HOSTED BY
ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

International Journal of e-Navigation and Maritime Economy 5 (2016) 001 – 020

International Journal of e-Navigation and Maritime Economy

www.elsevier.com/locate/enavi

Original article

Requirements for e-Navigation Architectures*

Axel HAHN [1], Andre BOLLES [2], Martin FRÄNZLE [1], Sibylle FRÖSCHLE [2], Jin Hyoung PARK [3†]

[1] Dept. of Computer Science, University of Oldenburg, Germany, Corresponding Author, hahn@wi-ol.de

[2] Transportation Research Division, OFFIS, Germany, andre.bolles@offis.de, sibylle.froeschle@offis.de

[3†] KRISO, Korea, jin.h.park@kriso.re.kr

Abstract

Technology is changing the way of navigation. New technologies for communication and navigation can be found on virtually every vessel. System architectures define structure and cooperation of components and subsystems. IMO, IALA, costal authorities, technology provider and many more actually propose new architectures for e-Navigation. This paper looks at other transportation domains and technical as normative requirements for e-Navigation architectures. With the aim of identifying possible synergies in the research, development, certification and standardization, this paper sets out to compare requirements and approaches of these two domains with respect to safety and security aspects. Since from an autonomy perspective, the automotive domain has started earlier and therefore has achieved a higher degree of technical progress, we will start with an overview of the developments in this domain. After that, the paper discusses the requirements on automation and assistance systems in the maritime domain and gives an overview of the developments into this direction within the maritime domain. This then allows us to compare developments in both domains and to derive recommendations for further developments in the maritime domain at the end of this paper.

Keywords: e-Navigation, IT-Architectures, Safety, Security, Requirements

* This is a revised version presented at the 3rd Ai-MAST held at Daejeon, Korea, November 12-14, 2015

I. Introduction

Information and communication technology is dramatically changing the way we live, work and travel. The impact on transportation systems is correspondingly high. New assistance systems and high automation technologies require novel approaches to system architectures, design processes, tests and certification. To take advantage of developments in other domains, this paper compares developments and concepts of the maritime and the automotive domain.

Until now the captain on a vessel and the driver of a car are controlling their vehicle by using their own environment perception with the help of additional sensor technologies such as radar. External control is based on optical signals (traffic lights, traffic signs) or voice communication (VHF radio and traffic message channel). However, with the advent of improved communication technologies and higher computational power this situation changes dramatically in both domains.

Similar technologies are under development in the maritime as well as in the automotive domain: assistance systems for heading control, distance warning, traffic management, road side / shore side infrastructure or even studies for autonomous vehicles are investigated or even already under development. Cooperative driving / navigation technologies are of high interest. Car-2-X communication is intensively investigated in the automotive domain, while in the maritime ship-to-shore or ship-to-ship communication is in the focus.

However, there are also differences between the different modes of transportation. In the maritime domain, a vessel is handled by professionals forming a bridge team backed by extensive education and training. On the road, only commercial transportation is handled by professionals, whereas people with vastly varying capabilities (novice drivers, elderly persons) drive private cars, motorcycles etc. Additionally, the system dynamics are fundamentally different. Time horizons relevant to situation awareness, prediction, and planning in automotive are significantly shorter than the horizons in the maritime domain. On the other hand masses, inertia, momentum and kinetic energy, and thus also dead times in control, are much higher in the maritime domain.

In the maritime domain, new e-Navigation and even traffic management systems are under development for ship-side and on-shore usage. This covers ship-side technologies like Integrated Navigation Systems (INS) integrating electronic charts, navigation and conning data or integrated surveillance systems on shore with technologies like Automatic Identification Systems (AIS), Global Maritime Distress and Safety System (GMDSS), Resilient Position, Navigation and Timing (PNT) etc.

II. Developments in the automotive domain

Supporting the driver with assistance functions has been a research topic for decades in the automotive domain. A model to cover the socio-technical aspects of this driver vehicle system has been developed already since 1982 and is described in the following section. After that we give an overview of technical and standardizing aspects in the automotive domain.

2.1. Human centred design of assistance systems

The so-called three layer approach for vehicle control to model driver tasks that was developed in 1982 by Donges (Donges 1982). This model is still the actual basis not only for human-in-the-loop technologies, but also serves as a template for automated driving functions in highly automated or even autonomous driving systems. Figure 1, which is taken from (Donges 2012) yet modified by adding "system" on the left, shows these three layers with the tasks to be solved on each layer and the corresponding environmental context.

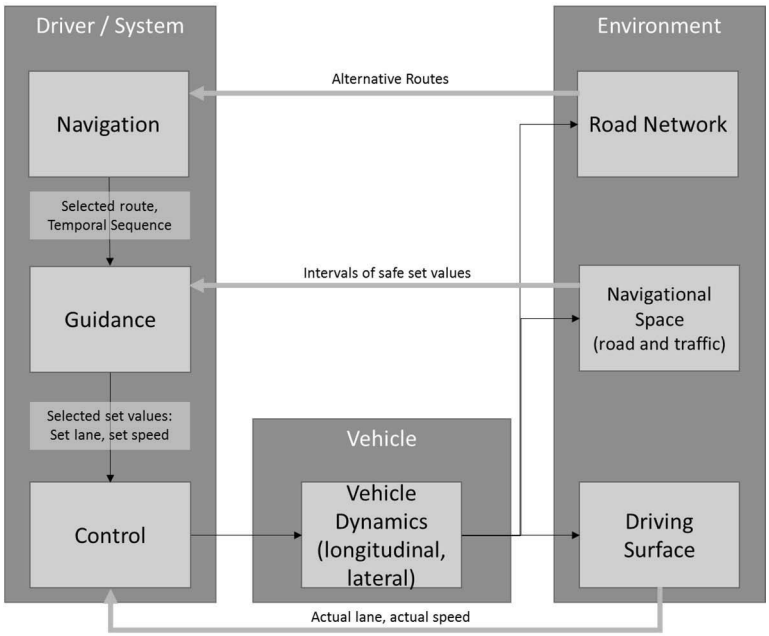

Figure 1: Three-layered approach for driving

This model states that there is a strategic component for navigation, which has its focus on finding a good or better, even the best, route. The next level then is to give input to the vehicle according to the current traffic situation (e. g. reducing speed to avoid a rear end collision). The lowest level is the control level, which needs to directly react on deviations from the expected state. E. g. if the given pressure on the brakes does not lead to sufficient speed reduction, more pressure will be exerted to the brakes. This model has been developed with focus on the mental states and processes of the human driver while steering the vehicle. But this model obviously also holds for technical systems supporting humans in their task to steer a vehicle, since these systems must operate according to the expectations of the human driver, the passengers in the vehicle as well as to the expectations of other traffic participants. This split of objectives is also used for autonomous driving systems like driverless transportation systems in intralogistics.

Having this in mind, the model above is also a good tool for deriving requirements on assistances systems supporting human drivers on the several levels or even for autonomous systems. The most important category of requirements is about timing. While on the navigational level, only informative data is expected and no real-time requirements have to be fulfilled, on the guidance level and on the control level hard real-time constraints have to be satisfied to keep the vehicle in a

safe state. Furthermore, the level of required dependability increases from the navigational level to the control level. While the failure of a navigation system usually does not cause an accident directly, the failure of a control system in a vehicle may have fatal impacts. Therefore, the development of systems for vehicle guidance and control has to consider dependability aspects and hard real-time requirements before deployment in series vehicles. Guidance and control systems must guarantee a reaction to input values in a pre-defined time interval. The accuracy of the reaction must be guaranteed to be in a certain interval. Furthermore, the system must have very high reliability and for acceptance should have high availability. When a failure of the system occurs, it must be guaranteed that the system will automatically transfer into a safe state (e. g. steering the vehicle to the side lane on a highway) or that the human driver will be able to take over the control of the system within a sufficient time frame and with sufficient situation awareness.

2.2. Cooperation and Corresponding Architectures

Providing assistance to a driver is not only an in-vehicle task. As in many real-life situations, teamwork mostly is superior to lone fighting. Thus, in the last decades the cooperation aspect became more and more important to the automotive domain. With the advent of broadband communication and dependable communication networks like IEEE 802.11p based systems, the idea of car to car or car to infrastructure communication gained high interest in the automotive industry. It is expected that car-to-X communication based assistance systems cannot only increase comfort while driving, but also save thousands of lives due to avoidance of accidents. For this, a dependable real-time capable communication between vehicles and to the infrastructure must be available. A number of more or less similar architectures for cooperative driving have been developed. One example for this is shown in the following figure (Stübing 2013):

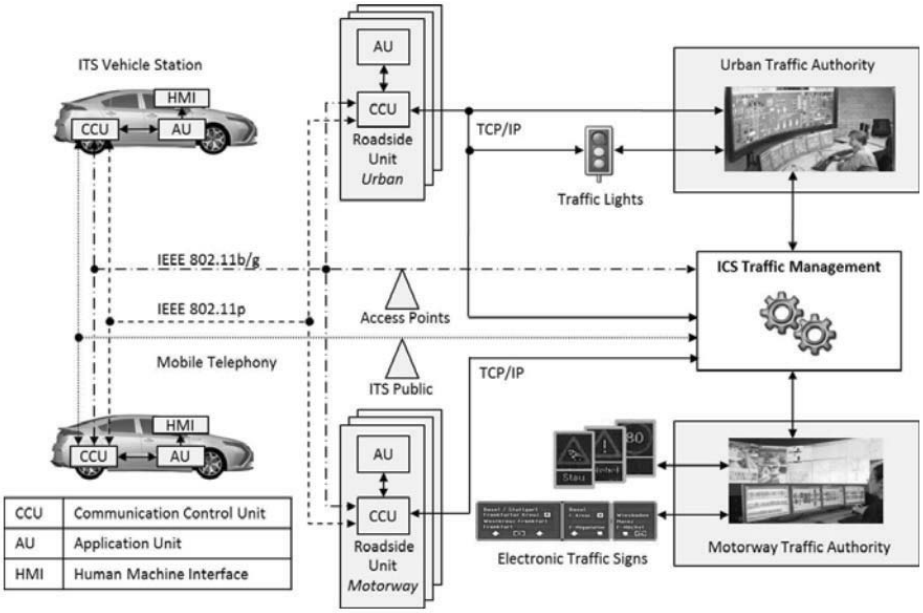

Figure 2: Architecture for car-to-x communication

The original e-navigation strategy has been developed based on user-driven rather than technology driven methodology. Therefore the basic idea of e-navigation solutions might be to avoid system failures, e.g., causing delays because the ship is deemed unseaworthy, avoid loss of basic good seamanship by crews, avoidance of inappropriate substitution of the human element by technology and degradation of bridge resource management. In contrary e-Navigation encourages best practices by crews (MSC 85/26 Add.1. Annex 20). Based on extensive user needs and gap analyses, e-Navigation solutions[1] were identified in order to meet user needs, which mainly reflect concerns experienced most often during daily routine work as the problems that may cause accidents. This architecture covers the vehicle technology on the left, the interface to the infrastructure in the middle and the road-side technology on the right-hand side of this figure. Furthermore, it is foreseen to have direct communication between vehicles as well as between road-side authorities (e. g. responsible for urban traffic and for motorway traffic). The IEEE 802.11p standard is a promising candidate for providing a dependable communication link between the several nodes of this distributed cooperative traffic system. Furthermore, it can be seen that the human machine interaction explicitly is part of this architecture, because the HMI in the vehicle as well as the HMIs in the traffic management centers are explicitly mentioned in this architecture.

2.3. Safety and Security

It is obvious that the development of assistance functions, car-to-X communication applications and eventually autonomous vehicles, have a strong impact on safety and security. This especially holds, the lower the level of control with respect to Figure 1 implemented using these functions are. In the automotive industry, the development of safety critical systems often refers to the ISO 26262 standard, which mainly describes the requirements on the development processes for such systems. For assistance systems, the focus on technical reliability and safety despite technical faults taken by the ISO 26262 is generally complemented by extensive test driving as a means of function validation. While the latter proves to be sufficient for current, sporadically active assistance functions, like the anti-locking brake or the electronic stability program, and for low automation keeping the driver in the loop and fully liable, like adaptive cruise control which leaves lateral control to the driver and thus forces him to actively supervise longitudinal control also, there is widespread agreement that this is insufficient and impractical for higher levels of automation. Given the very low rates of accidents achieved in human-controlled car traffic, which amount to one injury every 2,4 Mio. km on average in Germany (Anon 2015), proving by test driving with sufficient confidence that autonomous systems achieve at least the same safety levels would require hundreds of millions of test kilometers. As this clearly is infeasible, given the budgetary and temporal constraints of automotive system engineering, industry jointly with academia currently is actively looking for more advanced methods for quantitatively assessing functional safety of automated driving functions. It seems that the mind-set of the ISO 26262 with its systematic approach to risk identification and qualification, as well as for consideration of technical safety measures aiming at risk mitigation, will form the basis of such an approach. The most prominent aspect of the ISO

1 see Tables 1 to 5, Annex 7 of NCSR 1/28 for detailed description for solution and its sub-solutions.

standard in this respect is the so-called Automotive Safety Integrity Level (ASIL). This is a concept for mapping a safety critical function into a certain ASIL category (ASIL A-D) quantifying its effective risk as a function of the exposure to the risky situation, the controllability of the risky situation, and the severity of its consequence should controlled risk mitigation fail. As this provides a semi-quantitative classification of risk, based on the ASIL, specific methods, processes and tools for the development, test and certification of an assistance system have to be used, whereby the addition of safety measures is systematically accounted for based on their risk coverage. Problems with directly lifting these approaches to highly automated or even autonomous driving functions do, however, arise due to the following primary reasons:

1. The idea of primary faults occurring stochastically independently according to a certain rate, as formalized by the concept of exposure, becomes shaky, as primary faults tend to be correlated and thus dependent (e.g., blinding by the sun for the computer vision systems in a fleet of cars) and rates vary wildly with environmental conditions (e.g., the likelihood of overlooking other traffic participants in fog vs. good visibility).
2. Mathematical models for the genesis and propagation of errors are missing for certain types of primary faults crucial to driving functionality, like overlooking or misclassifying other traffic participants in computer vision applications.
3. Reactive control observing the behavior of other traffic participants and drawing strategic decisions as well as effecting feedback control based on this establishes numerous covert channels and induces emergent behavior potentially impeding safety measures
4. The safety impact of redundancy is potentially significantly reduced, and in any case much more intricate to analyze, due to the numerous stochastic and functional dependencies in the system and even its environment.
5. Information coming from outside the vehicle and its controllable information infrastructure will increasingly be used for safety-critical functions of the vehicle, using input data stemming from external data sources, like real-time traffic information systems, for which stringent quality assessment is impossible.

Concerning the security aspect of communication leads to two categories of threats. One category of threats is that an attacker can target the communication itself. The two main threats of this type are message injection and denial-of-service of the communication medium by jamming. Take a collision avoidance application as an example. An attacker could inject forged collision warnings, and thereby induce braking maneuvers in an unsuitable situational context. Alternatively, an attacker could deliberately provoke a collision situation and prevent assistance systems to step in by jamming the communication channel at the same time. The second category of threats is that an attacker can target the computing platform of the vehicle itself: every communication interface provides an attack vector via which an attacker can try to infiltrate the vehicle with malware, and ultimately take over the control over safety-critical functions of the vehicle.

During the last few years a number of news reports were published describing such hacking attacks on vehicles via existing communication interfaces such as cellular and Bluetooth.

Car-2-x communication based on IEEE 802.11p has been prepared over the last decade and security has been one focus from the start. Both categories of threats as well as privacy concerns have been taken into account: based on research projects such as Evita, Sevecom, and Preserve. The current Car-2-x standards by ETSI advocate a sophisticated security architecture, which includes digitally signed Car-2-x communication, cryptographic keys and credentials management, privacy enabling technologies by pseudonyms, and also in-vehicle software and hardware security to prevent hacking attacks. Most of this is ready for deployment.

Two interrelated research questions remain: how can central components of the security architecture such as hardware security modules (HSMs) that safeguard the security credentials be validated to a very high evaluation assurance level? And: how can the safety impact be assessed and mitigated if something goes wrong with the security architecture (such as an attacker obtains a key)? We address these questions currently by research within the Oldenburg Center for Critical Systems Engineering for Socio-Technical Systems.

III. Architectural Requirements in the maritime domain

The ever increasing maritime traffic density together with increasing vessel sizes and decreased navigational space due to other usages of the maritime space such as offshore windfarms has raised the need for more assisting technology for mariners as well as for pilots and shore-based personnel. Therefore, the IMO has conducted a gap analysis, which is covered in the following subsection. But also other committees from the IMO and IALA have stated some needs, which will be covered in the other following subsections.

3.1. e-Navigation

The IMO initiated an e-Navigation implementation process based on an extended gap analysis (IMO 2012) which has been lead to a strategic implementation plan (IMO 2014a) and work plan (IMO 2015). The IMO identified safety-directly-related gaps as follows (not a complete list, relevant gap numbers listed in brackets):

1. Future e-Navigation system shall support a harmonized data model/structure (gaps 111-Gte01, 111-Gte02, 111-Gte03, 211-Gte01, 235-Gte01). This harmonized data model/structure must regard security issues rising with information exchange between maritime stakeholders (shore-side and sea-side, 211-Gte01).
2. Systems shall be able to execute self-checks. (111-Gre02)
3. Data and information quality has to be assessed automatically (112-Gte01, 112-Gre01)
4. Systems must support secure communication between systems including a sufficient access management for information access (120-Gte04)

5. Systems shall cover not only navigational information but also maneuvering information (control level) in a standardized way (134-Gte04, 134-Gte05)
6. Systems shall be self-descriptive, appropriately designed for the task at hand, controllable, compliant with user's expectations and fault tolerant (134-Gte06).
7. Systems must support evolving updates of software and hardware in a way that type approval can still be done in an efficient way for the updated system (134-Gre02).
8. Systems shall be designed in a way that familiarization is easy to achieve for personnel when transferring from ship to ship (134-Gtr01).
9. Systems shall allow to receive and display safety critical information such as maritime safety information in real-time (135-Gte01) or in valuable time e. g. for SAR (330-Gte01). This information shall be processed (e. g. filtered, selected) before presenting on an electronic display.
10. Systems shall be integrated wherever possible, e. g. to allow the dispaly of maneuver information (134-Gte04), to allow automated reporting of ship internal data (140-Gte04) or to use relevant e-navigation information for SAR (310-Gte01, 320-Gte01). For this, standardized interfaces have to be provided.
11. Architectures shall support the processing of large amounts of data (260-Gte01, 260-Gte02). From the authors perspective they should even incorporate big data technologies for the generation of better situational awareness.
12. Information about vessels (as is sent e. g. via AIS) must be more accurate and dependable (260-Gte07).

Furthermore, architectures of e-Navigation system must be built on a modular basis, since they usually consist of a number of complex subsystems that are based on different standards (like ECDIS, ARPAR, Conning, VTS, portable pilot units, etc.). The IMO for example supports this requirement with its resolution MSC.252(83)(IMO 2007) on modularization of INS performance standards. This leads to the mentioned work program which references the following primary/direct safety relevant issues:

- Preparation of draft new modules, to the revised performance standards for INS
- Amendments to the general requirements for shipborne radio equipment forming part of the GMDSS and for electronic navigational aids.
- Guidelines on harmonized display of navigation information received via communications equipment

Which were named with ship reporting and the implementation of Maritime Service Portfolios (MSP). The IMO e-Navigation work plan so far did not define specific requirements on e-Navigation systems and their architectures. The IMO plans also address required interoperability of e-Navigation services by requesting a Common Maritime Data Structure (CMDS) (Weintrit 2011).

In the actual discussion this in addressed by the work on the S100 specification driven e.g. by IHO, IALA and others (IHO 2010). (Jonas & Oltmann 2013) describes the requirements for the CMDS:

- Ergonomically improved, harmonized and standardized shipboard equipment
- Infrastructure for seamless data exchange from board to board to shore
- Management of Vessel Traffic Services and other services e.g. for automatic reporting
- Harmonization of Maritime Safety Information
- Improved reliability, resilience, and integrity of navigation information
- Information for search and rescue operations.

The latter two have a direct impact on safety

3.2. User Perspective

The e-Navigation strategy of the IMO explicitly makes clear that all future developments shall have the user in the focus. This means that special attention has to be given to user needs on board the vessel and on shore. Therefore, the above mentioned IMO gap analysis was a user centric approach to identify the needs of the users. E-Navigation systems shall provide the information to satisfy such user needs for safe and efficient navigation from berth to berth including support from shore based systems. Identified needs and corresponding solutions cover technical, operational, process, training and regulatory aspects, which means that on all these levels adoptions, new developments or enhancements shall clearly state the intended user benefits.

The IMO MSC 85/26 Annex 20 (IMO 2008) shows the results of a comprehensive identification of e-Navigation users and stakeholders. The list covers different types of vessels with different purpose of usage and public and private/commercial shore site stakeholders. Of course a military vessel, a small costal fishing boat and a 6000pax cruise ship has different requirements and needs for services. Starting from this list the IMO set up a maritime service portfolio MSP as described in NCSR1.28, Annex 7 (IMO 2014d). The MSP is structured regionally and covers 16 services which are generally safety-related and require real time hardness.

For all services IMO requires Cost Benefit Risk Analysis to ensure cost efficiency of e-Navigation technologies (Skjong 2005).

3.3. Legislative and Governmental Perspective

Regulations for Ships and Equipment are specified by SOLAS regulations from 1972 with amendments by the Maritime Safety Committee of the IMO. Actual Version is (IMO 2014e). It defines the responsibility of the flag state for certification of a vessel intended for international voyages. The state are entitled to follow their due by assigning this to other bodies. The certificates for ships rely on proven equipment as to be certificated according to (EC 2014). The directive lists the equipment items, applied regulations (mainly originating from SOLAS) and testing standards.

INS has to be compliant to IMO resolutions A.694(17), MSC.36(63), MSC.97(73), MSC.191(79), MSC.252(83) and SC.302(83). Testing has to be done according to EN 60945, EN 61162, EN 62288 and IEC 61924-2 (2012).

Onshore costal states need technology to ensure the integrity of their coastal waters (Costal Surveillance Systems) also need systems to ensure lightness and safety of traffic, while safety and effectiveness requirements often lead into different directions.

3.4. Physical / Technical Perspective

E-Navigation technology comes with numerous technical requirements. They are derived from aforementioned perspectives. For example, communication channels reach, bandwidth, latency, integrity/safety/security and dependability are a set of typical requirements. Maintainability and extendibility are also technical requirements from development and maintenance perspective.

3.5. Safety

Because safety and easiness of traffic are the driving forces for e-Navigation as mentioned, safety measures supporting e-Navigation undergo a cost/benefit analysis. Weekly reports on shipping accidents are not any longer tolerated by the global society as they have negative impact on economy and ecology and touch ethical aspects. However, as stated in Section III.III safety and security measures in the development phase of equipment is still based on very old standards and regulations that are amended in an incremental way to cover new developments. However, no overarching structure of safety assessment including security measures, which would be necessary due to cooperative nature of e-Navigation, is available.

Concepts like Safety Integrity Levels as defined in ISO 61508 are currently missing in the discussion on e-Navigation.

3.6. Physical / Technical Perspective

There is awareness at the IMO on cyber-attacks initiated by the report of Canada (IMO 2014b). A roundtable of international shipping associations comprising BIMCO, ICS, INTERCARGO and INTERTAKO are developing standards and guidelines to address the major cyber security issues faced by the shipping industries. The topics covered by the discussion are: awareness and education; a generic risk-based framework drawing on existing standards and guidelines augmented by current intelligence and best practice; addressing the integrity, confidentiality and availability, management of guidelines; physical and software security; and last but not least review and assessment of cyber systems to ensure their continued robustness.

The IMO has formulated special security related requirements in the FAL 39/INF.2 (IMO 2014c), which formulates requirements on the usage of electronic certificates in the maritime domain:

1. Maritime stakeholders shall be identified via electronic certificates. This includes persons, institutions as well as equipment.

2. Certificates shall give evidence for the performance of a certificate holder and shall be used for identity and access management.
3. Checking of certificates shall be possible online and offline, since a vessel may be disconnected from internet in some areas.
4. Systems based on certificates or using certificates shall support the complete lifecycle from initial issuing of a certification until invalidation.

It has to be mentioned that these requirements are addressing e-business like applications. None of the both documents cover specific requirements for e-Navigation. Furthermore, in the maritime domain no safety architecture as defined by ETSI for the automotive domain is available.

3.7. Summary

To summarize this, the main overarching requirements on e-Navigation compliant system architectures are:

1. Systems shall be easy to integrate benefits from a comprehensive situational awareness and be able to support mariners on its several navigating and administrative tasks.
2. Systems shall be modular to allow update of subsystems independent from other systems.
3. Systems shall support a secure and dependable communication between systems for information exchange.
4. Systems shall support the processing of data on several levels of criticality (administrative, informative as well as safety-related).
5. Systems shall always have the user in focus.

IV. Developments in the maritime domain

The usage of new information technologies to increase safety, security and efficiency in maritime transportation is mainly covered by the IMO e-Navigation strategy (IMO 2008). E-navigation is defined as “the harmonized collection, integration, exchange, presentation and analysis of marine information on board and ashore by electronic means to enhance berth to berth navigation and related services for safety and security at sea and protection of the marine environment.” Figure 3 shows the IMO overarching e-Navigation architecture. From this figure, you can see a strong separation between ship-side technologies and shore-side technologies that are linked via communications links that enable operational services that may cover several aspects like safety, security, efficiency, environmental protection but also operational services like maintenance. It is important to see, that on both sides, the human operator plays an important role, which leads to special requirements on the human-machine-interface. However, the separation between ship and shore in this architecture is not only a structuring element. It is mirrored also in aspects like standards and regulatory for the technologies under consideration. This means that on the ship-side other standards and rules are important than on the shore-side.

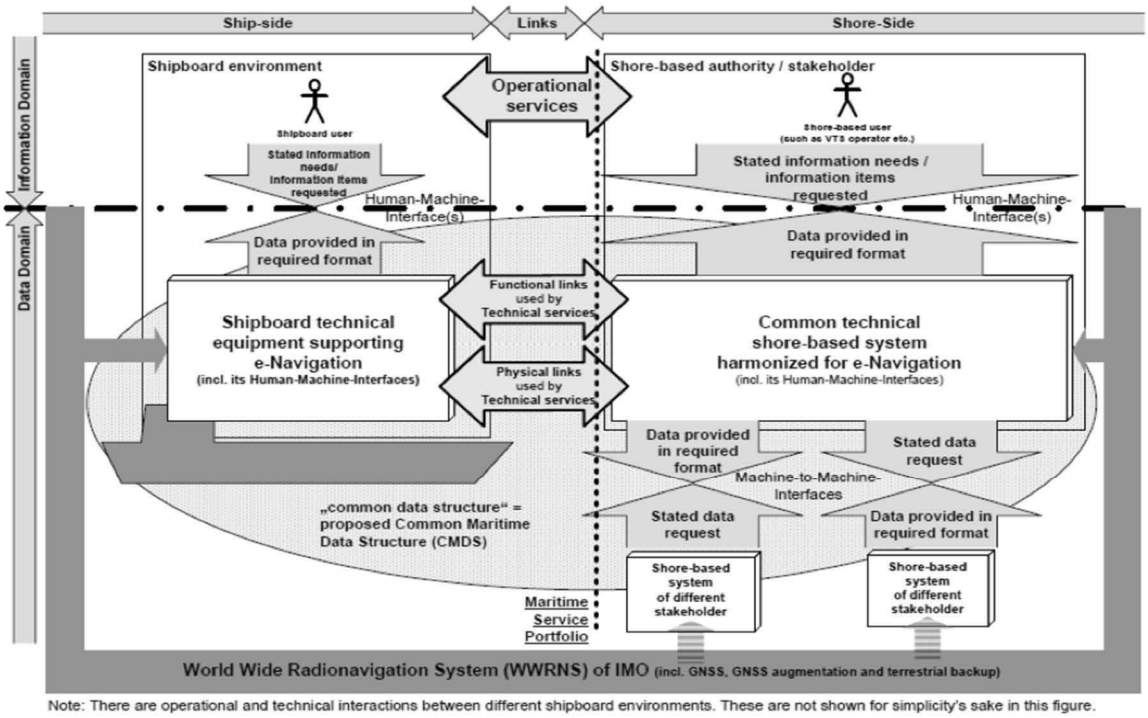

Figure 3: IMO overarching e-Navigation architecture (IMO 2011)

4.1. Ship Side Systems

Standard nautical systems on board are of course echo, log and compass in its different technological implementations. Global Navigation Satellite Systems (GNSS) have a significant impact on PNT. Radar with ARPA was a major technology to identify and track vessels, aid to navigation and obstacles. AIS is one of the most important technologies for increasing safety in maritime transportation introduced in last two decades. AIS is a system used to broadcast information about vessels (like SOG, COG, length, width, etc.) its intention (e. g. destination port) and other relevant information. The information provided either automatically set by sensors (like speed and course) or manually edited by the ship crew (like destination port) and broadcasted via a VHF communication link in an unencrypted way. INS and Integrated Bridge Systems integrate the ship side service.

4.2. Shore Side Systems

Besides Aids to Navigation (AtoN) such as buoys, lighthouses and beacons, shore side systems are established mainly for surveillance (for safety or national security reason) and to provide additional consultation in extension of the pilot services. Main technologies are radar chains along the water ways and coasts with automatic tracking using MARPA. The surveillance systems also make use of AIS receivers. Vessel Traffic Service and Coastal Surveillance System combine the information into an operational picture.

4.3. Link

Communication and the link between ship and shore side services are done using MF, HF or VHF radio communication like AIS. Services of the GMDSS provide digital information exchange for maritime safety notes and to support SAR. Satellite systems provide an additional digital communication channel. The IMO follows the vision of a Common Maritime Data Structure (CMDS) as a semantic data model to be used for ship-, shore-side systems as for their link.

4.4. Upcoming Architectures

Due to the implementation of the IMO e-Navigation strategy, but also due to operational needs from maritime stakeholders a lot of activities are currently ongoing to improve/enhance existing system infrastructures or even develop new ones.

4.4.1. Common Shore Based System Architecture

With the recommendation e-NAV 140 in combination with the Guideline 1114 in 2015 the IALA has announced a recommendation how to structure and design shore based surveillance systems and the underlying services. This IALA recommendation gives a concrete description of the interfaces between ship and shore, but also between several service types that are used on shore to support the mariner with essential information for navigation. The services are categorized into: (1) data collection and data transfer services, (2) value added data processing services, (3) user interaction services and (4) gateway service.

1. The data collection services are used to collect traffic data (e. g. from AIS or radar), weather data, hydrological data or even other data.
2. Via data couplers this data is used by value added data processing services to generate context specific information like the recognition of hazards in maritime traffic.
3. This information is then presented to the user via specific HMI services.
4. Gateway services allow to connect to external systems to either provide data to them, to collect data with them or exchange data with them.

These shore based services are linked to the vessel via communication links like VHF for AIS, satellite communication for meteorological data etc.

This architecture is the reference for implementation of future shore based e-Navigation system and will be the basis for interoperability between systems of different authorities and even beyond different nations. This reference architecture shall support the information exchange between these systems and by this integrate the information to form a comprehensive picture of the situation to make maritime transportation safer and more efficient.

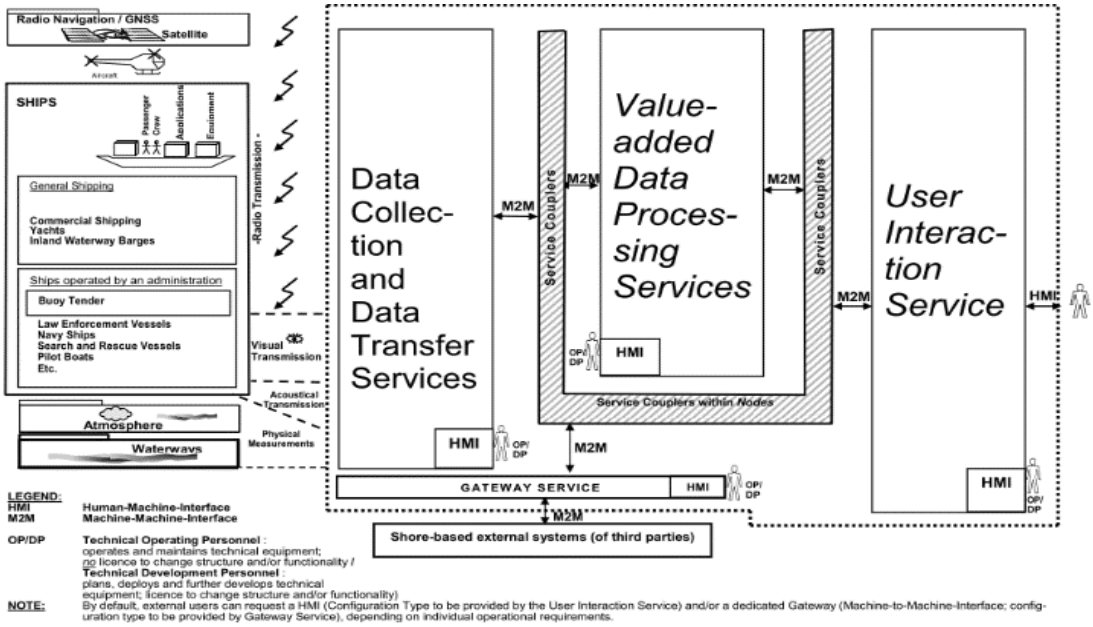

Figure 4: IMO overarching e-Navigation architecture (IMO 2011)

Having such a service oriented view will allow for a service provider to be easily integrated with the existing system compliant to this architecture and to provide value added services. In combination with the CMDS and the Maritime Cloud (see next section) this will contribute to a harmonized system environment. A use case for this could for example be an advance route planning not only considering information about the traffic in the region where a vessel currently is (e. g. the English channel) but also already regard information about traffic in the area of the destination port like the port of Hamburg.

4.4.2. The Maritime Cloud

The Maritime Cloud (Lind, JENSEN, et al. 2015) is another very promising strategic approach in the maritime domain. This approach focuses on the facilitation of the provision of maritime services. It consists of the following main components

1. Identity Management allowing maritime stakeholders like shipping companies, mariners, pilots but also equipment to get a unique ID and register for service provision and usage.
2. Service Portfolio Registry providing a catalog of services provided by service providers. This registry allows the maritime stakeholders to find a service, get a link to it and then be able to use it.
3. Maritime Messaging Service (MMS) “is a carrier agnostic messaging hub, designed to allow seamless roaming, enabling global interoperable connectivity across varying data links with varying technical characteristics and limited bandwidth.” (Lind, JENSEN, et al. 2015)
4. The ALMANAC, which is an offline copy of the identity and service registry to allow for identity and service discovery also in situation with no internet connection.

The Maritime Cloud will be a distributed platform providing a standardized way for service discovery and service usage. Its objective is, that after deployment of the Maritime Cloud the entry barriers for service provision will be significantly decreased.

4.4.3. SeaSWIM

The SeaSWIM concept (Siwe et al. n.d.) targets on setting up system wide information management (SWIM) environment in the maritime similar to the SWIM concept of the air traffic management domain. SeaSWIM builds upon the Maritime Cloud as a base infrastructure and will provide an environment for effective and efficient information exchange between maritime stakeholders. This information management environment shall support use cases like port collaborative decision making (PortCDM) (Lind, Haraldson, et al. 2015) to increase efficiency in port approaches and operations. The SeaSWIM concept is a strategic approach supporting the concept of Sea Traffic Management (STM), which was developed in the Mona Lisa project and is currently under validation within the STM Validation Project. STM aims at introducing a management infrastructure for sea traffic to benefit from a cooperative and comprehensive situation awareness to increase efficiency and safety in maritime transportation.

The SeaSWIM concept therefore will add a layer of application driven services to improve logistics and other transport related use cases with special focus on efficiency and safety. This application layer will make use of sensitive business related and personal data. So, from this concept, strong requirements on identity management, access management and secure communication channels between participating systems are drawn.

V. Comparison and Conclusions

The above sections show, that despite their differences the maritime domain and the automotive domain have some common characteristics and that they are in a similar way taking advantage of the integration of new information technology. In both domains, there is a strong need for support of driving/navigation by electronic systems. At least the following common overarching requirements exist in both domains:

1. Both domains require to have fault tolerant systems (ISO 26262 (automotive) and ISO 17894 (maritime))
2. Both domains require making information of several categories (informative and safety-related) available in a sufficient way.
3. Both domains have strong focus on the human (driver, operator, captain, etc.). Systems to be developed have to be designed in a way that they fit to users' expectations.
4. Both domains regard highly distributed systems that require secure communication channels, identity management and access management.

Furthermore, both domains follow the approach that cooperative driving/navigation will bring the most valuable benefits to the driver/mariners/operators. The architectures for such cooperative transportation systems are similar in both domains, since they consider the vehicle side and base station side and have the user in the focus. However, despite these commonalities some important differences exist:

5.1. Criticality of Systems

One of these important differences is that the theoretical concepts used in the maritime domain diverge more than in the automotive domain. While in the automotive domain, the three-layered approach shown in Figure 1 is used throughout the whole domain, such an approach does not exist in the maritime domain. This can, for example, be seen by the expectations on the AIS. Using the three layered approach from the automotive domain, AIS will obviously be mapped on the guidance level, since it gives an overview of the traffic situation. However, there are stakeholders in the maritime domain that expect AIS also to be capable for real-time data exchange of safety-related information, which would be on the control level of Figure 1. It has been explained, that due to missing real-time capabilities and security measures, this is not the case.

5.2. Safety

Besides this three layered approach, safety assessment is based on very old standards that are updated incrementally based on new requirements coming from ship accidents or new technologies available. However, the e-Navigation strategy is not adequately addressed by this approach. Especially, a concept like the ASIL is missing in maritime domain. However, this would help to standardize the development of future assistance systems with respect to their safety-criticality. At the moment, most systems are designed based on the assumption that in case of a system failure, the mariner is obliged to use paper based charts etc. However, the automotive domain shows that other approaches are possible. Furthermore, the ASIL concept will not only support the design of the systems, but also the development of services. Since at the moment, in the maritime domain a quality of service (QoS) concept for e-Navigation is missing, this could be introduced together with a Maritime Safety Integrity Level (MSIL) concept. This would mean, that for several levels of criticality, specific QoS requirements and procedures will have to be defined. These will then have to be applied to each system or service mapped to a specific MSIL. This would also give legal assurance to system and service developers, since they could simply certify their systems and services against such a standard.

Having both concepts, the three layered approach as well as a MSIL available in the maritime domain would additionally allow system developers and authorities to clearly define the use cases for such systems. As we learned from the IMO gap analysis and other maritime requirements documents, it must be avoided that safety relevant systems are used for lesser safety critical applications like e-business/logistics.

In addition, although cooperation aspects are of high importance in the e-Navigation strategy, security issues rising due to data exchange are not covered in an overarching structure or even architecture as will be summarized in the following.

5.3. Security

Threat Analysis and Security Requirements: We expect that a comprehensive threat analysis for e-Navigation will unearth threats analogous to those against V2X, and that analogous security requirements will be derived. In particular, this will include digital signing of safety-relevant messages as well as the use of hardware security modules to safeguard the necessary key material. However, we also expect various differences. We discuss here two. In the automotive as well as the maritime domain it has been demonstrated that GPS can be manipulated. While in the automotive domain in most situations the driver will easily spot such tampering by inconsistencies with the environment, in the maritime domain the authenticity of GPS is a major concern, also in view of the risk of piracy. The second example is privacy. While the V2X security architecture includes measures against location-tracking by pseudonymization, this will be less relevant in the maritime domain. E.g. a vessel can just as well be tracked by radar on the open sea. Privacy could play a role with a different emphasis, e.g. the need to remain undetected by pirates.

Identity Management and Public Key Infrastructure: The V2X architecture prescribes that every vehicle must have a unique cryptographic identity represented by a public/private key pair, and that the private key is protected by a HSM, installed during an initialization phase and managed by a Public Key Infrastructure (PKI). As we have explained in Section IV.III, in the maritime domain there are various communication architectures emerging, many of which will also require authenticated communication and with it security credentials management. Moreover, we have seen in Section III.V that the IMO has already required the usage of electronic certificates. Action is required now to orchestrate the various activities, to make sure that they do not lead to a jungle of various security credentials that exist in parallel and will be difficult to manage. The security and ultimately success of e-Navigation will depend on whether a simple, and hence, usable and maintainable security credential management system can be achieved.

Security Components and Security Certification: When it comes to specifying the details of a cryptographic architecture for e-Navigation the V2X PKI could act as a model in many aspects. In particular, V2X signatures are based on Elliptic Curve Cryptography (ECC). The main advantage of ECC schemes compared to e.g. traditional RSA is that they achieve the same level of security with a much smaller key size. This is why ECC schemes are employed in applications with real-time demands such as V2X. Since V2X is close to being ready to mass-market deployment various security components such as HSMs with ECC implementations are available on the market. We expect that these components could be used in the maritime domain just as well. Such components are typically certified according to Common Criteria, with an evaluation assurance level of at least 4+. For active cooperative applications we expect the ISO26262 will require an even higher evaluation, e.g. involving formal methods. The Maritime domain will immediately profit from such certification requirements.

Evolvement and Deployment: While V2X communication has been developed and standardized together with its security architecture, in the maritime domain there are already various communication systems in place, mainly based on radio communication. For example, AIS is an obvious candidate to serve as the basis of sophisticated collision avoidance but for this it needs to be secured. Being able to build on existing communication infrastructure brings in the usual problems of downwards compatibility and consensus on which technology to extend and which not. However, we argue here that this should be seen as a chance to avoid the "penetration paradox" of V2X: Most V2X applications based on 802.11p realize their full potential only when this technology is already widely deployed within the traffic system. Hence, unless V2X is introduced by law it might prove difficult to start it off, since it is not a feature easy to market when V2X penetration is minimal. The maritime domain has another advantage when it comes to a gradual deployment of e-Navigation: concerning shore-based e-Navigation one could anticipate a transitional phase that makes use of the piloting tradition, where ships are provided with portable e-Navi boxes brought onto the ship just as a pilot enters a ship in the beginning of the "maneuver".

To summarize the outcome is that design in the e-Navigation domain is often driven to react to specific interfaces or development focused on a specific technology. An example is AIS which is used way beyond its design rationales and misses critical safety and security aspects. It is recommended to develop future e-Navigation systems in the context of an overall safety and security approach

5.4. Seamless Roaming

Conventional maritime communication system is based on GMDSS and has narrow bandwidth that would introduce difficulties in using IP-based data communication. Data communication systems for e-navigation need to include IP-based system and non-IP-based system as well. As autonomous vehicle R&D projects does, most approaches in e-Navigation R&D projects assume a broadband communication system that could easily use IP-based data communication. Only mobile telephone network and satellite communication network can support such bandwidth. Unfortunately, unlike land vehicle, the former suffers from insufficient coverage at sea and the latter from excessive costs. With these reasons, even in the future, ships with a broadband data communication system must have interactions with ships without it during their navigation at the sea. This raises a compelling need for a seamless roaming between such data communication systems. The MMS of the Maritime Cloud could be one of the options to support a seamless roaming.

Submitted: Feb. 26, 2016 Accepted: May 25, 2016

VI. Acknowledgements

This work is funded in major parts by the Research Center Critical Systems Engineering for Sociotechnical Systems by the State of Lower Saxony

References

Anon.(2015), Pressemitteilung Nr. 15/2015 - 14.259 Kilometer: Die jährliche Fahrleistung deutscher Pkw - Erstmals Ergebnisse aus Echtdaten, Kraftfahrtbundesamt.

Donges, E.(1982), Aspekte der aktiven Sicherheit bei der Führung von Personenkraftwagen. Automobil Industrie, 27(2). Available at: http://trid.trb.org/view.aspx?id=1044474 [Accessed October 23, 2015].

Donges, E.(2012), Fahrerverhaltensmodelle. In H. Winner, S. Hakuli, & G. Wolf, eds. Handbuch Fahrerassistenzsysteme. Vieweg+Teubner Verlag, pp. 15–23. Available at: http://link.springer.com/chapter/10.1007/978-3-8348-8619-4_3 [Accessed October 23, 2015].

IHO(2010), S-100 - Universal Hydrographic Data Model.

IMO(2011), Development of an E-Navigation Strategy Implementation Plan, IMO. Available at: http://www.e-nav.no/media.php?file=96 [Accessed May 25, 2012].

IMO(2014a), Development of an e-Navigation Stregy Implementation Plan, IMO.

IMO(2014b), FAL 39/7 Ensuring Security In an Facilitating International Trade Measures toward enhancing maritime cybersecurity, London: IMO.

IMO(2014c), FAL 39/INF2 e-Business Possibilities for the facilitation of Maritime Traffic Information paper from ISO TC8 on technical options for implementing electronic certificates (ISO).pdf, London: IMO.

IMO(2007), MSC 83/28/Add.3 Annex 30 --- Resolution MSC.252(83) --- Adoption of the revised performance standards for integrated navigation systems.pdf, International Maritime Organization.

IMO(2015), MSC 95-19-8 - Implementing e-navigation to enhance the safety of navigation and protectionof the marine... (Australia, Denmark, Finla...).pdf, London: IMO.

IMO(2014d), NCSR 1.28 Report To The Maritime Safety Committee, London: IMO.

IMO(2012), Report e-Navigation Working Group, SUB-COMMITTEE ON SAFETY OF NAVIGATION, IMO.

IMO(2008), Strategy for the Development and Implementation of e-Navigation, IMO.

ITF(2012), STCW Guide for Seafarers, International Trasport Workers Federation. Available at: http://www.mptusa.com/pdf/STCW_guide_english.pdf [Accessed July 10, 2013].

Jonas, M. & Oltmann, J.H.(2013), IMO e-Navigation Implementation Strategy–Challenge for Data Modeling. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 7(1). Available at: http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-33cab930-396a-4839-b7b4-8e68f0ab3fc6 [Accessed September 11, 2015].

Lind, M., Haraldson, S., et al.(2015), Port collaborative decision making–closing the loop in sea traffic management. In 14th International Conference on Computer Applications and Information Technology in the Maritime Industries, Ulrichshusen, Germany. Available at: http://monalisaproject.eu/wp-content/uploads/Compit-2015-Port-CDM-Lind.pdf [Accessed October 27, 2015].

Lind, M., JENSEN, J., et al.(2015), Service and Communication Infrastructure for Sea Traffic Management, COMPIT, Ulrichshusen. Available at: http://monalisaproject.eu/wp-content/uploads/Compit-2015-Service-and-Comm-Infra-Lind.pdf [Accessed October 27, 2015].

Siwe, U. et al., Sea Traffic Management–Concepts and Components. Available at: http://monalisa project.eu/wp-content/uploads/Compit-2015-STM-paper-Siwe.pdf [Accessed October 27, 2015].

Skjong, R.(2005), Formal Safety Assessment and Goal Based Regulations at IMO: Lessons Learned (Invited Lecture). In ASME, pp. 319–328. Available at: http://proceedings.asmedigitalcollection. asme.org/proceeding.aspx?articleid=1575436 [Accessed October 28, 2015].

Stübing, H.(2013), Car-to-X Communication: System Architecture and Applications. In Multilayered Security and Privacy Protection in Car-to-X Networks. Wiesbaden: Springer Fachmedien Wiesbaden, pp. 9–19. Available at: http://link.springer.com/10.1007/978-3-658-02531-1_2 [Accessed October 28, 2015].

Weintrit, A.(2011), Development of the IMO e-Navigation Concept – Common Maritime Data Structure. In J. Mikulski, ed. Modern Transport Telematics. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 151–163. Available at: http://www.springerlink.com/index/10.1007/978-3-642-24660-9_18 [Accessed October 10, 2012].

There is no conflict of interest for all authors.