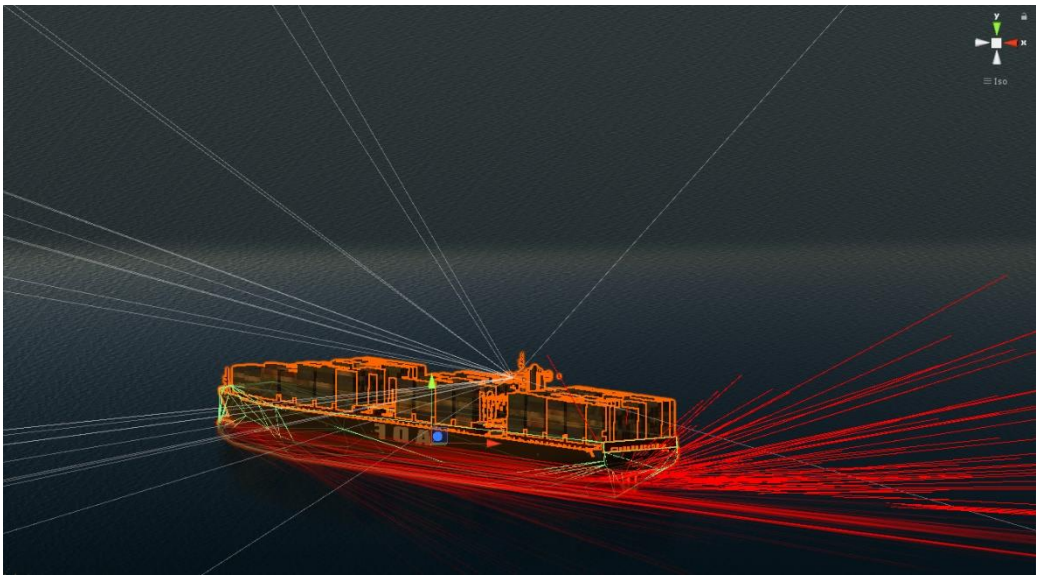
ACTRESS



Feb 22nd 2018

Architecture and Technology Development Platform for Realtime Safe and Secure Systems

Ensuring the dependability of modern open and adaptive maritime systems.

ACTRESS

ARCHITECTURE AND TECHNOLOGY DEVELOPMENT PLATFORM FOR REALTIME SAFE AND SECURE SYSTEMS

INTRODUCTION / CHALLENGES

Shipping and maritime transport provide the truly global base for the worldwide production and distribution of goods. In the year 2015 a total of more than 600.00 million containers were shipped over the world ocean routes; nearly 50% thereof were handled by the 20 most important container ports worldwide. Crude oil still serves 35% of the global primary energy needs. 25% thereof (or 1.500 million tons) were recovered and shipped offshore in 2015. In 2017 the Cruise Lines International Association (CLIA) expected 25 million passengers to enjoy the pleasure of a luxurious joyride on one of the worldwide operating 4.500 cruise liners. Without a doubt our oceans, coastal regions and inland waterways are amongst the most important ingredients to ensure wealth and prosperity, not only for the well-being of our coastal nations.

The increasing awareness about the role and sensitivity of our ocean and atmospheric environment, the ever-growing globalisation and competition and, last but not least the consumers expectations towards the immediate availability and delivery of goods any time and any place – these are the trends and demands, which will deeply impact on the future setup for a global maritime domain. A multitude of different actors, may it be from the state maritime administrations or from the commercial sector, from NGOs or private recreational interests, they are all in need for safe and reliable in-time information regarding their own domain of maritime interests. May it be the exchange of relevant ship traffic information in congested areas, the coordination between arriving vessels and the port-of-calls or the synchronisation of maritime and related land-based cargo and logistics operations – with the actors a multitude of different maritime systems need to be interconnected via different connection routes. Ship-based integrated bridge systems communicate with shore-based vessel traffic services, shipping companies have their vessels on a global digital line 24/7, seamen and passengers expect to stay connected with the rest of the world anywhere and anytime.

Taking a closer look on the maritime dimension of this new realm of global connectivity shows, that this is not just about getting digital instruments physically connected to the World-wide-Web, and it's not just about developing appropriate marine standards for communication and data exchange. With tomorrow's dynamic digital interplay between vessels, ports, terminals and so many more marine infrastructures we indeed begin to create new functional capabilities, which go far beyond the physical limits and functionalities of any local system. Tomorrow vessel traffic services, integrated ships bridges and port coordination systems will all become part of an all-embracing maritime System-of-Systems (SoS), where

each of the individual stakeholders will contribute with their home capabilities but gain significantly through the embedded synergies of such an overarching maritime connectivity platform.

With the eNavigation initiative of the International Maritime Organisation (IMO) the maritime world has long embarked on this voyage. Safer shipping, better protection of the environment and huge cost benefits in maritime transport are the promises and hopes. And indeed, politics and industry of the major shipping nations expect huge improvements through the participation in this undertaking. But it comes at a price! Global maritime connectivity surely requires an in-depth review of all current maritime practices: of legal and commercial regimes; responsibilities, liabilities and insurances; and, foremost of it all, it requires a complete re-thinking of the engineering processes for the design, integration and testing of maritime systems.

In the classical engineering approach, a system has a dedicated system boundary and comprises of connected elements which interact with each other as well as with elements beyond the system boundary. The elements themselves are regarded as black boxes. The emergent behavior of the system is defined by the behavior of its elements and their organization.

In the world of eNavigation however, system boundaries become permeable and time-variable, subject to actively participating stakeholders and processes. In such a dynamic SoS there is no central operations center, executing SoS-wide monitoring and control. Functional boundaries of operating software are no longer identical with hardware boundaries of computers and boxes. Engineers are therefore no longer in control of all functional elements in such a SoS. Failures and deficiencies occurring in a local sub-system may cause huge consequential damages in every other corner of the SoS.

HOW ACTRESS FACES THESE CHALLENGES

The BMWI-funded Architecture and Technology Development Platform for Real-Time Safe and Secure Systems (ACTRESS) is the starting point of this re-thinking of the engineering process. Partners from academia (OFFIS, Fraunhofer FKIE), industry (ATLAS Elektronik, Raytheon Anschütz, AVL Software and Functions), classification societies (DNV GL) and governmental authorities (Bundesamt für Seeschifffahrt und Hydrographie) have set up a partnership to look at these engineering challenges from all relevant perspectives. Within ACTRESS they will develop and provide new methods for verification and validation of complex highly-automated cyber-physical SoS. These methods will cover

- New architectures for safe and secure maritime SoS
- Approaches for simulation and physical based testing of highly-automated maritime SoS
- Approaches for security validation of connected maritime SoS

In additional to this theoretical background ACTRESS will provide a technology development platform, which can be used by stakeholder such as technology providers to develop, verify and validate their new maritime SoS-technologies. This technology development platform will provide

- A simulation-based environment for full virtual engineering
- A simulation-based environment for verification and validation (V&V-Lab)

- A physical mobile platform providing sensors, network and bridge systems to be brought on research vessels and boats for verification and validation of new technologies in their later operational environment
- An in-situ platform providing sensor stations at the coastline for covering land-based aspects for maritime SoS

ACTRESS will provide the foundation for future maritime SoS-engineering and also for the education of future engineers in this sector. ACTRESS will support the transfer of these new foundations into future certification and classification processes as well as into new standards and regulations for future maritime SoS.

ACTRESS methodologies, technologies and approaches will be verified within three use cases:

- On Board Cyber-Security
- Accident and emergency /SAR technologies
- Simulation based certification of ships designed as an integrated system of system

SYSTEMS OF CYBER-PHYSICAL SYSTEMS

To get a proper understanding and basis for the core ideas of ACTRESS the concepts of engineering systems of systems are defined.

The Theory of Systems

Systems engineering and therefore the underlying theory was always an encounter to manage complexity. It follows the general concepts of divide and conquer. An artefact is understood as a system with interacting elements. The NASA Systems Engineering Handbook states: "(1) The combination of elements that function together to produce the capability to meet a need. The elements include all hardware, software, equipment, facilities, personnel, processes, and procedures needed for this purpose. (2) The end product (which performs operational functions) and enabling products (which provide life-cycle support services to the operational end products) that make up a system."

Therefore, a system has a dedicated system boundary and contains connected elements with interact with each other and elements beyond the system boundary. The elements themselves are regarded as black boxes. The emergent behavior of the system is defined by the behavior of its elements and their organization. Nether the less each element can be regarded as a system themselves. This leads to an aggregation hierarchy. Engineer can address the design challenges of each system in the hierarchy in a clearly demarcated way. One of the most critical aspect of Systems is its architecture, therefore the organization.

Cyber-physical Systems (CPS)

Today’s technology with integrated sensors, actors for interaction of the physical and the virtual world lead to a specific breed of systems. Cyber-Physical Systems (CPS) are integrations of computation with physical processes. Computing elements monitor and control the physical processes. Usually there are feedback

loops where physical processes affect computations and vice versa. There are specific aspects of CPS like the passage of time is inexorable and concurrency is intrinsic.

System of Systems

Systems Theory is designed to manage complexity by assuming that a system is a properly defined aggregation of elements and optimally under full control of the engineer. This ideal assumption is not applicable always. Open systems may have a permeable system boundary, so elements can get in or out of the system. Additionally, elements may change their behavior in an uncontrolled way. This is open systems are named a systems of systems (SoS). Systems of Systems Engineering constitutes a major challenge for the 21st Century and research into this topic has become an imperative.

Systems Engineering

The term Systems engineering is an outcome from the Bell Telephone Laboratories in the 1940s. System Engineering covers design and manage complex systems over their life cycles. There are numerous approaches for methodologies for system engineering.

Systems engineering encourages the use of modeling and simulation to validate assumptions or theories on systems and the interactions within them.

TECHNOLOGY DEVELOPMENT PLATFORM – METHODS

To support the development of future maritime SoS ACTRESS will analyze the development process of such systems and develop new methods for maritime SoS engineering in the several development steps. ACTRESS will especially focus on the following to main aspects:

Architectural concepts

Safe and secure cyber-physical SoS need a solid foundation – its architecture – to provide safety and security already by the design of the SoS itself. Therefore, ACTRESS will develop new architectural concepts for SoS engineering that will cover several aspects of safety and security. The main goal of these concepts will be an increasing resilience against cyber-attacks for ensuring safety of the SoS. For this, ACTRESS work on the following research questions:

- How can open point/ports in existing architectures be identified systematically or event (semi-) automatically?
- How can a SoS detect that is has been attacked and that parts of it are not secure/trustworthy anymore?
- Which automatic counter measures are possible?
- How can sub-system in a SoS collaborate to limit the attack and protect the rest of the SoS?
- How can a safe and secure fallback level be reached and guarantee that the system will be safe with less functions?
- How can a safe and secure system recovery be implemented that can be run automatically in case of a cyber-attack?

- How can safe and secure architecture be realized while guaranteeing real-time capabilities?
- How can self-learning systems and system updates be considered in system architectures without the need of recertification of the whole system?

Verification and Validation Methods

Besides the architectural concepts, which cover the design time of a SoS the verification and validation methods focus on the assurance that the design follows its specification and behaves correctly with respect to its later operational environment. The research questions to be addressed within this field can mainly be derived from the following to characteristics of highly automated maritime SoS:

Dynamic SoS configuration

While traditional systems are static in their operational environment, future maritime systems will be connected to other systems and by this will build up a maritime SoS. However, this configuration will not be static, since during operation of these systems new systems like new vessels entering a VTS area will enter a certain SoS configuration and other will leave it. This makes it necessary to handle a multitude of different system configurations within a SoS environment.

High-automated functions and artificial intelligence

While traditional systems usually have a deterministic input/output behavior within a well-defined system scope, this does not hold for highly-automated systems anymore and even not for systems using artificial intelligence. The following example illustrates this.

Testing a light on a vessel is fairly simple: A light detecting sensor will be installed in a specific distance and angle to the light and measure the brightness and wave lengths. If the values are within a predefined interval the test is passed.

However, testing an automatic collision avoidance system for autonomous vessels will be much more complex. Not only that the operational space, in which such a system will operate, has an infinite number of traffic situations also the possible number of reactions with evasive manoeuvers is infinite. This makes it hard to define the test cases that representative enough to guarantee a safe operation of such a system in all potential situations.

Thus, for the V&V phase of the development process ACTRESS addresses the following research questions:

- How can seamless verification and validation be realized allowing V&V already in the early steps of the development process?
    - This will cover aspects for model-, software-, hardware- and physics-in-the-loop technologies
- How can rare events like safety relevant situations and cyber-attacks be verified and validated realistically?
- How can real-time capabilities be verified and validated for highly-automated maritime SoS?
- How can a sufficient test-coverage be reached for highly-automated maritime SoS?

TECHNOLOGY DEVELOPMENT PLATFORM – INFRASTRUCTURE

The structure of a Technology-Development-Platform is described as an environment, where systems or System of Systems (SoS) are tested, validated and verified in simulative and physical scenarios with the aid of test methods. Under normal conditions and especially in adverse environment there is a substantial demand for the protection of functional and real-time properties of security-critical SoS. For the development of products in the maritime industry the provision of secured test methods carried out in a Technology-Development-Platform is essential. The infrastructure of the Technology-Development-Platform is divided in four segments

Co-Simulation

The simulation environment base on a Co-simulation already includes a maritime traffic simulation, sensor data simulation and an environment simulation. These simulators will be expanded by a simulator for underwater and airborne operations.

V+V-Lab

The shore-based researches are carried out in a laboratory environment to develop verification and validation procedures. Data obtained in In Situ platform and the Co-Simulation are integrated to cover scenarios with ship system and System of Systems.

In Situ Platform

In ACTRESS a test track in the German bay in the triangle of Helgoland, Wangerooge and Cuxhaven is built to carry out experiments and to try out new technologies. The test track is monitored with specific sensors like Radar, AIS and video, the obtained data can be transmitted by a communication infrastructure.

Mobile Platform und Sensors

For the test at sea coverage a mobile platform is constructed to provide an addition test infrastructure that can be installed aboard ship. The mobile platform can be used as a complete bridge to run assistance system tests. Additionally, a multi-sensor platform (MODAR system) is installed aboard ship to incorporate optical measurement data.

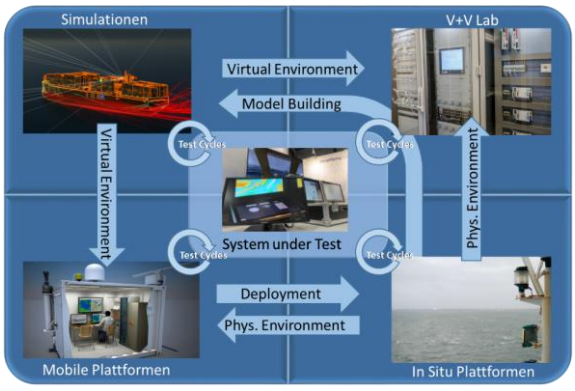


FIGURE 1: ACTRESS V+V PLATTFORM ELEMENTS

Open Platform Concept in eMIR

All of the above infrastructure will be integrated into the e-Maritime Integrated Reference Platform (eMIR). Via eMIR this infrastructure will be accessible by all interested parties. The platform is explicitly designed to be used by other research projects, by industry but also authorities. Concrete usage requests can be negotiated via OFFIS with the involved partners.

eMIR is designed to be an open platform that can and shall be extended and improved incrementally by industry, research and authorities. Therefore, new systems, components and ideas to be integrated into eMIR are very welcome.

USE CASE „ON BOARD CYBER SECURITY“

Numbers and possibility of cyber-attacks are increasing worldwide, especially the number of professionally organized attacks is rising dramatically. Fast growing and often under engineered systems of systems are levering the potential risk and degree of damage additionally. Risks often emerge from loosely coupled system compounds. Most systems today are not yet integrated navigation systems, providing deterministic backup layers. Fulfilling complex technical workflows, nautical staff is dependent on proper working technology more than ever. Different regulations regarding cyber security are arising in the maritime context today, but a coherent set of requirements, including very pragmatic customer and manufacturer needs does not yet exist. To ensure cyber security aboard is the first step to us, before we will think about taking a second one towards autonomous systems.

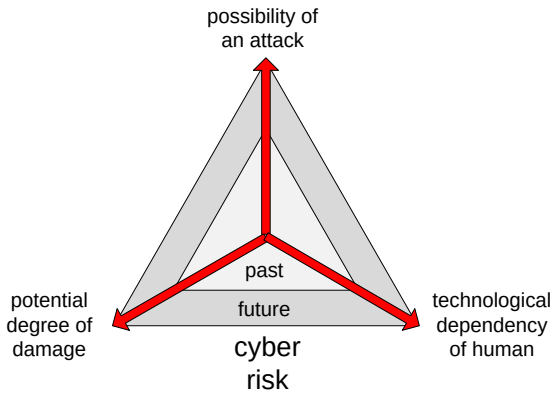


FIGURE 2: THE IMPACT OF CYBER RISK

Using the example of a navigation system our undertaking is to analyze the weak points of nautical IT systems today in order to identify ways to:

- secure the navigation system throughout its lifetime against cyber-attacks (close entry points for attacks)
- identify attacks in the case that they could not be prevented
- notify the navigator about the attack in a meaningful way, also pointing out the consequences for the navigational functionality as intuitive as possible
- fight back an attack or to render it harmless, if it has been identified

- re-design the architecture for future systems to behave resilient and non-problematic even in the case of unidentified attacks and to prevent domino effects
- support the crew in restoring the systems functionality (free of malware) after an attack
- enable the system to self-diagnose whether it has been manipulated, damaged or corrupted
- notify and document all security related events

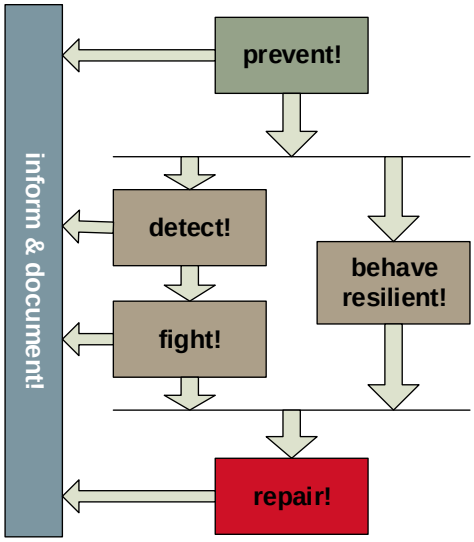


FIGURE 3: MEASURES AGAINST CYBER-ATTACKS

USE CASE „ACCIDIENT AND EMERGENGY / SAR TECHNOLOGIES“

According to the World Shipping Council (WSC) it is estimated “that for the combined nine year period from 2008 to 2016, on average, there were 568 containers lost at sea each year, not counting catastrophic events, and 1,582 containers lost at sea each year including catastrophic events. And although the number of containers lost at sea represents a very small fraction of the total number of containers carried on ships each year, the industry continuously strives to reduce these losses further. “

Most of these efforts however concentrate on measures to better secure those containers on board. Once a container gets lost at sea however, further options become very limited. Like in the Hollywood drama „All is lost“ most drifting containers remain afloat with nearly neutral buoyancy, i.e. they become extremely dangerous and nearly invisible shipping hazards just at or beneath the ocean surface.

Containers get lost at sea in heavy weather, vessels listing after water ingress or during final catastrophic events like e.g. the grounding of MV RENA on Wednesday, 5 October 2011 on the Astrolabe Reef off the Bay of Plenty, New Zealand. The ship was carrying 1,368 containers, eight of which contained hazardous materials, as well as 1,700 tons of heavy fuel oil and 200 tons of marine diesel. Besides a major oil spill 88 of her 1368 containers had fallen into the sea.

In case of such a catastrophic event it is of highest priority for the search & rescue team to quickly scan the scene for all relevant information, helping to compile a reliable and consistent operational picture – both

underwater and at the surface. First on-scene sightings are usually limited to visual and radar observations. Underwater information in most cases however remains limited to a-priori information gathered from local sea charts. The true underwater scenario with shallow rocks, hull fractures of the disabled vessel, drifting containers and other debris however may pose major additional risks to the rescuers – risks which go undetected without special precautionary measures.

In order to gain further on-scene knowledge without putting rescuers or valuable rescue gear at incalculable risk, a combination of manned and unmanned platforms (diving, afloat & flying), systems and sensors will play a major role in future. Their ability to collect and provide fast and reliable situational awareness – in the air, at the surface and sub-sea – significantly eases the pressure for on-site commanders. But it will also in future help to expedite necessary rescue decision making.

Starting point of the scenario is a vessel involved in a damage or grounding happening within a confined traffic route or fairway in rough weather conditions. Shortly after the initial emergency call just an estimated position and rudimentary information regarding the nature of the incident are known. It is however suspected that containers and other debris might have got washed over-board and are supposed to be still adrift in close proximity to the stricken vessel.

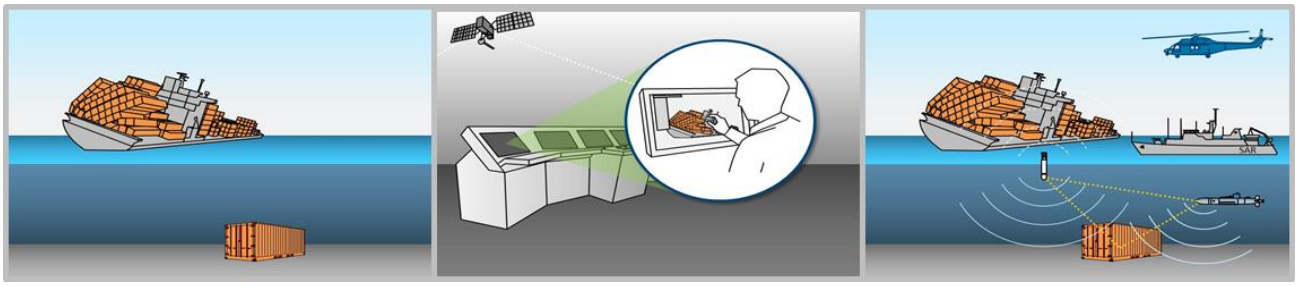


FIGURE 4: DRIFTING CONTAINERS POSING MAJOR RISK TO RESCUE TEAMS

The MRCC or the on-scene commander will then need to take immediate action. The fairway gets closed right away to keep upcoming traffic away from collateral collisions with the obstacles.

Various sensors, systems and platforms are now to be deployed in the best available manner to quickly collect all relevant information, without putting the rescue team at risk. Assets might include search from land, air, ships or underwater.

- All observations and sensor missions are to be planned due to available fragmentary incident information, environmental conditions, the vessel's past records and the actual and specific performance characteristics of the available sensor systems. The overall set-up is complex and will include an extensive catalogue of both technical as well as operational challenges, as e.g.: Planning of observation and deployment of sensor systems
- Data acquisition and evaluation of underwater situation using multi-sensor configurations
- System interfaces, integration and data- communication from all involved sources
- Configuration, safety and stability of a dynamic, multi-domain communication network (space, air and sub-sea)
- Reliability, quality and integrity of autonomous data acquisition, processing and analysis

- Integration of survey results in overall situational awareness and rescue mission planning.

The following graph gives an overview of the scenario set-up including the involved actors, the boundary conditions and the available sensor systems available for immediate employment.

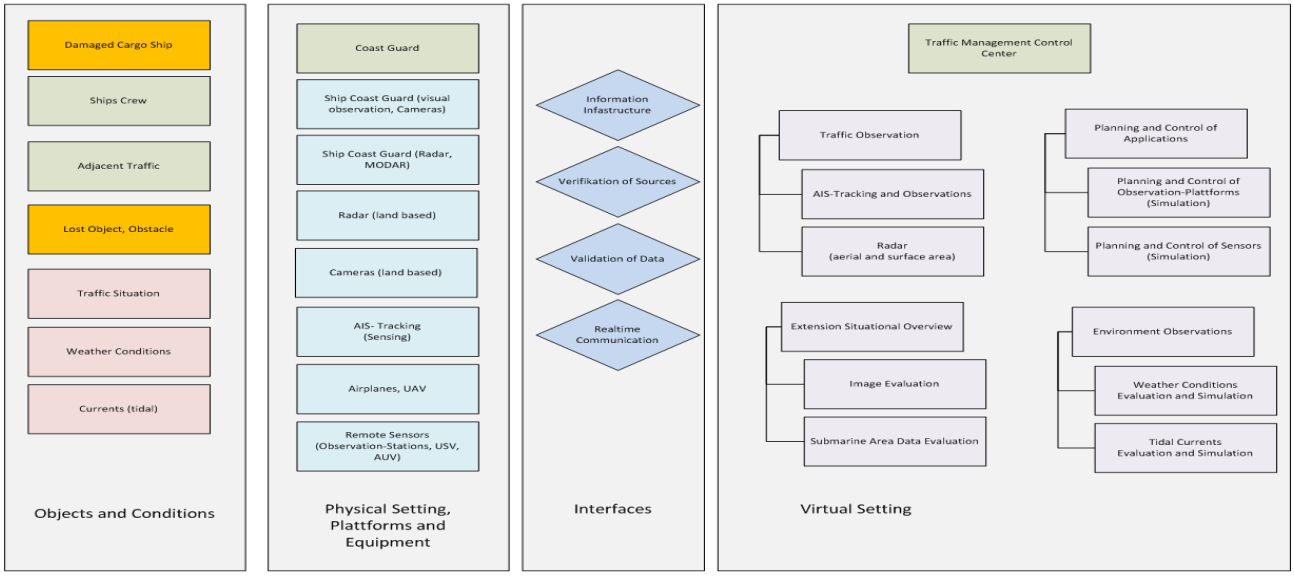


FIGURE 5: COMPLEX RESCUE SET-UP OF DIFFERENT ACTORS AND OPERATIONS

Primary focus of this scenario aims at the development of new methods and tools for the seamless and reliable integration of remote sensors in manned SAR missions. Ultimate goal here is a true cooperation between humans and machines in complex and time-critical situations, where circumstances and resources do not allow for human-controlled laborious and time-consuming pre-survey missions.

ACTRESS contributions to this scenario shall primarily be based on simulation-driven exercises aiming at the development of a basic understanding of the critical components in such complex human-machine cooperation. With this the planned studies will contribute significantly to a deeper understanding of complex System-of-Systems and their specific design challenges.

USE CASE „ SIMULATION BASED CERTIFICATION OF SHIPS DESIGNED AS AN INTEGRATED SYSTEM OF SYSTEMS “

The classic architecture of the system cluster ‘ship’, consisting of functionality focused units, follows the trend towards inter-influential ‘networking systems’, which already is state of the art in industry plants and automotive technology. This shift gives rise to new attack scenarios and fault propagation and requires appropriate protection to mitigate these effects. The security focus of AVL is on the propulsion system of the ship which consists of many subsystems working hand in hand to ensure the maneuverability of the ship. Both the interconnection and the subsystems itself need a high level of self-monitoring, failure recognition and –management to insure reliability in operation.

The construction of a ship as a complex technical system in a huge structural shell offers numerous points of attack against the technical equipment. In this structural environment, cyberattacks may come in new

and unique shapes which must be investigated, analyzed and evaluated. Cyberattacks don't normally occur out of the blue, they must be prepared in advance and often can be deployed in a critical traffic situation cause maximum harm. These circumstances have to be researched and discussed between partners with different points-of-view to design the network architecture with optimal security characteristics for a reliable protection of ocean shipping.

The increasing interconnection of systems gives rise to new challenges for the operating staff and the design of human-machine-interfaces. Even high complex self-monitoring systems must be able to report the system status to humans without causing misconceptions or overstraining them with poorly coordinated failure reports. Spoofing of monitoring systems poses an additional threat and may be used to deceive the operators and to veil upcoming technical problems caused by malfunctions or cyberattacks.

Based on the simulation environment used in this project we shall evaluate, how far these issues can be reconstructed and researched and what capabilities of the simulations are essential. The goal is to find out to what extend the technical and behavioral characteristics of complex systems can be investigated with simulation technology to perform a certification process.

Even before autonomy becomes a reality onboard ships, use of assistance and support systems will gradually increase. As in the automotive industry, assistance systems will become capable to influence the vehicle's motion. In early scenarios, humans will of course still interact with the systems and will stay responsible. But even in this case, the direct interaction of onboard systems including bridge, automation and propulsion systems, will lead to new challenges which will need to be considered in approval and certification of such systems of systems (see Figure 6). Today, bridge console and assistance systems do not communicate directly with ship propulsion. Safety relevance of such direct interaction will need to be examined.

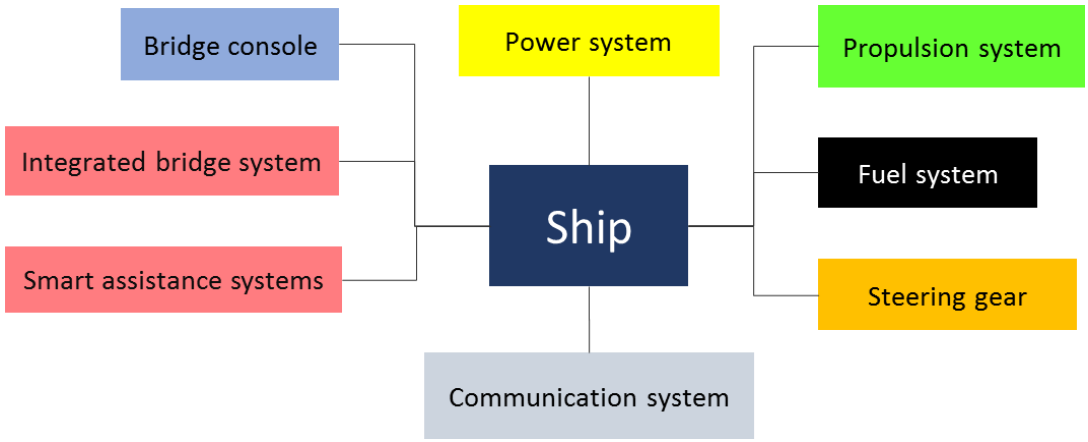


FIGURE 6: SHIP AS SYSTEM OF SYSTEM

As software has a central role in control systems and even more so in assistance systems, the ACTRESS project will utilize simulation based methods to assure the integrity of systems of systems. Such simulations will include the embedded software either through Hardware in the Loop or Software in the Loop procedures. The application of simulation based testing approaches in connection with approval and

certification of systems of systems will be investigated in the project where safety relevant functions are affected.

Actual deployment of integrated assistance systems in ship operation will start in those areas where complexity is higher already today. This would most likely be navy, cruise, mobile offshore units and research vessels as is visible e.g. through increasing use of dynamic positioning systems.

We assume that the next step towards autonomy will be taken through assistance systems realizing partial autonomy. These would support ship officers e.g. through navigating and operating in selected profiles. Consequently, integrated bridge systems would interact with control and monitoring components of the propulsion system, with power management, and with positioning and navigation systems. Through these connections, cyber risk could increase if cyber security and cyber safety are not managed appropriately.

For that reason, ACTRESS will examine scenarios relevant in the deployment of such systems of systems. Particular focus will be on those cases where safety critical functions can be affected. Several scenarios will be considered in the ACTRESS project.

a. Scenario „Loss of maneuvering capability through loss of propulsion“

   Loss of propulsion might be caused on the one hand through e.g. engine failure, mishandling of the control lever, or failure in secondary / supply systems. On the other hand, assuming direct interaction of systems, cyberattacks could affect several different control systems relevant in this scenario. These include engine control, control of secondary systems, higher level control systems coordinating the interaction of secondary systems, control of rudder and controllable pitch propellers, bridge systems with connection to the propulsion system or remote monitoring and alarm panels in UMS operation. Mechanisms for updating control system software will need special consideration as they might pose an additional risk. This affects both procedures for appropriate testing of a new software version to ensure safe operation (-> cyber *safety*) as well as procedures ensuring secure communication and a controlled update process itself (-> cyber *security*).

b. Scenario „Simulation based approval and certification of integrated assistance systems for ship operation“

   This scenario will consider the case of an integrated bridge system which directly interacts with the propulsion control system. Approval and certification of such interconnected systems with the help of system simulation will be examined. This will build on the simulation of partial systems such as the navigation system and the propulsion system. Vulnerability to cyberattacks, in particular regarding the interaction between systems, will be considered.

c. Scenario „Simulation based re-certification of integrated assistance systems for ship operation“

   This scenario will check how simulations performed for system approval can be re-used to verify system integrity in the operation phase (see Figure 7). This refers to the case after a disruption of operation because of failure of a system after a cyberattack. Assuming erroneous inputs from an

integrated assistance system, it will be checked how a safe operational state can be re-established despite direct connection between systems.

In this scenario, the mobile platform on board the BSH vessel ATAIR will be used to acquire actual sensor signals and use them as inputs for the system simulation.

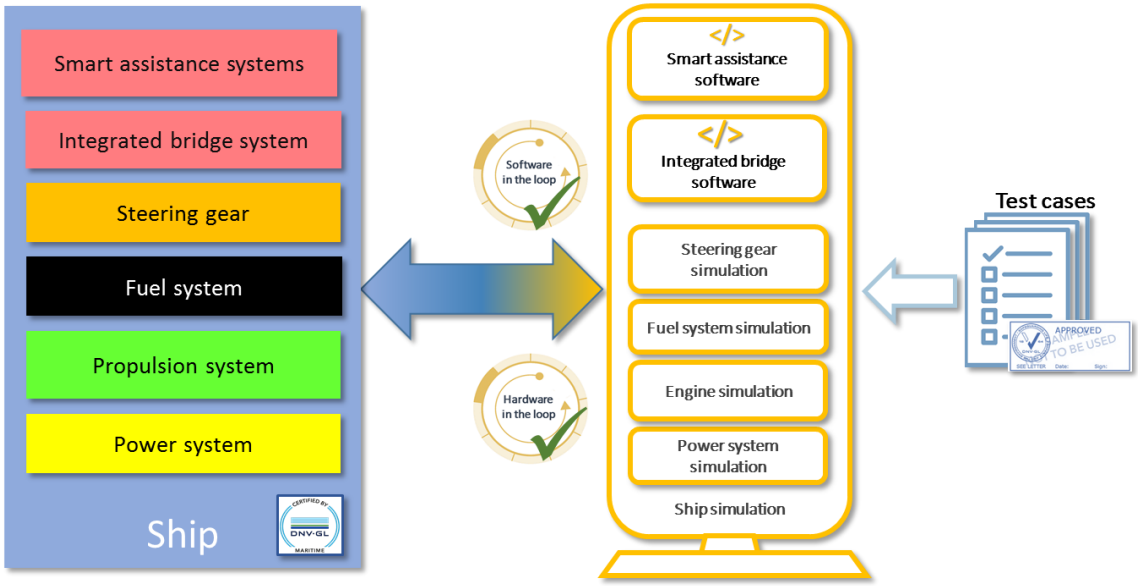


FIGURE 7: CRITICAL SYSTEMS ONBOARD THE PHYSICAL VESSEL WILL BE VERIFIED THROUGH SIMULATION BASED ON A DIGITAL TWIN.

ACKNOWLEDGEMENTS

This work is co-funded by the German Federal Ministry of Economic Affairs and Energy within the "Förderung von Forschung, Entwicklung und Innovation auf dem Gebiet der Echtzeittechnologien für die Maritime Sicherheit".

THE ACTRESS RESEARCH COLLABORATION

ATLAS ELEKTRONIK

AVL

BSH

DNV·GL

Fraunhofer FKIE

OFFIS

Raytheon Anschütz