working on a new standard for BAM (IEC 62923), which will in addition to standardized serial line (IEC 61162-1) and standardized LAN (IEC 61162-450) explain a converter between historical legacy, proprietary, etc. and the standardized interfaces. The standard is planned for 2018 publishing.	
173	HP	Clause 5.2.3 Figure 4 Figure 5	structural	See pictures 3 and 4 in the end of this review document	Agree to the proposed changes, figures updated.
174	HP	Clause 5.4	editorial	Typo. Change "IEC 62162-460" as "IEC 61162-460"	fixed
175	HP	Clause 5.4 Figure 6	structural	For EfficienSea2 "eNavigation" is IMO e-Navigation. IMO e-Navigation is within IMO type approval. Otherwise e-Navigation solutions cannot legally replace current paper based solution. The figure 6 is not correct for this detail. Another confusion is around Automation System being part of type approval. They are subject to class society approvals, which are not similar to the type approval required for the rest. Last confusing detail is the fact that all communication devices are in the Figure 6 out of type approval domain. That is not true today and will not be true for the future. Satellite terminal being part of GMDSS (today Inmarsat, very soon also Iridium) are part type approved regime - VSAT is not part of type approval regime although it is covered partly (environmental rules, especially EMC rules) by IMO resolution A.694(17). See Picture 5 in the end of this review comment document	E2 is not only eNavigation. eNavigation is not planned to become mandatory. Will it then be within the type approved domain? It should be noted that Class is also using the term Type Approved for equipment that is fulfilling their rules. It will however be useful to highlight that in the text of the report. Text updated to clarify difference between IMO type approval and Classification type approval.
176	HP	Clause	structural	Basic component of cyber security are: authentication, integrity and	Have tried to make it more clear

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
		7.2 Figure 10		confidentiality. Today in the second year of establishing of the IMO Cyber Security Guideline it is unrealistic to assume that any new service could be without basic authentication. Another detail which is totally missing in Figure 10 is "integrity". Obviously Integrity check shall be added to every service. See Picture 6 in the end of this review comment document	that integrity is part of data authentication. We see the two types of authentication .. one is entities (clients/servers/users) … another is authentication of data. The latter is supposed to include integrity. MSP tables reviewed and updated.
177	HP	Clause 7.4 Figure 11	structural	Some priority classification should be changed. Biggest finding is that data volumes for Sea Charts is totally underestimated See Picture 7 in the end of this review comment document	Agree to comments, we need to do more work on the MSP use-cases and the MSP design. Input will be used there. However, at this point in time, it is not seen that changes will have effect on the proposed architecture. MSP tables has been updated with the received input. Disclaimer of numbers in MSP tables added to report.
178	HP	Clause 7.5 Figure 12	structural	Some classification should be changed and a column for Inmarsat C should be added. See Picture 8 in the end of this review comment document	Same action as HP-9
179	HP	Clause 7.6 Figure 13	structural	Several issues Use of MMS for MSI. MMS is not very well defined. Some understand it as a maritime chat. I do not say that use of MMS for MSI is impossible, but the use of MMS for mandatory items for which user has obligation to act shall be arranged to be clearly distinguishable for nice to know, etc. Also one cannot use a common history log with all the other MMS chat to fulfill equipment rule to preserve history log of MSI. This comment is applicable in addition to MSI for all services which have identified legal	Same action as HP-9

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				status and end user obligation to act. Route data. IEC has standardized the Route Exchange format used by the Monalisa-project (available in IEC 61174 Ed4). This format is mandatory to implement for all new ECDIS equipment. It is very difficult to see how other formats or methods could penetrate to the market especially as such formats should go through the type approval process based on international standard. Therefore it is difficult for me to understand how MMS could be used for Route data unless the idea is a "monkey interface" (= a human operator read text of MMS and then enter the coordinates into his ECDIS)	
180	HP	Clause 7.7 1st para	structural	The list of data formats miss ISO 8211, which is used by ENC charts and their updates (both current S-57 ENC charts and future S-101 ENC charts)	Added.
181	HP	Clause 9.3	structural	Basically the existing content is good, but it miss one important element already going on in the international standardization. This element could be added at the end of existing clause 9.3 (Below is proposal for text to be added) IHO has created and maintains the baseline S-100 standard which is selected by IMO to be the baseline for all IMO e-Navigation. Within IHO two workgroups (S100WG and DPSWG) are already drafting cyber security to be included into the S-100 baseline most probably for 2018 publishing. The S-100 metadata will already amended for edition 2.1.0 publishing to include placeholders for digital signatures. Basic concept of cyber security can be summarized Authentication: Will use PKI, digital signature(s) are embedded in header section of dataset(s). Receiver check digital signature against delivered Public Key Integrity: Will share PKI and digital signature used for authentication. The method is such that he digital signature is calculated over the data. Result is both authentication of the source and integrity check of the data. Confidentiality: This is the encryption. S-100 will not require mandatory encryption (note depending of service the data is either confidential or	Have added the first suggested paragraph. The chapter purpose is here to mention ongoing work, but not in detail.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				intended for public availability). S-100 will include multiple encryption methods and it is a task of the S-100 based Product Specification (for example S-101 for ENC chart, S-102 for Bathymetric charts, etc.) to specify if encryption is used and, if used, which method of the available is in use (Note: similar arrangement as for encoding: for example S-101 use ISO 8211, S-102 use HDF-5, etc.) Distribution of keys. IHO has already in use a PKI method based on pre-distributed Public keys. This is different arrangement than the certificate method used by HTTPS (HTTPS use chain of trust in which linked certificates are checked until a Certificate Authority (CA) is found in the end of chain). The pre-distributed public key method is not vulnerable to long latency times and dropouts (see 7.6.2 and SATCOM providers offering file transfer to overcome problems with latency and drop-outs) and under IHO S-63 it has a successful service history close to 20 years in maritime domain.	
182	HP	Clause 9.3.4	structure	The 2 first paragraphs are about "Mission critical equipment" in which it is written that there are 2 subcategories: a) very rare 61162-460 compliant equipment and b) uncontrolled legacy. I strongly disagree so black and white view. First issue to note is that IEC 61162-460 is just recently published (Aug 2015) and therefore manufacturers have not had enough time to make products available in the market. Further I know that first equipment has passed type approval test in Apr 2016. Second issue is that one can build -460 compliant network by just utilizing 460-Switch(es) and 460-Gateway(s), if the connected navigation or communication devices do not include open UBS-ports, open SD-memory card slots, etc. for which user could insert an uncontrolled memory/device/etc.. Based on what I said above it is already possible to build a type approved -460 based system.	Reformulated to illustrate that there is a range from legacy not conforming at all, to full conforming.
183	HP	Clause 9.3.4	Structure	Within 9.3.4 there is "sub-section" "2) uncontrolled equipment" Basically I agree. Maritime Cloud itself will be seen as an "uncontrolled	Will use this input when we get to service design later in E2.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				network". Nice to know features like the 3 bullet points could stay forever within the "uncontrolled part". Further I agree with the idea that the Maritime Cloud is connected to a controlled Navigation network through 460-Gateway. My first comment start from "How to use the files inside 460-network" Simplest method to make files available inside the 460-Network is to make the DMZ of the 460-Gateway visible as mapped network drive (for example M:). This is very handy as in practice every ECDIS include a method to load ENC charts and updates. Loading from internal DVD (for example drive D:), internal USB-port (for example E:) is not different from loading a mapped network drive in DMZ. This method is also field proven by many companies although their "service boxes", "gateways", "what do you call it", etc. have not yet been type approved as -460 (this because -460 is a new standard from Aug 2015 and the services has operational histories up to 5-10 years already). This mapped network drive makes also unnecessary to specify/recommend port number, etc. at the 460-Network side. The current wording propose 1) manual or 2) automatic transfer of data between Maritime Cloud and DMZ. Off course at this level I agree that both are possible. For automatic transfer there exists however two principally different solutions. Automatic transfer could be initiated by the Cloud (push-method) or by the 460-Gateway (pull method). Both methods have their pros and cons. In case of the pull method the 460-gateway include an automatic loading robot who is able to use the discovery methods of the Cloud to find ports, URL addresses, etc. of the available service(s) which the user have requested. The big cyber security pro for pull method is that the 460-Gateway can be made stealth (i.e. it do not answer to any external request from the uncontrolled network / Internet side). In the push method the Cloud need to know port number, address etc. of every 460-Gateway for which he need to push data. The big cyber security con is that through this path also the cyber attacker can penetrate inside the secure 460-Network side.	
184	ESP	Figure 20	Editorial	no connection between automation and navigation and no connection to navigation	Changed

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Re-viewer Initials	Reference in doc. (General or Paragraph, Figure …)	Type (editorial, structural, formulation error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
185	ESP	Figure 21	Editorial	no connection between automation and navigation	Changed
186	ESP	Figure 22	Structural	"-450 secure network" to be changed to "Secure Network"	Changed
187	ESP	Figure 22,23 and 24	Structural	Novel E-navigation to be separate entity outside navigation, and with own -460 gateway	Changed
188	ESP	Chapter 11	General	MCC to exist as multiple instances on-board … i.e. one in each -460 gateway	Notes on this discussion has been added to report. This topic to be discussed in the further work on MSP design.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".