ROBUST ON-BOARD SHIP EQUIPMENT

TRITON

PROJECT FINAL REPORT

Grant Agreement number: 312687

Project acronym: TRITON

Project title: Trusted Vessel Information from Trusted On-board Instrumentation

Funding Scheme: Collaborative project

Period covered: from 01/12/2014 to 31/03/2016

Name, title and organisation of the scientific representative of the project's coordinator[1]:

Dr. Marco Pini, Istituto Superiore Mario Boella

Tel: +39 011-2276436

Fax: +39 011-2276299

E-mail: pini@ismb.it

Project website[2] address: http://tritonproject.eu/

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the Grant Agreement.

[2] The home page of the website should contain the generic European flag and the FP7 logo which are available in electronic format at the Europa website (logo of the European flag: http://europa.eu/abc/symbols/emblem/index_en.htm logo of the 7th FP: http://ec.europa.eu/research/fp7/index_en.cfm?pg=logos). The area of activity of the project should also be mentioned.

Table of Content

1 Final publishable summary report

1.1 Executive summary

As a matter of fact, Ship Reporting Systems (SRS) are today the backbone of maritime surveillance and control, but their contents can be counterfeit by malevolent operators. Nowadays, intentional attacks to SRSs are increasing and the advances of mass-price technology make such attacks a potential and serious threat for the civilian and commercial maritime surveillance.

TRITON stands for **TR**usted vessel **I**nformation from **T**rusted **O**n-board i**N**strumentation and aimed at improving the intrinsic robustness of some on-board equipment used in SRSs, namely the Automatic Identification System (AIS) and the Global Navigation Satellite System (GNSS) receiver. The project wanted to increase the awareness on the problem of cyber-attacks and contributed to increase the overall trustworthiness of SRSs and, in turn, the security of the maritime domain as a whole. From a general point of view, the project focused on a twofold objective:

- the first concerned a robust GNSS receiver, able to mitigate intentional jamming and spoofing attacks (complementing GNSS authentication mechanisms foreseen by the next generation of Galileo signals), providing a "trusted" satellite-based source for Position, Navigation and Timing (PNT) data. The TRITON team worked on the design and development of proper signal processing algorithms for the detection of intentional interference over legacy signals. The use of Galileo signals added value to the demonstrations, that revealed the importance of a multi-GNSS scenario to intrinsically increase the level of security associated to some cyber-attacks;

- the second dealt with a secure communication link from the vessel to vessels and from vessel to shore base stations. The TRITON team worked on the design and development of an additional communication layer over the standard Very High Frequency (VHF) band used by AIS, exploiting the frequency diversity provided by the "white spaces" segment of the Ultra High Frequency (UHF) band. This improved the reliability of current communication links, ensuring the necessary Quality of Service.

The effort resulted in the realization of prototype, that serve to demonstrate the "proof of concept". The performance of such nav/com prototype were assessed through a dedicate test campaign at the Joint Research Center (JRC) of the European Commission, in Ispra Italy.

The technical and scientific work was complemented by an early business assessment of the technical solution, through a Cost-Benefits Analysis (CBA). This served to identify key added values of the new solution compared to the system currently in use. Finally, a specific analysis was carried out to assess the existing *corpus legis* in the field of maritime surveillance and identify rules and legislative proposals at EU and international level related to the topic studied in TRITON. This analysis provided a set of recommendations in order to address the major results of the project to the most suitable working groups and regulatory committees involved in maritime security affairs.

1.2 Context and project objectives

In the frame of the maritime domain awareness (MDA), the ship reporting systems are the main source of information. Vessel unique ID, date, time, position, course and speed are some of typical information automatically and periodically provided by these systems (e.g., each hour, at least 4 times a day, etc. depending on the applicable regulation).

Systems such as AIS (Automatic Identification System), LRIT (Long Range Identification and Tracking) and VMS (Vessel Monitoring System) are today the backbone of maritime surveillance, safety and security. Further non-cooperative systems exist as well (e.g. coastal radar), but data provided by ship reporting systems is taken for the most part at face value.

1.2.1 The role of GNSS

Services based on Global Navigation Satellite Systems (GNSS, including GPS) are currently in use for navigation, precise positioning and timing reference and synchronization in a large number of critical systems. In the maritime sector, GNSS-based services include ocean and costal navigation, vessel collision avoidance, fisheries monitoring and emergency management.

GNSS signal power levels are extremely low due to the large satellite-receiver distances. The use of GNSS in safety (e.g.: collision avoidance) and liability critical (e.g.: fishing monitoring) applications rises concerns about intentional interference, which attempts to deliberately disrupt nominal GNSS operations. In this context, attention must be paid to the threats posed not only by unintentional and intentional jamming, but also, even more, by spoofing. Spoofing refers to the transmission of counterfeit GNSS-like signals that force the victim receiver to compute erroneous positions. Spoofing's objective is to convince the user that he is somewhere he is not.

1.2.2 The role of the communication segment

In principle, naval safety can be split into autonomous and cooperative. The former can be identified by all the autonomous actions of the vessels, such as their respective positioning and communications towards a central control station (also through satellites). This constitutes a first layer. However much more safety services can be designed by the cooperation among nodes. This, indeed, requires a secure and robust communication segment.

In fact an ideal communication segment for cooperation among vessels should provide the architecture with the following characteristics: a) Distributed approach; b) Scalability; c) Flexible authentication infrastructure; d) Robustness against DOS attacks and selective jamming interferences; e) Robustness against possible hidden terminal scenarios; f) Broadband transmission resources. Unfortunately, current AIS systems cannot fulfil all these requirements, and basically satisfy only the first two, namely a) and b). TRITON does not criticize current AIS solutions, but rather proposes to enforce them, based on techniques which have been developed in the meantime and to complement them with wireless resources which have been recently freed worldwide (white space bands).

1.2.3 The concept

The TRITON project aimed at improving the intrinsic robustness of the *on-board equipment of ship reporting systems* (e.g. AIS-transponder, VMS-equipment, LRIT-transponder), contributing to increase the overall trustworthiness of these cooperative systems and, in turn, the security of the maritime domain as a whole.

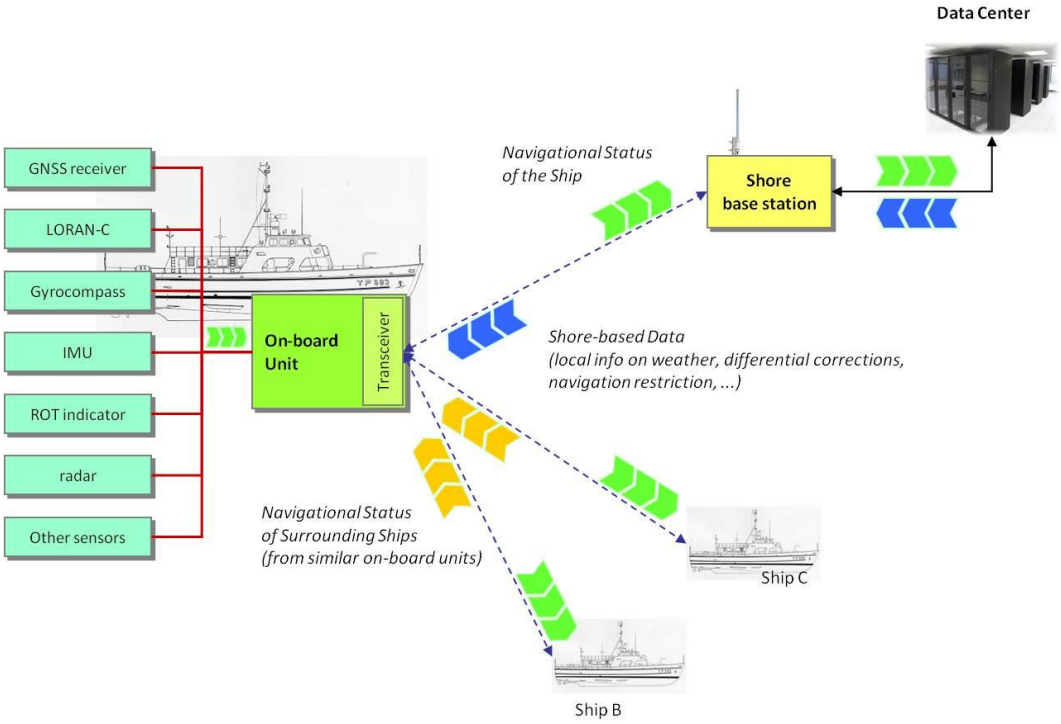


Figure 1: The role of the on- board unit of a ship reporting system.

As critical part of a cooperative reporting system, sketched Figure 1, the on-board unit typically:

1. **gathers** significant information concerning the navigational status of the ship, such as its ID, accurate position, course over ground (COG), speed over ground (SOG), heading, rate of turn (ROT) and other safety-related data. To do this, the on-board unit (the transceiver) relies on the data provided by both positioning systems and other navigation sensors (gyrocompass, ROT indicator, etc.);
2. **transmits** the information via a radio link to be received by other vessels and/or shore-based stations;
3. **receives** similar navigational data from other ships (basically for anti-collision avoidance) and/or data from shore-based stations (i.e., local information on weather, restriction to navigation, differential corrections, etc).

Taking into account this scenario, the TRITON project focused on a twofold objective: (i) the first concerned a GPS/Galileo receiver robust to intentional jamming and spoofing attacks; (ii) the second aimed at enhancing the robustness of the communication link from the vessel to vessels and from vessel to shore base stations.

1.2.3.1 Hardening GNSS receivers against spoofing and jamming

Acknowledging the primary role of GNSS to support present ship reporting systems, the TRITON project focused on the GNSS-based positioning systems which interface with the on-board unit. The aim was to provide to the on-board unit a "trusted" GNSS-based source of positioning and timing information, robust to some intentional jamming and spoofing attacks, supporting the purposes of a robust ship reporting system. This is sketched in below.

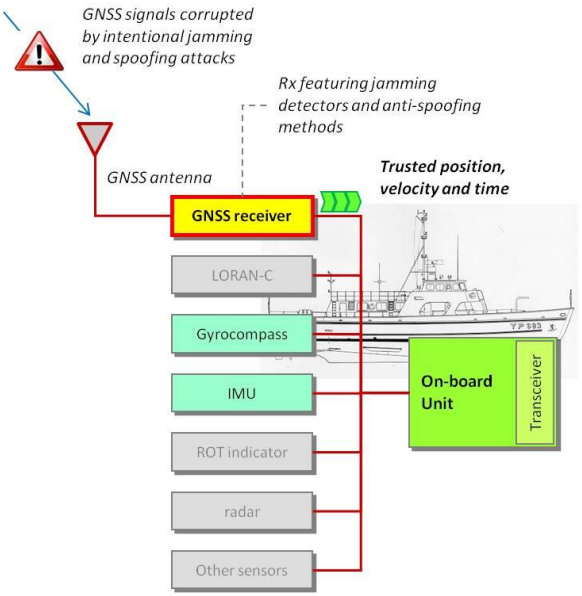


Figure 2: The role of the robust GNSS receiver under development in the TRITON project.

Particularly, the TRITON project analysed, studied, designed and developed possible countermeasures against GNSS spoofing which can be implemented in GNSS receivers typically used in maritime applications.

1.2.3.2 Enhancing communications

TRITON proposed to enforce AIS reliability and safety, by adding a new communication channel in the UHF band. The proposed approach is based on the introduction of a secure communication module on top of a standard AIS transceiver. This module exploited the "white spaces" freed by analog TV, offering a broadband channel enabling several services and enhancements to the current system.

As shown in Figure 3, the two modules will be connected via a cabled link, on which they will share different type of information: the AIS module sends a copy of its messages (for redundancy) as well as a snapshot of the current VHF channel allocation; the WSC module, after a computation based on the channel perception of his neighbours, sends back indications for an optimal slot allocation, implementing new mechanisms for guaranteeing a secure communication in the VHF segment.

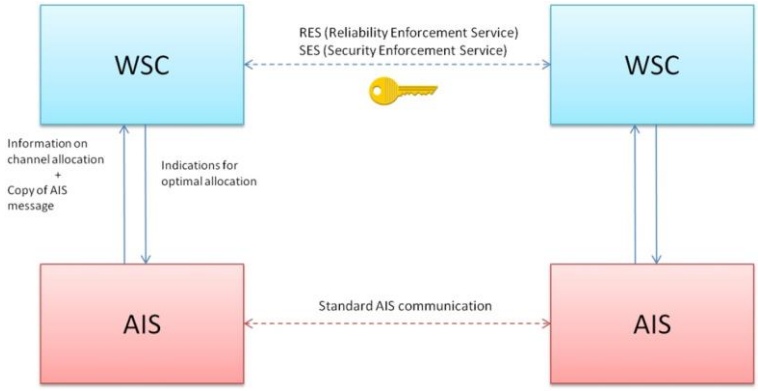


Figure 3: Architecture of the White Space Communication layer

The main issues related to security concern the lack of mechanisms guaranteeing authentication, integrity and reliability of messages. In particular, the widely used techniques for securing other families of communication networks do not suit this specific case, mainly in terms of bandwidth.

Moreover, the current AIS systems use a limited and "closed" set of messages, resulting in a low flexibility of the message structure for what concerns possible extensions enabling security.

1.2.4 TRITON objectives

The main objective of the TRITON project was the improvement of the on-board unit of ship reporting systems, contributing to increase the overall trustworthiness of these cooperative systems and, consequently, the security of the maritime domain. Particularly, the **objectives defined at the beginning of the project were:**

- the implementation of GNSS anti-spoofing techniques for improving the robustness of on-board ship GNSS receiver;
- the use of GNSS jamming detectors to warn users in case of intentional attacks on legacy signals;
- to enhancement of communication standards, aiming at improving the security and reliability of ship-to-ship/ship-to-shore communications, through the introduction of additional services for security purposes;
- the analysis of "cooperative positioning" concept borrowed from car-to-car (road transportation) to ship-to-ship (maritime segment), aiming at improving the availability of ship positioning/timing service in case of GNSS outages;
- the design, implementation and validation of a "proof of concept" prototype platform;
- an early business assessment of the technical solutions proposed by the TRITON project, through a Cost-Benefits Analysis (CBA) to identify key added values of these solutions over the currently available technologies;
- the analysis of current EC policy and regulations to provide guidelines considering future maritime applications and advances brought by project results;
- the dissemination of the project results in a final workshop, inviting interested stakeholders.

1.3 Main scientific and technological results

This section summarizes the most important scientific and technological results achieved along the project. These are explained in a simple fashion and, as far as possible, in a non-technical language.

1.3.1 Results of the initial desk analysis

The first part of the project, from T0 to M4, was dedicated to an initial desk analysis. The WP2 established a common baseline on current SRSs depending on positioning data originating from GNSS or similar navigational tools. This WP was divided in 4 different tasks to carry out a complete analysis from different perspectives (i.e.: technological, business and legal/regulatory). This section reports only the major results related to technological aspects.

1.3.1.1 Dependency of vessel monitoring systems on GNSS

The description of the state-of-the-art of SRSs reported in Section 3 of [AD. 3] demonstrates that many of them depend on positioning data originated from GNSS. Among all SRSs, the AIS is a fundamental piece of equipment for vessel traffic control through VHF data channels. AIS is a very common piece of equipment. According to IMO SOLAS (International Convention for the Safety of Life at Sea) (Chapter V, Regulation 19), functional AIS equipment is mandatory on all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and all passenger ships irrespective of size. This requirement became effective for all ships by 31 December 2004.

AIS stations use an internal GNSS receiver to estimate the vessel positions and have a reliable time reference for synchronization purposes. AIS also accepts GNSS data from external devices. Figure 3 1 shows the AIS 300, manufactured by Kongsberg, that has been selected as a key component of the prototype developed in the rest of the project.

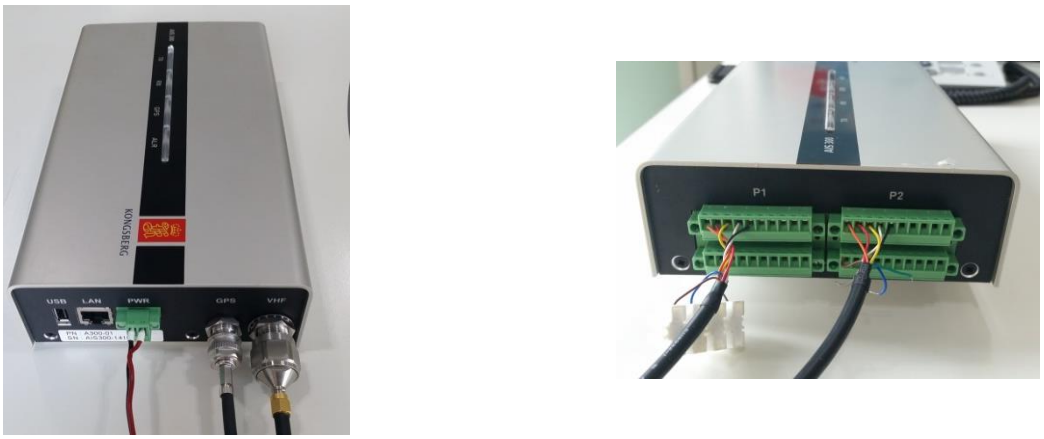


Figure 4: AIS 300 mobile station included in the TRITON prototype

Result of the analysis: Many commercial AISs, like that reported below, embed single frequency (i.e. 1575.42 MHz), mass-market GNSS receivers, generally employed in consumer grade devices. This type of GNSS receivers do not have any barriers against intentional interfering attacks on legacy signals.

1.3.1.2 Vulnerabilities due to intentional interfering signals

GNSS receivers used in maritime transportation are vulnerable to different type of intentional interference. The classified Annex of [AD. 3] reports a detailed overview of possible attacks to GNSS receivers, ranging from jamming (i.e.: RF signals blockage, by deliberately emitting electromagnetic radiation to disrupt the receiver, through the reduction of the signal to noise level) to more sophisticated spoofing. This last refers to the transmission of false GNSS-like signals, with the intent to fool the receiver and produce false information).

The problem of intentional interfering signals against GNSS-based devices is an actual issue, as demonstrated in the classified Annex of [AD. 3] by the high number of references (i.e.: scientific papers, news, web links, etc.), showing the disruptive effect of interference in marine applications. It is worth of mentioning that a high number of articles and scientific publications on this topic were noticed even after the end of the desk analysis, and demonstrated once again that the research community is seriously considering the problem of cyber security. For sake of completeness, we report three different quotes of distinguished experts, that explain well why the problem of interfering signal is an actual concern.

- Authors of [AD. 4] reported that ***'Although GPS jamming incidents are relatively rare they can occur; and, when they do, their impact can be severe'***.

- On February 13, 2014, the *Financial Times,* published an interview to Professor Bradford Parkinson [AD. 5], focused on the security of GPS: *[…"We have to make the GPS system more robust…our cellphone towers are timed with GPS. If they lose that time, they lose sync and pretty soon they don't operate. Our power grid is synchronized with GPS [and] our banking system']*.

- [AD. 5] is concluded with a reference to the maritime sector, reporting a sentence of Professor David Last, a consultant to the UK's General Lighthouse Authority: ***[…"When a ship loses GPS, it isn't like a car satnav. Multiple systems fail simultaneously"]***. Examples of systems on board of vessels that fail due to a GPS outage are: the AIS station, the ship's gyro calibration system, the Electronic Chart Display & Information Systems (ECDIS).

The desk analysis on the vulnerabilities of SRSs, considering a list of known threats was carried out taking into account the level of feasibility (intended as the complexity required to accomplish the attack) and the residual risk left by countermeasures already in use or envisaged.

Result of the analysis: according to the analysis reported in the classified Annex of [AD. 3], the team concluded that jamming is currently the most dangerous attack, because it can be easily accomplished with (illegal) low cost devices available for purchasing on the web. Although it is detectable, it is hard to mitigate. Only back-up terrestrial technologies (i.e.: e-Loran) or sophisticated countermeasures, and still expensive, (i.e.: antenna arrays) can tackle jammers. Meaconing is potentially harmful, since it is the simplest form of attack (i.e.: reception, delay, and rebroadcast of radio-navigation signals), but can be detected and mitigated with appropriated methods. Spoofing seems not yet common and understood by most, even if some real attacks have been reported. These have been carried out by fraudulent fishermen to cheat monitoring systems. Spoofing is a growing concern, that can be detected and mitigated using methods not yet state of the art. More

sophisticated spoofing attacks (e.g.: those involving high gain antenna) are considered unlikely, at least for civilian applications, even if they can be severe and difficult to detect.

The WP2 also investigated the vulnerabilities of the AIS-bases communication segment. The analysis confirmed that the data used to track maritime activity worldwide is increasingly being manipulated in order to disguise a ship's identity, location or destination port. Vessels tracking, using AISs, is becoming subject to fraud, manipulation and spoofing, with severe implications for global trade and maritime security.

Result of the analysis: according to the analysis reported in the classified Annex of [AD. 3], the team concluded that jamming against AIS, S-AIS, VPCS and LMR is a highly feasible threat that can completely destroy communications. It is possible to detect it and some mitigation measures are feasible. All the forms of spoofing of AIS/S-AIS (with the exception of the unintentional form) are potentially harmful, because they are already accomplished at present, using low-cost equipment.

1.3.2 From users' needs to new solutions

Part of the WP2 served to collect users' requirements through dedicated interviews to selected stakeholders and experts. Such requirements, along with the results of the investigation on the cyber threats, were the inputs of the WP3 "Robust Ship Reporting System Specification". Such a WP3 acted as the bridge between the desk analysis and the development phase of the TRITON prototype. The methodology followed in WP3 has been detailed in [AD. 6][AD. 7] and is sketched below.

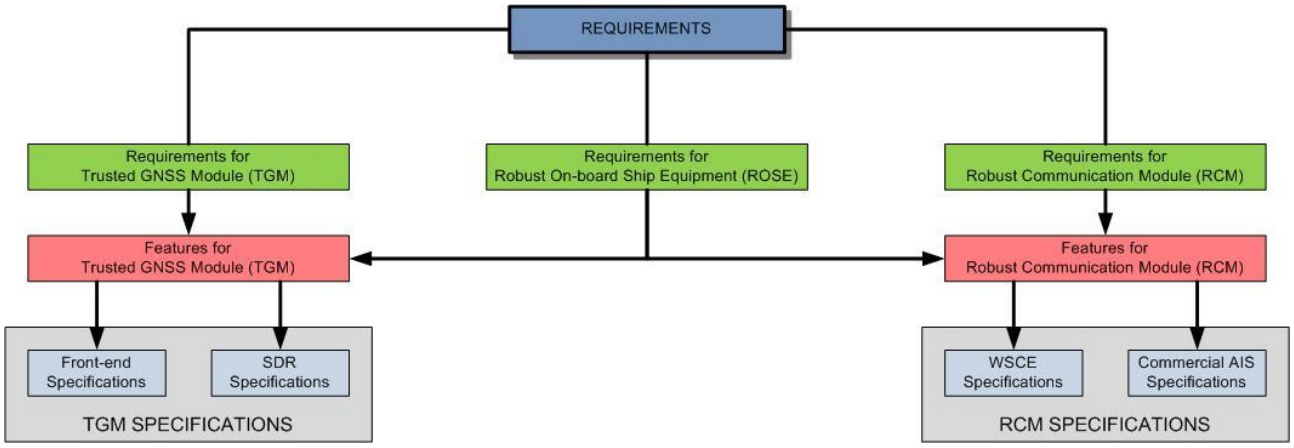


Figure 5: High level diagram of the methodology used to convert users' requirements into specifications

Such a methodology can be summarized in two main consecutive steps:

- The user requirements were critically reviewed, filtered and associated to the Trusted GNSS Module (TGM) or to the Robust Communication Module (RCM) – Task 3.1;
- The requirements were translated in specifications – Task 3.2.

Result of the analysis: at the end of the WP3, a set of clear and concise specifications was available either for the TGM and the RCM. Such specifications drove the design of the two prototypes.

1.3.3 Development of the TRITON prototype

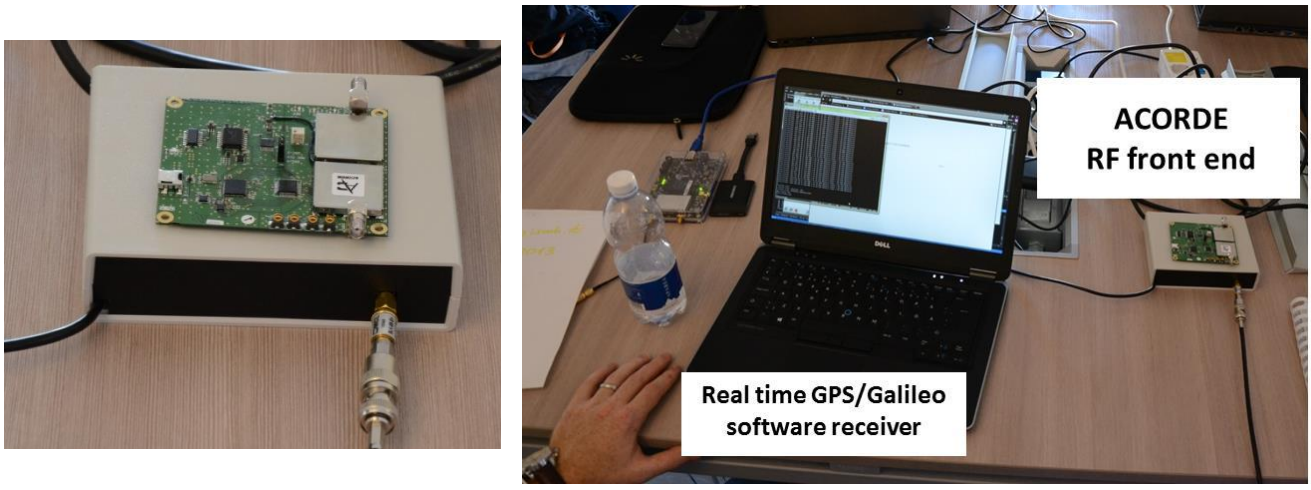
The prototype developed in TRITON was composed by two components:

- The Trusted GNSS Module (TGM), featuring mitigation algorithms against intentional interference;
- The Robust Communication Module (RCM), featuring a secure UHF channel in addition to conventional AIS links.

The TGM was developed in the WP4, whereas the RCM was developed in the WP5. Both the WPs run in parallel for 12 months. In addition, the WP6 was dedicated to functional lab tests, prototype integration, software tuning, and test campaign at JRC.

1.3.3.1 The Trusted GNSS Module

The algorithms implemented in the TGM were selected after a careful analysis of those introduced and explained in the scientific literature, considering their performance (in terms of an increased robustness and more accurate measurements in the presence of interference) and complexity. The TGM was developed in software radio technology, that allowed for the full design and implementation in a short period of time. In addition, the software radio development (i.e.: the receiver consists of software routines running on Personal Computer) introduced the level of flexibility required by the performance assessment of innovative algorithms. For instance, the receiver was tested under different configurations with a variety of possible settings to enable (disable) algorithms. The TGM, showed in Figure 6, was used as source of PNT data to the RCM.



(a) **(b)**

Figure 6: RF front end naked board (a) and TGM composed by the RF front end the real time GPS/Galileo software receiver running on a PC (b)

Result of the development: looking at the results of some lab tests during the WP4, we can conclude that the monitoring of the Automatic Gain Control (AGC) level, coupled with the observation of the signal statistics, is a valid method to detect unexpected signal power increments. Simulations and lab tests confirmed that the algorithm considered in TRITON outperforms conventional methods, because it is able to detect also the presence of weak interfering signals.
Some types of spoofing attacks induce a distortion of the received signal. This can be detected by monitoring the output of the correlation banks, with a negligible increment of receiver complexity.

The results stressed the importance to have an aggregated test at the receiver logic. Such test takes as input the results of all monitoring algorithms implemented along the receiving chain and provides a single measurement on the level of trust of the estimated position and timing data.

The level of trust (i.e.: warning in case of detection of interference) is an important piece of data generated by the TGM, that on board of vessels should be sent to other devices slaved to the GNSS receiver. A possibility is to dedicated one (or more) field of a specific message of the NMEA protocol. Currently, GNSS receivers lack in providing a measure of the level of trust of their estimates and no messages of the NMEA consider this option.

1.3.3.2 The Robust Communication Module

The RCM featured a secondary channel, that enhanced conventional AIS communication, with respect to security-related issues and to the limited bandwidth. The most suitable technology, proposed as a candidate for the secondary channel, was selected after a preliminary analysis, taking into account the maritime environment, and comparing different systems on two main points: achievable data rate and maximum coverage area. Note that in parallel to integration and testing of the RCM prototype, an intense simulation campaign was performed to investigate some aspects related to the Cooperative Vessel Positioning concept (techniques for recovering position in absence of GNSS availability exploiting the WSC layer) and to the optimal allocation for time-slotted transmission protocols.

The RCM showed in Figure 7 was developed integrating two main components: a commercial AIS Class A module (AIS 300 produced by Kongsberg) and a White Space Communication (WSC) module, that is an embedded PC with wireless transmission capabilities on the 700 MHz TV White Space (TVWS) band.

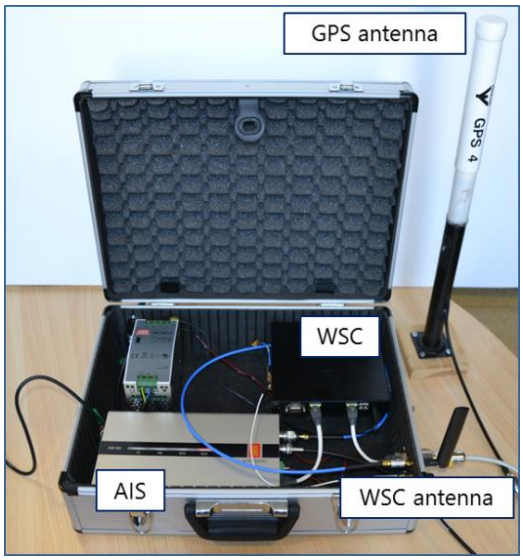


Figure 7: the RCM prototype

Result of the development: from a technical perspective, the 700 MHz TVWS band demonstrated to be suitable for maritime communication to enhance current links.
In addition, the WSC was able to accept data coming from the AIS forward them through the high bandwidth wireless, encrypted channel. This implemented a backup communication segment, where

transmitting stations could be authenticated. The integration has been carried out by means of standard interfaces, without modifying the existing, standard devices.
The activities performed in WP5 were invaluable to assess that the presence of a dual-frequency system, by design, strengthened the RCM against jamming on a single frequency. In addition, the WSC wireless link has plenty of bandwidth, that can be exploited for enabling multimedia services related to security (i.e. emergency calls among vessels). The simulations of CVP showed promising results, with a positioning accuracy less than 10 m for radars and of 15 m for some of the Time of Flight (ToF) techniques.

The complete prototype was successfully integrated and validated at the ISMB lab, during the Integration Readiness Review (IRR).

Figure 8: TRITON team working during the IRR meeting

1.3.4 Test campaign at the JRC and off-line analysis

In order to effectively validate the advantages of the TRITON prototypes in terms of security and reliability with respect to the state-of-the-art devices, a dedicated test campaign has been performed either on the TGM and the RCM. Some of the tests were conducted in the anechoic room of the Joint Research Centre (JRC), in Ispra (Italy), while others at the ISMB laboratories. During the tests, both the prototypes were stressed with intentional interfering signals to prove their enhanced performance with respect to commercial devices.

The results of the tests are included in the classified deliverable [AD. 14] and the main conclusions on the assessment of the two prototypes can be summarized as follows:

- **Conclusions on TGM attack detection technology.** The suite of attack detection tests included in the TGM allowed for robust detection of all attack types tested during the test campaign. In fact, the combination of several tests (e.g., Goodness of Fit, Ratio Test, PVT tests, AGC monitoring) was able to successfully detect, mitigate (when possible) and prevent large position errors in all of the attack scenarios considered in this project, which included jamming, spoofing and meaconing

- **Conclusions on RCM assessment.** The tests performed on the RCM underlined its main features and its key role in enforcing maritime communication security. Both device functionalities and new features have been tested. Specific tests have been set up in order to evaluate the performance in different scenarios. All in all, the main features of the WSC layer have been assessed, as well as possible enhancements enabled by this secure broadband link. Among those, message authentication, QoS management on the wireless link and VoIP emergency call availability are interesting features from the maritime security point of view.

1.3.5 Scientific and technological results versus initial objectives

The following table assesses the results of TRITON versus the original objectives defined in the Description of Work (see pages 16-17 of [AD. 8]).

Scope and objective of the topic	Compliance	How TRITON addresses the specific topic	**Results achieved**
Ship reporting systems (mainly LRIT, VMS and AIS) are today the backbone of maritime surveillance, control, safety and security. However their contents can be faked (spoofed) by malevolent operators.	✓	TRITON will analyse the current reporting systems in order to recognize their weaknesses and to identify means to increase their robustness. TRITON dedicates the WP200 to such analysis.	During the Task 2.3 "Security Threats of Ship Reporting Systems", the team deeply reviewed the scientific literature. The classified Annex to D2.1 contains 50 very recent references, reporting on the topic of SRSs vulnerabilities.
Research is needed into techniques to verify the sources of these messages [the messages provided by ship reporting systems (LRIT, VMS and AIS)]	✓	TRITON proposes a concept of trustable information transmitted from a trustable on-board equipment: • The position, velocity and timing information provided by the on-board GNSS receiver can be trusted, because the GNSS equipment features jamming detectors and spoofing countermeasures; • The reported information received from the radio link can be trusted, because the transmission protocol is made more robust; • The reported information from a ship can be checked through algorithms based on cooperative positioning, intrinsically robust against single malevolent operators.	TRITON developed, tested and demonstrated a nav/com prototype, enhancing the reliability of current devices: • Some of the tests performed at JRC showed that when the TGM is the positioning data source for the AIS, it outputs correct data, even during an interference attack. When the AIS uses its internal receiver, it is vulnerable; • Some of the test performed at JRC showed that the additional channel over the WSC band introduces redundancy and guarantees data authentication; • Simulations performed in WP5 have shown that in case of GNSS outages, cooperative approaches using communication signals can provide a valid alternative for positioning.

This should also take into account the use of ship navigation radar for ship detection and tracking.	✓	The focus of TRITON is on the trustworthiness of the on-board equipment, being a fundamental part of the overall architecture of vessel monitoring systems. For this reason, on-board radar equipments may be one of the sources of information to be exploited in a cooperative vessel positioning approach.	The results of the simulation of cooperative vessel positioning have been detailed in D6.2. For cooperative approached, both Time of Flight and radar based methods can ensure a good position accuracy. Among the ToF-based methods, the iterative Least-square method is preferable and it achieves very close results to the radar-based method, whereas the ARPA radar-based method is the most performant since it combines range and bearing measurements.
The authorities in the EU [etc.] need to be ahead of this potential security hole by evolving counter-spoofing methods.[etc.]. Counter-measures should be developed at EU (and global) scale.	✓	Counter-spoofing methods are elaborated in the TRITON project at two levels: 1) inside the GNSS equipment, so as to make its information still trustable at face value, without the concern of a misleading information caused by a spoofer. This is an action impacting most on the equipment manufacturers. 2) at the transmission level, by exploiting the possibilities offered by an additional redundant channel in the AIS transmissions. This is an action impacting on a global scale, as it has consequences on the spectrum management and is related to recommendations.	The deliverable D7.1 “Conclusions and Recommendations” summarizes the most important results achieved during the project, that are explained in a simple fashion and, as far as possible, in a non-technical language. The section 4 of D7.1 reports a set of clear and concise recommendation from a technical perspective, touching GNSS and communication aspects.

The project would anticipate the need to further verify (double-check) ship reporting systems.	✓	The two main focuses of this project (GNSS equipment and communication transceiver) work together toward the goal of providing a trustable ship information to the monitoring systems. This way, the stringent necessity to resort to "literally" double checking the reported information can be partially relaxed. On the other hand, the concept of cooperative vessel positioning can be seen as an additional method for double checking stand-alone ship information.	In a nutshell, redundancy and frequency diversity are simple, but effective, means to tackle interfering signals. This was demonstrated and stressed either for the GNSS and the communication part. See the technical recommendations on: • GNSS multi-constellation; • GNSS dual frequency; • AIS communication.
It should analyze possible different approaches and identify the most appropriate ones.	✓	Identify requirements and specifications applicable to the development of GNSS and communication modules. Several possibilities to realize the trustable on-board equipment will be explored, for both the anti-spoofing GNSS equipment and the robust communication module.	The project dedicated a specific WP (i.e.: WP3 Robust Ship Reporting System Specification) to the translation of users' needs to technical specifications. These were the input for the design of the TGM and RCM. Thanks to the software radio approach, the prototype offered a high level of flexibility and a number of settings and comparisons were possible during the tests and the off-line analysis.

The results of this project are expected to close a gap in the security of maritime domain.	✓	The final goal of the TRITON project can be described as: • To harden the ship-board GNSS module in terms of robustness against spoofing attacks (achieving then a "trusted" source of position/timing information for ship-board unit of reporting systems) and ability to detect interfering signals (i.e.: intentional jamming and unintentional interference). • To propose means to ensure/increase data integrity sent from vessels • To globally increase the counter-spoofing capability and then the trustworthiness of the on-board segment of vessel monitoring systems, thus "contributing to close a gap in the security of the maritime domain".	Looking at the main scientific and technological results, we concluded that • Intentional interfering signals are a growing security concern, but it is certainly possible to detect and mitigate them, with reasonably low probability of false alarms; • Sophisticated algorithms at signal processing level can be combined with simple cross checks to enhance reliability • More trusted and authentic data means more security for maritime transportation. Technical results need to be addressed to specific working groups focusing on cyber security and countermeasure.

1.4 The potential impact

This section summarises TRITON potential impact, presenting main socio and economic benefits, and main dissemination activities already described in [AD. 9] and in [AD. 10].

1.4.1 TRITON contribution to the maritime domain

The maritime domain provides a broad pathway for a wide spectrum of **illegal operations** (affecting maritime security) and **accidents** (impacting on maritime safety). A preliminary estimation of worldwide/ European impacts from illicit activities and ship accidents are presented below (for details and sources see [AD. 9])

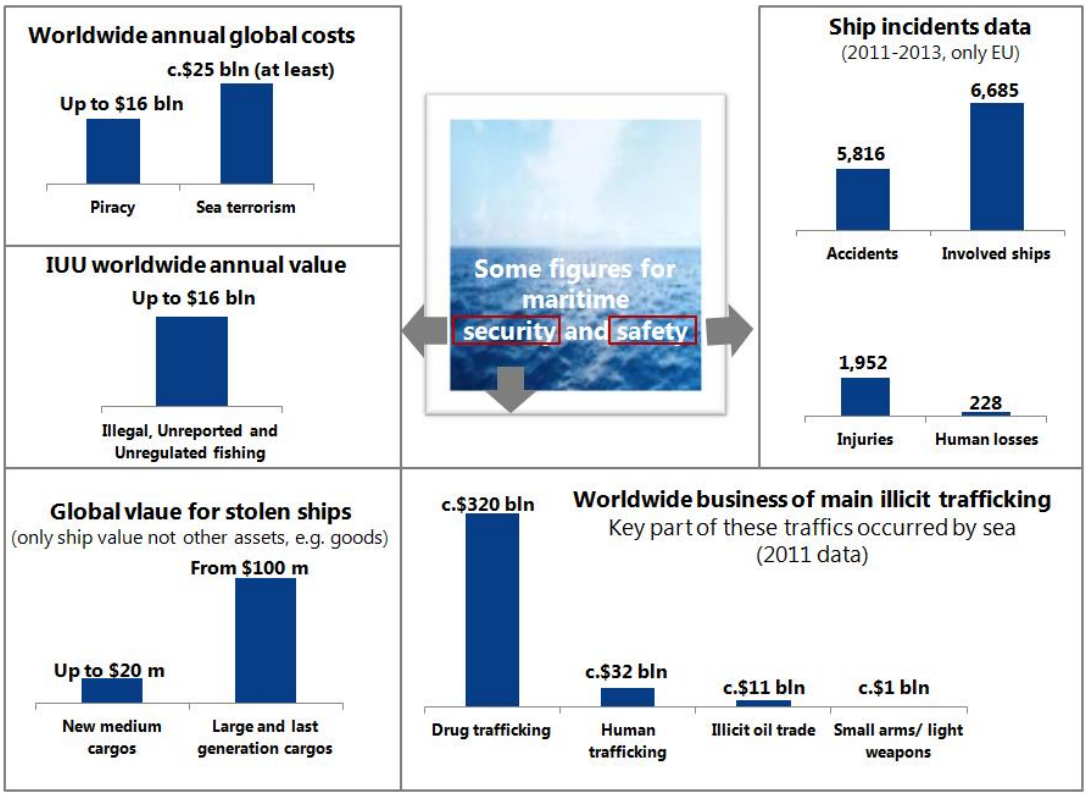


Figure 9: Maritime security and safety: some facts and figures

As it can be noted, costs due to illegal operations and accidents each year are extremely high and are caused by a handful of events (such as in case of piracy or terrorist attacks). Therefore, even a single attack produces very high costs to various stakeholders, if we consider e.g.:

- **Ship/ fleet owners** that could be subjected among others to higher insurance premia, costs for ransoms, extra fuel measured in tons per day required to divert around affected areas, costs for deterrent equipment and personnel;
- **Public authorities/ administrations** that should face these activities through dedicated operations and naval forces; and
- **Society** that pays in terms of security and safety e.g. for passengers, higher price for final products/ goods transported, potential trade and price inflation, decrease in potential jobs (e.g. for legal fishermen) and available sea resources. This impact could, in turn, increase poverty and exacerbate conflicts.

Speaking about illegal operations, nowadays, they are perpetrated through even more sophisticated technologies than in the past. This could mean an overall increase in potentiality and severity of these actions in the future. Considering the high impact of each event, this increase could represent a primary risk in this domain. Experts, such as Dee Ann Divis in [AD. 11] and several newspapers (e.g. Financial Times, see also [AD. 12]) pointed out that **cyber security** is emerging as the hidden threat to shipping. Today, technologies, e.g. portable jammer, can be used easily for illegal activities, or like in the case of Chinese vessels, they count for 44% of worldwide GPS manipulation to allow them for illegal fishing.

This kind of **GPS interference** was analysed in the TRITON project. Together with them, **ship-to-ship and ship-to-shore communication** was also a key topic, considering its relevance to better face security issues. Moreover, failing communication networks could cause various types of accidents and endanger emergency response. In this context, the project has to be considered as a contribution to a more programmatic, wide and structured answer for some of main cyber security threats affecting this domain. In line with that, the developed solutions (i.e. the two embedded modules, the TGM and RCM) should not be intended as stand-alone technologies resolving the problems faced during the project, but as a part of on-board equipments enhanced by them. In particular, TRITON aims at improving current on-board **Automatic Identification System transceivers** (AISs). For this reason the related market should be considered as the key one.

At the same time, TRITON marketable components (i.e. *AIS TRITON*$^{++}$ full optional or in one of its options – the TGM or RCM one – and TRITON intended as a *test platform*) could offer **unique potentialities and features in the AIS market**. Actually, according to our analyses, no comparable solution has been registered. Some projects on similar topics have been identified; however no commercial solution is commercially available or present in the market. Other technologies are used for similar purposes, such as radars or SatCom. Nevertheless, these systems are less common in the maritime domain than AISs. Moreover, they have higher costs to reach only few of the potentialities proposed by the two developed modules.

Thanks to its unique features, TRITON is expected to bring different types of benefits, in some way reflecting the major costs currently sustained by the maritime domain due to illegal activities and safety concerns. These benefits could be reached leveraging TRITON modules, together with (and not in place of) other technologies already adopted. In fact, a comprehensive approach is required to effectively face the analysed challenges. As a part of this approach, TRITON could impact the key maritime dimensions, bringing:

- A contribution to **enhance maritime security**, mainly anticipating a key future issue, i.e. potential cyber attacks;
- Even if to a smaller extent, a support to **improve safety**, through a better management of accidents/ collisions and a reduction of them; and
- **Other** potential **benefits**.

1.4.1.1 TRTION impact on maritime security

TRITON contribution to maritime security enhancement is reflected in the support provided by the solution components for the reduction of **occurrence** and/ or the **impact** of main **illegal operations**, when linked to cyber techniques (in particular to jamming and spoofing perpetuated by third-parties). Moreover, some recent events (see also [AD. 12]) stress the importance of having a

trustworthy positioning data for maritime security. This was, to some extent, one of the TRITON objectives.

Reducing the potentiality and the severity of illegal operations implies a decrease of the **overall costs** supported by **the economies** affected by them, with far-reaching **worldwide benefits expected**. Such benefits are split among different users and stakeholders, providing an overall socio-economic impact in terms of security aspects, as briefly summarised in the "impact table" presented below.

Contribution to enhance maritime security		
Type of impact	User and/or stakeholder	Benefits, intended as a contribution to reduce:
Private-economic impact	Private fleet owners	• Insurance premia • Costs for stolen and/or damaged ships • Costs for potential ransoms • Other direct or indirect costs
Public-economic impact	Authorities/ administrations	• Costs for operations aimed at detecting, mitigating or hindering cyber attacks • Costs of naval forces
Socio-economic impact	Society as a whole	• Sea security risks (e.g. for passengers), • Price for final products/ goods (lower costs would allow lower prices), • Costs to regional economies (e.g. trade and price inflation, illegal fishing and related jobs, resource availability…) • Related country's poverty or conflicts • Environmental damages and pollution.

Table 1: Impact on maritime security

1.4.1.2 TRTION impact on maritime safety

Even if to a smaller extent (the project was primarily focused on security issues), TRITON components could be leveraged also in terms of safety improvements.
Thanks to more reliable, accurate and robust information (e.g. PND data), the possibility of leveraging a dual-frequency communication channel, and a corporative positioning, an increase in maritime safety in case of AIS TRITON^{++} adoption can be foreseen.
Here, apart from **a better management of accidents/ collisions** and a **reduction of them**, additional **communication services** and **aids-to-navigation** brought by the RCM could be expected, mainly by crew. The safety "impact table" shows the main benefits by impacted users and/ or stakeholders.

A support to improve safety		
Type of impact	User and/ or stakeholder	Benefits, intended as a contribution to allow:
Socio-economic impact	Main private and public maritime end-users and	• A reduction of number and/or severity of accidents and collisions

A support to improve safety		
	society	• An increase of accuracy on forecast-calculations made by the onshore and onboard systems when it comes to e.g. congestion prediction
	Crew	• VoIP emergency calls • Port video surveillance • Cooperative positioning
	Search and Rescue (SAR) operators	• Improvement of operations

Table 2: Impact on maritime safety

1.4.1.3 Other potential impacts

In addition to those listed before, some other benefits could be brought by the system exploitation. The **scope of cyber attacks** in future is expected to be even wider than that designed in this analysis. Though criminals will actively use these systems for illicit activities; it is also likely that governments, which have already used them, will continue to do that. As a potential consequence, countries seeking to establish strong cyber warfare capabilities are more and more likely to utilize jamming or spoofing for gaining considerable advantage in all of the main domains - not just within the maritime one. This capability could have several societal implications.

Finally, looking at TRITON as a test platform, TRITON could be used as a test tool for other receivers or systems, monitoring and verifying in this way their robustness towards cyber attacks. For this reason, TRITON could contribute to **testing activities** and the definition of **minimum performance requirements** for maritime navigation.

1.4.1.4 Conclusions and fields of actions

The overall analysis of potential impacts brought by the TRITON solution allows some first conclusions. Costs supported by countries and economies for illegal operations and accidents are so important, that also a **small contribution** to their reduction could mean **significant savings.** This was demonstrated also during a simulated Costs Benefits Analysis (CBA) on security aspects. Assuming a minimum reduction of only three illegal activities (i.e. one piracy attack, a 0.1% of illegal fishing and one ship theft, all in one year), an annual saving of c. **€51 m** could be reached thanks to TRITON adoption. This potential impact could be achieved bearing only the marginal costs required to adopt the solution. At the same time, this saving could be translated into a financial benefit for ship owners and public authorities, with wider societal implications and effects (not considered in this preliminary estimation): affected countries and areas could reduce the weight that these illegal activities exercise on their economies and citizens.

Speaking of impact, it has to be mentioned that **benefits** are not only for system end-users and society as a whole, but also **for system providers**. In our Business Plan simulation, we considered an example of a small provider, part of the TRITON consortium, as part of an illustrative and possible business model. According to our results, the provider market share could grow up to ten times (from actual percentages) in the timeframe considered (ten years, from 2018 to 2028), becoming an

important player in the market. Related financial figures reveal a small but relevant growth for a player currently selling c.50/ 100 new AISs each year.

The project pointed out that there is a strong attention on the topics promoted, at least from a research point of view. It was confirmed by recent newspaper headlines, as mentioned before (see also [AD. 11] and [AD. 12]). However, several **difficulties** have been encountered **to exploit the solution potential** from a commercial point of view. As of today, despite this interest, a commercial will of system providers and end-users seems not yet mature.

To foster this commercial interest, allowing reaping the benefits of an increased maritime security and safety, some actions seem necessary. In fact, only after these actions have been undertaken, a real improvement in technology used by end users can be expected. These actions can be grouped into different "fields of action", i.e.:

- **Promotion of a specific regulation.** This is a fundamental driver in maritime domain for further technology improvement. Moreover, when it comes to cyber security regulations for the maritime community, several gaps seem to exist. A review and alignment of regulation could positively impact the overall domain, also from a commercial perspective. Specific tasks and activities during this project have been dedicated to this topic and a deliverable prepared. In particular, [AD. 13] was intended as a reference for the work of authorities and agencies regulating marine traffic and application;
- **Demonstration of financial benefits.** In this sense a project CBA and BP have been undertaken from a general and worldwide perspective. They tried to assess on one hand the potential project impact on end-users and society and, on the other, financial benefits for a potential solution provider. Moreover, considering the relevance of financial benefits in the adoption of new technologies, in our opinion it could be interesting to deepen the link between the adoption of an AIS TRITON^{++} (one module or full optional) or the use of TRITON test platform and some of the main costs sustained by end-users. In particular, the relation between more robust technologies and insurance premia presents a certain commercial potential and it should be analysed at a more mature stage of the technology development. If the developed components could contribute to a reduction of insurance premia and how they could contribute is an interesting topic (something similar has been studied in the road domain, where cars using GPS tracking where guaranteed lower premia, especially in countries with high theft ratios, like South Africa). These kinds of savings could revive the commercial interest of sheep owners (both public and private) towards the solutions due to the relevance of these costs; and
- **Promotion of awareness on cyber security.** Cyber security awareness in the maritime sector has been registered at a relatively low level. According to the first EU report on this challenge published by the European Network and Information Security Agency (ENISA) in 2011, cyber threats have grown steadily in the maritime sector, while **awareness** on them in the domain remained relatively **low**. In Germany and Norway, only recently, concerns start coming out from the authorities and the potential risk of cyber attacks is now recognised by the maritime industry. We assess that there **is a medium level of awareness on cyber attacks** among key actors in these countries, but it is mainly in terms of general considerations regarding future trends (more than current adoption of related systems). In fact, these topics are not considered as priorities or perceived as concrete risks at the moment. Therefore, TRITON dissemination and promotion activities were intended as a

mean to enhance the overall awareness on threats faced during the whole project, as better described in the paragraph below.

1.4.2 TRITON dissemination, communication and exploitations

The figure below summarises the overall TRITON "promotion system" among main target groups, as defined in [AD. 10].

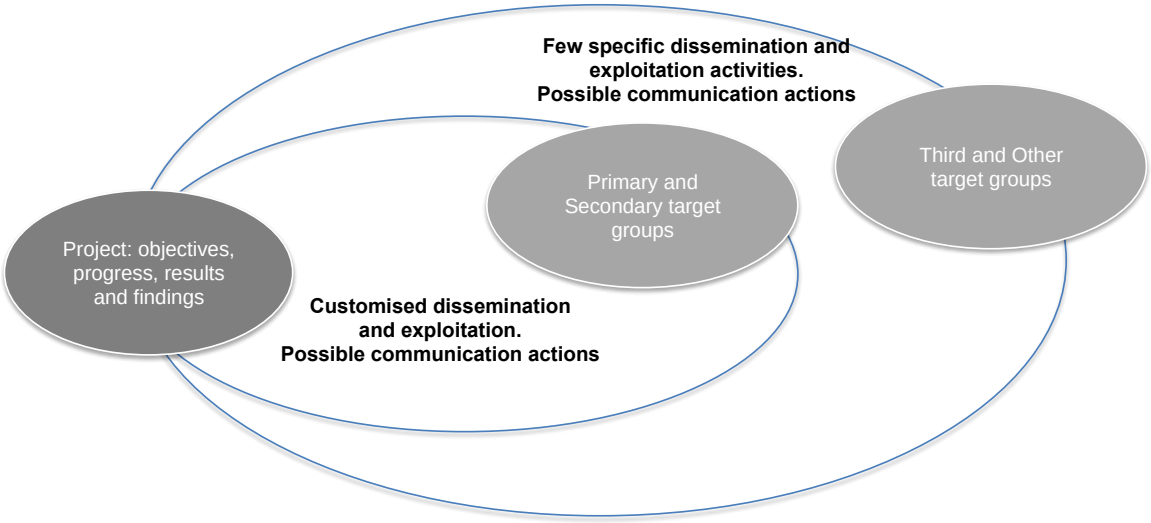


Figure 10: TRITON "promotion system"

During the project three different types of promotion activities have been undertaken:

- **Dissemination actions**. They were thought mainly for primary (i.e. end-users) and secondary target groups (e.g. regulators, experts, main maritime associations…) considering their impacts on core project issues and relevant direct and indirect benefits they could receive;
- **Exploitation actions**. Also in this case, primary and secondary target groups were considered key actors; and
- **Communication actions**. The majority of users were professionals and security was a concern. Therefore, specific dissemination and exploitation actions, more than a communication strategy for a wide audience, were identified as the most appropriate means since the beginning of the project.

Dissemination, exploitation, and communication were strictly connected and, in some cases, the same channels/ measures (e.g. website) have been used to undertake the activities, even if with a high level of customization (dedicated website sections) in relation to target audience and objectives.

Dissemination, exploitation, and communication activities have been undertaken both at consortium and partners' level, as a part of an overall strategy composed by four types of actions in relation to their objectives. In this context, first of all an **improvement of awareness** concerning the main maritime security threats has been considered as a key point. In line with that, promotion activities mainly aimed at overcoming this gap. At end of the project, this assumption on which we built our promotion strategy was confirmed also by the "Business and Exploitation" analyses.

The table below summarises the **promotion actions undertaken**, presented by type of action, their objectives and a brief description. Moreover, possible actions identified at the beginning of the project vs those concretely undertaken are reported. Section 1.4 reports further details on main actions (e.g. description of the events and submitted papers).

Type of action	Objective and Description	Activities foreseen in the TRITON proposal	Status of the action at the end of the project
Dissemination actions for awareness (most relevant activities for TRITON project)	**Objective**: set of activities aimed at improving awareness mainly among users on project topics and related technologies. **Description**: the majority of these actions start immediately after preliminary project results and after the conclusion of first WPs. It is strictly connected with project outcomes.	*Logo*	✓
		Website	✓ Website prepared and **regularly updated**
		Project leaflet/ brochure	✓ **3 brochures** and **2 posters**
		Articles and papers	✓ **4 papers** and **1 project advertorial**
		International conferences and events	✓ Participation to **7 events**
Dissemination for user and stakeholder involvement	**Objective**: engagement and involvement of relevant users and stakeholders in different phases of the project in relation to different objectives and activities. **Description**: this type of action starts early in the project and could last sometimes the project timeframe. It is strictly connected with specific WP and/or Task objectives (e.g. identification of user needs)	*Contact database*	✓ **2** different **databases** prepared and regularly updated
		Set of interviews for identification of user needs	✓ **2** set of interviews
		Other potential actions for user and stakeholder involvement, if necessary and possible	✓ A dedicated **final WS** organised
Exploitation	**Objective**: activities aimed at the market uptake of proposed solution **Description**: this type of action is linked to the last part of project activities aimed at commercial exploitation of results	*Project Business Plan*	✓
		Similar and new projects monitoring and interface	✓
		Interface with European Institutions	✓ **Event** participation and a dedicated **final WS** organised

Type of action	Objective and Description	Activities foreseen in the TRITON proposal	Status of the action at the end of the project
Communication	**Objective**: additional communication actions (with regard to dissemination activities) to communicate project results not only to the main stakeholders, end-users or scientific community (primary and secondary target groups) but also to the society at large (third and other target groups) **Description**: few potential communication actions (e.g. usage of specific web 2.0 social media) could be undertaken through the TRITON project, according to the security of the project	*Website*	✓ Website used also to inform community on main TRITON events
		Specific web 2.0 social media	✓ Even if only through project members' personnel accounts, Twitter was partially used
		Other communication tools	✓ *Ad hoc usage of a specific contact database for UW promotion*

Table 3: Overview of the dissemination, exploitation and communication types of actions

Concluding, a general and theoretical interest has been shown by different domain actors during the events where TRITON participated, through social media, when used, or with specific requests for more information related to the project. This interest confirms also the project findings coming from the business analysis.

1.4.3 Results achieved versus expected impacts

Expected impacts	Description	Results achieved
Increase the level of consciousness on the vulnerability of GNSS-based ship reporting systems	As GNSS is continuing to be modernized (i.e.: new constellations, signals and services) and adopted in critical infrastructures, few recognize that severe system failures can be caused by intentional interfering signals. The TRITON project will provide a detail analysis of jamming and spoofing threats for ship reporting systems, providing an assessment on the level of complexity associated to the attack and the corresponding risk. The work will provide clear recommendations for the improvement of real systems.	In [AD. 1], a detailed overview of possible attacks to GNSS receivers, ranging from jamming to more sophisticated spoofing, has been provided. The desk analysis on the vulnerabilities of SRSs was carried out taking into account the level of feasibility (intended as the complexity required to accomplish the attack) and the residual risk left by countermeasures already in use or envisaged. A dedicated deliverable ([AD. 13]) for conclusions and recommendations for the improvement of real systems have been provided.
Hardening GNSS module used by on-board unit	• By implementing jamming detection solutions (i.e.: the receiver will be able to recognized if it is being jammed or working in an interfered scenario, providing appropriate warning to the user) • By implementing spoofing mitigation solutions (i.e.: the receiver will be able to detect and mitigate some spoofing attacks) • By exploiting new methods for cooperative vessel positioning, exploiting technologies different from GNSS.	• Through the TGM, featuring mitigation algorithms against intentional interference • Through the RCM, featuring a secure UHF channel in addition to conventional AIS links and allowing cooperative vessel positioning
Improve the ability of the vessel's crew to react to GNSS failures, promptly reverting to traditional means of navigation	Some vessels have integrated systems that enable automatic execution of a passage plan on autopilot. If this system is operating when jamming occurs, the vessel's course and heading may change without informing the crew, potentially leading to hazardous consequences. The use of a "trusted" GNSS receiver (as that developed in TRITON project) able to detect jamming and rise warnings in case of temporary GNSS outages, helps crew to quickly react and take the most appropriated decision. In turn, this improves safety.	As described in paragraph 1.4.1, the two modules together effectively contribute to enhance security and improve safety. In particular, for crew: • The TGM can support the detection of GPS interferences, so consequent prompt reactions in these circumstances; and • The RCM allows a second communication channel in case of jamming or spoofing of the first one (dual frequency) an a set of additional communication services and aids-to-navigation

Enhancing ship-to-ship and ship-to-shore communications	By extend bandwidth or available communication channels as well as enhancing information integrity	Thanks to the RCM, TRITON allows the introduction of a secure communication module, by exploiting the "white spaces" freed by analogue TV and offering a broadband channel enabling several services and enhancements to the current system
Development of a robust system prototype on top of current systems	The prototype will be developed on top of equipment currently used on board of vessels. The test will demonstrated (and assess) how it is possible to improve the robustness of current systems, implementing low cost methods and alternative technologies.	Both the two modules have been developed on top of a standard AIS transceiver. In particular, Kongsberg Seatex AIS 300 has been included in the TRITON prototype. At the same time, current AIS market was considered in the business assessment. The WP6 was dedicated to lab tests and test campaign at JRC aimed at assessing the robustness of current systems, implementing low cost methods and alternative technologies.
Improvement of collaboration between industry partners and research institutes across Europe	By building up a scientific/technical team where industrial players, SMEs and research institutes (from different European countries and with different expertises) will work together for 2 years towards a common objective.	The Consortium know-how and network was strongly exploited thanks to this 2 years collaboration. The mix of scientific and commercial backgrounds was fundamental for the in-depth understanding of user needs, from a technical and business perspective. At the same time, the technical support has been a key driver for the overall commercial exploitation.
Contribute from a legal/regulation perspective	Together with the scientific analysis and the development of the robust system prototype, there will be the review of current EC policy and regulations. On the basis of the major outcome, the project will also provide recommendations from a regulatory perspective.	While [AD. 2] provides a wide a comprehensive overview on current regulation, [AD. 13], i.e. project conclusions and recommendations, were intended as a reference for the work of authorities and agencies regulating marine traffic and application.

1.5 Useful links and contacts

This section provides key contact details, presents some dissemination materials (i.e. logo and website) and provides useful links.

1.5.1 Project contact

Marco Pini – *Project Coordinator*
Head of the Navigation Technologies Research Area
Istituto Superiore Mario Boella (ISMB)
via P.C. Boggio 61, 10138 Torino (Italy)
e-mail: pini@ismb.it
office: +39 011 2276 436 | mobile: +39 335 6443351

1.5.2 TRITON logo and website

The **TRITON logo** aims at providing an immediate and visual indication of the forming blocks of the project: the maritime domain and the ship reporting systems. It is used in all materials produced within the project.

Figure 11: TRITON logo

The **TRITON website**, ***www.tritonproject.eu***, has been used as a key channel to disseminate the overall project and all relevant results achieved. It has been regularly updated during the whole project duration.

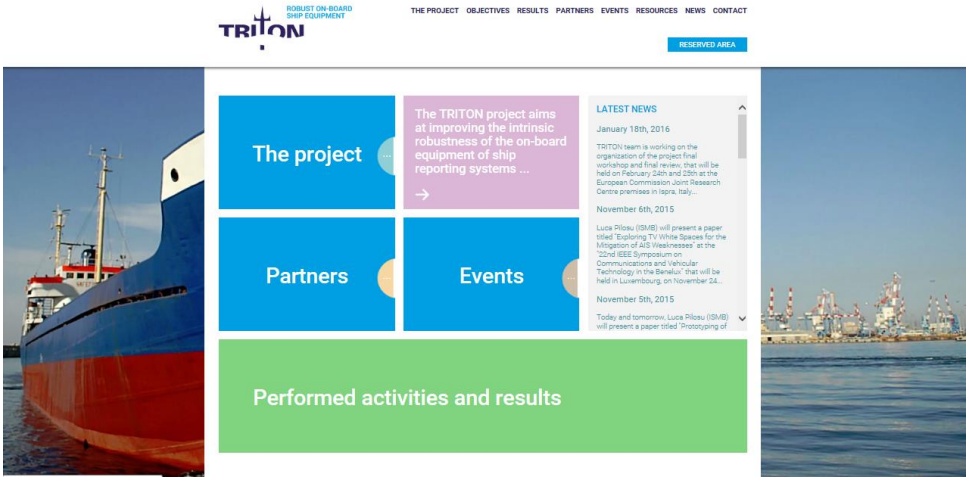


Figure 12: TRITON website

1.5.3 Useful links

http://tritonproject.eu/
http://ec.europa.eu/enterprise/index_en.htm
https://ec.europa.eu/jrc/
https://ec.europa.eu/jrc/en/institutes/ipsc

2 Use and dissemination of foreground

2.1 Dissemination events

Important dissemination activities (publications, conferences, workshops, etc.) have been performed during the two-years project.

Six months after the kick-off meeting, TRITON has been invited to participate in the framework of the 2014 "European Day for Border Guards" (ED4BG). The ED4BG 2014 took place in Warsaw (Poland) on May 22nd. This annual event is organized by FRONTEX, the EU agency for external border security which is responsible for co-ordinating the activities of the national border guards in ensuring the security of the EU's borders with non-member states. ED4BG presents Europe's border-guard community with an opportunity to share experiences and best practice. ISMB representative attended the event, presenting the TRITON project through an exhibition stand, among other 20 EU-funded border security research projects. Moreover, on May 23rd, TRITON has been presented in a dedicated workshop on the "Maritime surveillance" topic, joined by Member States representatives, experts on maritime surveillance, EU Commissions and FRONTEX Reserach & Developmet Unit.

At the end of the first year of the project, on December 9th to 11th, 2014, TRITON has been hosted by the EC stand at the "Global expo-conference on Community Protection 2014" in Genova. The "CPExpo 2014 is the event - organized by the Regione Ligura - as part of the Italian Presidency of the Council of the European Union. TRITON was one of the eight projects in the security field selected by the European Commission's Directorate General Enteprise (DG ENTR) to show at the European Security Research Conference (SRC) 2014 within the CPExpo 2014. ISMB and Alpha Consult representatives have had then the chance to illustrate the intended TRITON activities through a dedicated exhibition area in the EC stand as well as through two presentation sessions during the conference.

In June 2015 TRITON has been presented to the 2015 Loss Prevention Committee (LPC). The LPC was organised by the Norwegian Hull Club and took place in Bergen (Norway) from June 10th to June 11th, 2015. The purpose of the Committee is to share timely and relevant information related to loss prevention in order to improve safety for lives, environment and values in marine and offshore operations. In this context, Lene Vesterlund (from KNC) attended the meeting, presenting the main objectives and the prototypes of TRITON through a dedicated presentation.

The article "TRITON project advertorial" was published on The Parliament Magazine, a fortnightly EU Politics, Policy and People Magazine, on February 2015.
Furthermore, throughout the two years of project, scientific papers on the TRITON results have been presented at conferences and workshop.
All the details on the dissemination activities are summarized in table A2.

TEMPLATE A2: LIST OF DISSEMINATION ACTIVITIES								
NO.	Type of activities[3]	Main leader	Title	Date/Period	Place	Type of audience[4]	Size of audience	Countries addressed
1	*Presentation*	*Marco Pini*	*2014 European Day for Border Guards (ED4BG)*	*May 22-23, 2014*	*Warsaw, Poland*	*Policy makers, Scientific Community*		
2	*Conference*	*Marco Pini*	*10th International Symposium Information on Ships*	*September 4-5, 2014*	*Hamburg, Germany*	*Scientific Community*		
3	*Conference*	*Marco Pini*	*IEEE Joint Intelligence and Security Informatics Conference (JISIC)*	*September 24-26, 2014*	*the Hague, Netherlands*	*Scientific Community*		
4	*Presentation*	*Marco Pini*	*The global expo-conference on Community Protection 2014 (CPExpo 2014)*	*December 9-11, 2014*	*Genova, Italy*	*Scientific Community (higher education, Research), Industry, Civil*		

[3] A drop down list allows choosing the dissemination activity: publications, conferences, workshops, web, press releases, flyers, articles published in the popular press, videos, media briefings, presentations, exhibitions, thesis, interviews, films, TV clips, posters, Other.

[4] A drop down list allows choosing the type of public: Scientific Community (higher education, Research), Industry, Civil Society, Policy makers, Medias, Other ('multiple choices' is possible).

						Society, Policy makers		
5	*Press*	*Marco Pini*	*The Parliament Magazine*	*February 2015*		*Civil Society, Policy makers*		
6	*Presentation*	*Lene Vesterlund*	*2015 Loss Prevention Committee*	*June 10-11, 2015*	*Bergen,Norway*	*Industry, Civil Society*		
7	*Conference*	*Luca Pilosu*	*IEEE Advances in Wireless and Optical Communications - RTUWO 2015*	*November 5-6, 2015*	*Riga, Latvia*	*Scientific Community*		
8	*Conference*	*Luca Pilosu*	*22nd IEEE Symposium on Communications and Vehicular Technology in the Benelux - SCVT 2015*	*November 24, 2015*	*Luxembourg City, Luxembourg*	*Scientific Community*		

2.2 Section B (Confidential5 or public: confidential information to be marked clearly) Part B1

This section presents possible ways of exploitation of the project foreground. These have been discusses by partners in the last phase of the project (i.e.: during the preparation of the project workshop and the drafting of the last deliverables out of WP7), during and after the final review.

The following subsections discuss tangible foreground (i.e.: associated to the developed prototypes) and intangible foreground (i.e.: improved knowledge on the risk associated to interfering signals in maritime and possible countermeasures to enhance security).

2.2.1 Intangible foreground

- **Dissemination of a white paper to EU and international bodies (Public)**

One of the most important results of TRITON is indeed the increased awareness on the problem of intentional interference against electronic devices used in maritime navigation, and the possibility to enhance protection with new designs. The final project workshop was successful and involved several actors working the field of maritime security.
As agreed with the Project Officer, the team prepared a *white paper* to be disseminated to interested EU officers, some relevant international bodies and regulatory organizations (see the groups identified in D7.1)
Such a *white paper* comes along with presentation prepared at the end of the WP7 *"Critical Review of the scientific result"*, that was already delivered to the Project after the final review meeting. The presentation includes clear messages that can be used to disseminate the project results.

2.2.2 Tangible foreground

- **IP usage, including the possibility of patenting part of the prototype (Confidential)**

The Consortium Agreement signed at the beginning of the project already include a specific section to regulate the foreground. This section will be reviewed and updated on the basis of specific needs and requests of some of the partners, that intend to reuse the developed prototype for purposes different with respect to those identified in TRITON. The review of the Consortium Agreement will also consider the

[5] Note to be confused with the "EU CONFIDENTIAL" classification for some security research projects.

possibility of patenting some parts (e.g.: algorithms) of the prototype. In this case, the new version of the Consortium Agreement will regulate IP rights among partners.

- **Upcoming calls and funding opportunities to further enhance the solution (Confidential)**

Some partners are considering new EU funding opportunities to improve the Technology Readiness Level (TRL) of the prototype and achieve a product in a short/medium term. The *H2020 SME instrument calls* seem offering interesting opportunities and ACORDE demonstrated the interest to coordinate a new project proposal, leveraging on the TRITON results.

- **Evaluation of market opportunities in other domains (Public)**

One of the key results of the business analysis is that the current maritime market is not open to innovation, unless new products are supported by new standards and regulations. For the topic touched in TRITON, new regulation seems required to promote the adoption of interference mitigation strategies and back up communication links. Nevertheless, the Consortium identified other possible applications of the technological solutions studied and proposed in TRITON. Examples are:

    - Liability critical application in the road domain (e.g.: digital tachograph, road tolling, other segments)
    - Security critical applications based on Unmanned Air Vehicles (e.g.: land monitoring and patrol)
    - Safety critical application in road (e.g.: transportation of dangerous goods)

- **Provision of the solution to the EU or national agencies (Public)**

The Consortium agrees to have the developed prototype in use at some EU and/or national agencies, working in maritime security. The prototype could became a didactical tool to further enhance the awareness of the operators on the problem of intentional interference and demonstrate protections.

3 Report on societal implications

A General Information *(completed automatically when **Grant Agreement number** is entered.*

Grant Agreement Number:	312687
Title of Project:	Trusted Vessel Information from Trusted On-board Instrumentation
Name and Title of Coordinator:	Dr. Marco Pini

B Ethics

1. Did your project undergo an Ethics Review (and/or Screening)? * If Yes: have you described the progress of compliance with the relevant Ethics Review/Screening Requirements in the frame of the periodic/final project reports? Special Reminder: the progress of compliance with the Ethics Review/Screening Requirements should be described in the Period/Final Project Reports under the Section 3.2.2 *'Work Progress and Achievements'*	***No***
2. Please indicate whether your project involved any of the following issues (tick box) :	***YES***
RESEARCH ON HUMANS	
* Did the project involve children?	NO
* Did the project involve patients?	NO
* Did the project involve persons not able to give consent?	NO
* Did the project involve adult healthy volunteers?	NO
* Did the project involve Human genetic material?	NO
• Did the project involve Human biological samples?	NO
• Did the project involve Human data collection?	NO
RESEARCH ON HUMAN EMBRYO/FOETUS	
* Did the project involve Human Embryos?	NO
* Did the project involve Human Foetal Tissue / Cells?	NO
* Did the project involve Human Embryonic Stem Cells (hESCs)?	NO
* Did the project on human Embryonic Stem Cells involve cells in culture?	NO
* Did the project on human Embryonic Stem Cells involve the derivation of cells from Embryos?	NO
PRIVACY	
* Did the project involve processing of genetic information or personal data (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?	NO
* Did the project involve tracking the location or observation of people?	NO
RESEARCH ON ANIMALS	
* Did the project involve research on animals?	NO
* Were those animals transgenic small laboratory animals?	NO
* Were those animals transgenic farm animals?	NO
* Were those animals cloned farm animals?	NO
* Were those animals non-human primates?	NO
RESEARCH INVOLVING DEVELOPING COUNTRIES	
* Did the project involve the use of local resources (genetic, animal, plant etc)?	NO
* Was the project of benefit to local community (capacity building, access to healthcare, education etc)?	NO
DUAL USE	
• Research having direct military use	NO
* Research having the potential for terrorist abuse	NO

C Workforce Statistics

3. Workforce statistics for the project: Please indicate in the table below the number of people who worked on the project (on a headcount basis).

Type of Position	Number of Women	Number of Men
Scientific Coordinator	0	1
Work package leaders	2	4
Experienced researchers (i.e. PhD holders)	2	2
PhD Students	0	0
Other	6	13

4. How many additional researchers (in companies and universities) were recruited specifically for this project?	**1**
Of which, indicate the number of men:	1

D Gender Aspects

5. Did you carry out specific Gender Equality Actions under the project?

○ Yes
× No

6. Which of the following actions did you carry out and how effective were they?

		Not at all effective				Very effective
❑	Design and implement an equal opportunity policy	○	○	○	○	○
❑	Set targets to achieve a gender balance in the workforce	○	○	○	○	○
❑	Organise conferences and workshops on gender	○	○	○	○	○
❑	Actions to improve work-life balance	○	○	○	○	○
○	Other:					

7. Was there a gender dimension associated with the research content – i.e. wherever people were the focus of the research as, for example, consumers, users, patients or in trials, was the issue of gender considered and addressed?

○ Yes- please specify

× No

E Synergies with Science Education

8. Did your project involve working with students and/or school pupils (e.g. open days, participation in science festivals and events, prizes/competitions or joint projects)?

○ Yes- please specify

× No

9. Did the project generate any science education material (e.g. kits, websites, explanatory booklets, DVDs)?

○ Yes- please specify

× No

F Interdisciplinarity

10. Which disciplines (see list below) are involved in your project?

× Main discipline[6]: 2.2

○ Associated discipline[6]: ○ Associated discipline[6]:

G Engaging with Civil society and policy makers

11a Did your project engage with societal actors beyond the research community? *(if 'No', go to Question 14)*

× Yes
○ No

11b If yes, did you engage with citizens (citizens' panels / juries) or organised civil society (NGOs, patients' groups etc.)?

○ No

[6] Insert number from list below (Frascati Manual).

- [x] Yes- in determining what research should be performed
- [ ] Yes - in implementing the research
- [ ] Yes, in communicating /disseminating / using the results of the project

11c In doing so, did your project involve actors whose role is mainly to organise the dialogue with citizens and organised civil society (e.g. professional mediator; communication company, science museums)?	[ ]	Yes
	[x]	No

12. Did you engage with government / public bodies or policy makers (including international organisations)

- [x] No
- [ ] Yes- in framing the research agenda
- [ ] Yes - in implementing the research agenda
- [ ] Yes, in communicating /disseminating / using the results of the project

13a Will the project generate outputs (expertise or scientific advice) which could be used by policy makers?

- [ ] Yes – as a **primary** objective (please indicate areas below- multiple answers possible)
- [x] Yes – as a **secondary** objective (please indicate areas below - multiple answer possible)
- [ ] No

13b If Yes, in which fields?

Agriculture		Energy		Human rights	
Audiovisual and Media		Enlargement		Information Society	
Budget		Enterprise		Institutional affairs	
Competition		Environment		Internal Market	
Consumers		External Relations		Justice, freedom and security	
Culture		External Trade		Public Health	
Customs		Fisheries and Maritime Affairs	x	Regional Policy	
Development Economic and Monetary Affairs		Food Safety		Research and Innovation	
Education, Training, Youth		Foreign and Security Policy	x	Space	
Employment and Social Affairs		Fraud		Taxation	
		Humanitarian aid		Transport	x

13c If Yes, at which level?

- ○ Local / regional levels
- ○ National level
- ✘ European level
- ✘ International level

H Use and dissemination

14. How many Articles were published/accepted for publication in peer-reviewed journals?	-
To how many of these is open access[7] provided?	-
How many of these are published in open access journals?	-
How many of these are published in open repositories?	-
To how many of these is open access not provided?	-
Please check all applicable reasons for not providing open access:	
❑ publisher's licensing agreement would not permit publishing in a repository ❑ no suitable repository available ❑ no suitable open access journal available ❑ no funds available to publish in an open access journal ❑ lack of time and resources ❑ lack of information on open access ❑ other[8]: ……	

15. How many new patent applications ('priority filings') have been made? *("Technologically unique": multiple applications for the same invention in different jurisdictions should be counted as just one application of grant).*		-
16. Indicate how many of the following Intellectual Property Rights were applied for (give number in each box).	Trademark	-
	Registered design	-
	Other	
17. How many spin-off companies were created / are planned as a direct result of the project?		-
Indicate the approximate number of additional jobs in these companies:		

18. Please indicate whether your project has a potential impact on employment, in comparison with the situation before your project:

❑	Increase in employment, or	❑	In small & medium-sized enterprises
❑	Safeguard employment, or	❑	In large companies
❑	Decrease in employment,	✘	None of the above / not relevant to the project
❑	Difficult to estimate / not possible to quantify		

[7] Open Access is defined as free of charge access for anyone via Internet.
[8] For instance: classification for security project.

19. For your project partnership please estimate the employment effect resulting directly from your participation in Full Time Equivalent (*FTE = one person working fulltime for a year*) jobs:	*Indicate figure:*
Difficult to estimate / not possible to quantify	✘

I Media and Communication to the general public

20. As part of the project, were any of the beneficiaries professionals in communication or media relations?

○ Yes ✘ No

21. As part of the project, have any beneficiaries received professional media / communication training / advice to improve communication with the general public?

○ Yes ✘ No

22 Which of the following have been used to communicate information about your project to the general public, or have resulted from your project?

✘	Press Release	❑	Coverage in specialist press
❑	Media briefing	❑	Coverage in general (non-specialist) press
❑	TV coverage / report	❑	Coverage in national press
❑	Radio coverage / report	✘	Coverage in international press
✘	Brochures /posters / flyers	✘	Website for the general public / internet
❑	DVD /Film /Multimedia	✘	Event targeting general public (festival, conference, exhibition, science café)

23 In which languages are the information products for the general public produced?

❑	Language of the coordinator	✘	English
❑	Other language(s)		

***Question F-10*:** Classification of Scientific Disciplines according to the Frascati Manual 2002 (Proposed Standard Practice for Surveys on Research and Experimental Development, OECD 2002):

FIELDS OF SCIENCE AND TECHNOLOGY

1. NATURAL SCIENCES

1.1 Mathematics and computer sciences [mathematics and other allied fields: computer sciences and other allied subjects (software development only; hardware development should be classified in the engineering fields)]

1.2 Physical sciences (astronomy and space sciences, physics and other allied subjects)

1.3 Chemical sciences (chemistry, other allied subjects)

1.4 Earth and related environmental sciences (geology, geophysics, mineralogy, physical geography and other geosciences, meteorology and other atmospheric sciences including climatic research, oceanography, vulcanology, palaeoecology, other allied sciences)

1.5 Biological sciences (biology, botany, bacteriology, microbiology, zoology, entomology, genetics, biochemistry, biophysics, other allied sciences, excluding clinical and veterinary sciences)

2 ENGINEERING AND TECHNOLOGY

2.1 Civil engineering (architecture engineering, building science and engineering, construction engineering, municipal and structural engineering and other allied subjects)
2.2 Electrical engineering, electronics [electrical engineering, electronics, communication engineering and systems, computer engineering (hardware only) and other allied subjects]
2.3. Other engineering sciences (such as chemical, aeronautical and space, mechanical, metallurgical and materials engineering, and their specialised subdivisions; forest products; applied sciences such as geodesy, industrial chemistry, etc.; the science and technology of food production; specialised technologies of interdisciplinary fields, e.g. systems analysis, metallurgy, mining, textile technology and other applied subjects)

3. MEDICAL SCIENCES
3.1 Basic medicine (anatomy, cytology, physiology, genetics, pharmacy, pharmacology, toxicology, immunology and immunohaematology, clinical chemistry, clinical microbiology, pathology)
3.2 Clinical medicine (anaesthesiology, paediatrics, obstetrics and gynaecology, internal medicine, surgery, dentistry, neurology, psychiatry, radiology, therapeutics, otorhinolaryngology, ophthalmology)
3.3 Health sciences (public health services, social medicine, hygiene, nursing, epidemiology)

4. AGRICULTURAL SCIENCES
4.1 Agriculture, forestry, fisheries and allied sciences (agronomy, animal husbandry, fisheries, forestry, horticulture, other allied subjects)
4.2 Veterinary medicine

5. SOCIAL SCIENCES
5.1 Psychology
5.2 Economics
5.3 Educational sciences (education and training and other allied subjects)
5.4 Other social sciences [anthropology (social and cultural) and ethnology, demography, geography (human, economic and social), town and country planning, management, law, linguistics, political sciences, sociology, organisation and methods, miscellaneous social sciences and interdisciplinary , methodological and historical S1T activities relating to subjects in this group. Physical anthropology, physical geography and psychophysiology should normally be classified with the natural sciences].

6. HUMANITIES
6.1 History (history, prehistory and history, together with auxiliary historical disciplines such as archaeology, numismatics, palaeography, genealogy, etc.)
6.2 Languages and literature (ancient and modern)
6.3 Other humanities [philosophy (including the history of science and technology) arts, history of art, art criticism, painting, sculpture, musicology, dramatic art excluding artistic "research" of any kind, religion, theology, other fields and subjects pertaining to the humanities, methodological, historical and other S1T activities relating to the subjects in this group]

4 References

[AD. 3] TRITON D2.1 - Report on ship reporting systems vulnerability assessment, v1.0, 09/04/14

[AD. 4] A. Grant, P. Williams, "GNSS Solutions: What is the effect of GPS jamming on maritime safety?" *Inside GNSS, vol 4, n.1*

[AD. 5] S. Jones, C. Hoyos ,*GPS pioneer warns on network's security*, Financial Times

[AD. 6] TRITON D3.1 - Report on critical review of security threats affecting ship reporting systems and user needs, v1.0

[AD. 7] TRITON D3.2 – Specification of the Trusted GNSS Module (TGM) and Robust Communication Module (RCM), v1.0

[AD. 8] TRITON – Annex I - Description of work

[AD. 9] TRITON_D7.2_Business and exploitation plan_Close2Final_for_EC_review

[AD. 10] TRITON_D8.1_Project Dissemination Plan_v1.1 - final for EC review

[AD. 11] U.S. Nears eLoran Decision with Broad International Implications", Dee Ann Divis, Inside GNSS, p.24-31, March/ April 2015

[AD. 12] Europe's ports vulnerable as ships sail without oversight, Sam Jones, Financial Times, February 2016

[AD. 13] TRITON - D7.1 Conclusions and Recommendations_Close2Final_for EC review

[AD. 14] TRITON – D6.3 Report on validation test results, v. 1.0, 22/01/2016