ARENA

SEC-2010.2.3-3

Architecture for the recognition of threats to mobile assets using networks of multiple affordable sensors

ARENA WP3: Gap Analysis and Road Map

Filename: ARENA Gap Analysis and RoadMap.doc
Deliverable D3.3 Gap Analysis and Road Map
Report Version 0.8
Classification: PU
Grant Agreement number: 261658
Contract Start Date: May 16, 2011
Duration: May 15, 2014
Project co-ordinator: FOI
Partners: FOI, BMT, ITTI, Sagem, Morpho, TNO, UoR
Responsible for report: FOI, BMT, ITTI, Sagem, Morpho, TNO, UoR
Project website address: www.arena-fp7.eu

1 Executive summary

This document gives an overview which requirements posed by users and stated during specification of ARENA Project have been considered during the specification of the ARENA system concept and its architecture. Furthermore, this document gives also information on which of the requirements that have been implemented and validated during the truck case demo.

The document explains also how the requirements are connected with particular use cases defined in D2.1 and to what extend the gained knowledge could subsequently be used to prepare the demonstrator (implementations) of use cases defined but not covered by ARENA.

Furthermore, the document contains also a Roadmap which defines what priorities should be given to the remaining requirements which has not yet been implemented.

2 Version Management

Version	Date	Author	Modification
0.0.1	May 15 2014	Grzegorz Taberski (ITTI)	First Draft
0.5	July 17 2014	Grzegorz Taberski (ITTI)	Use cases mapping and conclusions
0.8	July 18 2014	Grzegorz Taberski (ITTI)	RoadMap section added, conclusion updated

3 Table of contents

4 Introduction

The aim of this document is to give an overview which system requirements, which are based on user requirements, are supported by the ARENA solution.

The chapter “User requirements” provides information on which of requirements have been considered and fulfilled during the specification of the system concept, which are implemented and finally which have been demonstrated.

The chapter “ARENA Requirements based on DoW” provides information on which of the requirements stated during the specification of the ARENA project and its Description of work that have been considered and fulfilled during the specification of the system concept, which are implemented and finally which have been demonstrated.

The chapter ”ARENA Use Cases” provides information on considered use cases and which of them that have been selected for implementation and demonstration by the project.

The chapter ”Analysis of Use Cases and requirements” connects information from previous chapter into one table which states which requirements have been implemented/demonstrated for selected use cases and maps the requirements to use cases.

The chapter ”RoadMap” presents a table of the requirements which has not been implemented and proposes a prioritization of them. This gives an overview in what order they should be implemented.

The last chapter ”Conclusions” summarizes the whole document and gives an overview what the project has achieved and how it could be hereafter used.

5 User Requirements

The following table is a summary which gives a general overview on which of the user requirements defined in D2.1 are:

- addressed by the generic ARENA concept[1],
- implemented within work on truck and vessel cases and
- demonstrated at the final demo on truck case.

ARENA User Requirement	Score from D2.1	Addressed by the ARENA solution	Implemented	Final demo
Detect & recognise skiff at max range	9,08	Yes	Proof of principle	Yes (recorded data)
To be friendly to the user	8,75	Yes	Yes	Yes
Identify and confirm potential threats	8,67	Yes	Yes	Yes
Detect vehicle abnormal/suspicious behaviour	8,58	Yes	No	No
Surveillance system which is sufficiently modular/flexible to adapt to different vessels - plug 'n play sensors to match potential threats	8,50	Yes	Yes	No

[1] generic architecture of the whole solution described In WP3 could be extended and adapted to fulfil those requirements.

ARENA User Requirement	Score from D2.1	Addressed by the ARENA solution	Implemented	Final demo
Low false alarm rate	8,50	Yes	Partial	Partial
Identify mother ships at distance and avoid	8,50	Yes	No	No
Detection of mother ship	8,50	Yes	Yes	No
Recognize mother ships	8,33	Yes	No	No
Provide simple information from complex situation and multiple sensors to allow people under pressure to make the best decisions	8,33	Yes	Yes	Yes
Identify and avoid mother ships	8,25	Yes	No	No
Detect ships which are close and identify friend from foe	8,25	Yes	No	No
Any system to have low false alarms to be operationally viable	8,25	Yes	Partial	Partial
Situation awareness with increasing resolution (near vessel)	8,17	Yes	No	No
Overlay intelligence regarding positions of mother ships or those without AIS signature and overlay on existing AIS mapping software	8,17	Yes	Yes	Yes
Link information from surrounding vessels via arena to improve situational awareness	8,08	Yes	No	No

ARENA User Requirement	Score from D2.1	Addressed by the ARENA solution	Implemented	Final demo
Integration and fusion of different sensors/systems, intelligent and autonomous surveillance aspect	8,08	Yes	Yes	Yes
Warn of approach to vulnerable areas	8,00	Yes	No	No
Recognize pirate threats and terrorist threats	8,00	Yes	Yes	Yes (simulated)
Identification, modelling and recognition of specific vessel behaviours (activity)	8,00	Yes	Yes	Yes (simulated)
Threat can be wide range of boats - skiffs, larger vessels. mother ships: detection methods need to be relevant to current and foreseen tactics	7,92	Yes	No	No
The equipment to be for safe use with dangerous cargoes	7,92	Yes	No	No
Real-time detection of location, speed and direction of vessels at different ranges	7,92	Yes	Yes, for location	Yes (recorded data)
Distributed system architecture (i.e. two or more ARENA systems working together and sharing information)	7,92	Yes	Partial	Partial (operation center HMI)

ARENA User Requirement	Score from D2.1	Addressed by the ARENA solution	Implemented	Final demo
Detection of all attack modes, not just skiff vessels	7,92	Yes	No	No
Detect any breach of security around the ship	7,92	Yes	No	No
Know when threat is no longer there	7,83	Yes	Yes	Yes
Automatically communicate to others - vessels in area - authorities etc	7,83	Yes	No	No
Probing of vessel(s) - i.e. vessel detected, change ship course/speed, judge how other vessel responds	7,75	Yes	No	No
Immediate perimeter breach detection	7,75	Yes	No	No
Have a local monitoring and threat recognition system on the ship that also can cooperate with other ships' monitoring and threat recognition systems	7,75	Yes	No	No
Detect any suspicious movements at anchorages	7,75	Yes	No	No
Use of AIS data	7,67	Yes	Yes	Yes (simulated)
Intrusion detection	7,67	Yes	No	No
Work around privacy legislation issues	7,58	Yes	Yes	Yes

ARENA User Requirement	Score from D2.1	Addressed by the ARENA solution	Implemented	Final demo
Threat it may not always be a skiff	7,58	Yes	Yes	No
Environmental conditions modelling and monitoring	7,58	Yes	Yes (modelling)	Yes (model ling)
Combine track and trace with close-in sensors	7,58	Yes	Yes (truck case)	Yes (truck case)
Being able to continuously adapt to new threats or ways of attacking the ship	7,58	Yes	No	No
Lower cost than alternatives	7,50	Yes	No	No
Detect tampering of cargo	7,50	Yes	Yes	Yes
Detect persons loitering around vehicle	7,50	Yes	Yes	Yes
Detect malfunctioning of sensor	7,50	Yes	No	No
Focus on ships	7,42	Yes	Yes	Next after truck
Portable surveillance system	7,33	Yes	Yes	No
Focus on 3 ranges of detection: close, medium and long	7,33	Yes	No	No

ARENA User Requirement	Score from D2.1	Addressed by the ARENA solution	Implemented	Final demo
Detection of anomalous signatures <10m	7,33	Yes	No	No
Identify patterns of activity and link to threats	7,17	Yes	Yes	Yes
Focus on 3 areas: cargo, vehicle and people	7,17	Yes	Yes	Yes (only vehicle and people)
0-10m and 10-500m case	7,17	Yes	No	No
Record information for later intelligence and evidence	7,08	Yes	Yes	Yes
Port/shore based attack detection	7,00	Yes	No	No
Directional sensors to monitor speed/direction of approaching vessels	7,00	Yes	No	No
Countermeasures for jamming and spoofing	7,00	Yes	No	No
Also considering threats that can happen to the vessel in the port	7,00	Yes	Yes, if such threats are similar to the ones that can appear on the truck parking	Yes, if such threats are similar to the ones

ARENA User Requirement	Score from D2.1	Addressed by the ARENA solution	Implemented	Final demo
			lot.	that can appear on the truck parking lot.
Real-time video feed of an attack to assist response planning	6,83	Yes	Yes	Yes
Countermeasures for jamming	6,83	Yes	No	No
Transmit alerts between vehicles	6,75	Yes	No	No
Detection of equipment on the approaching skiffs	6,75	Yes	No	No
Recognize vehicles following	6,50	Yes	No	No
Identify patterns of activity and link to mitigation tactics	6,42	Yes	No	No
Information can easily be transferred across national boundaries in quick time	6,33	Yes	No	No
Provide information on a "need-to-know" principle	6,25	Yes	Yes	Yes
Communication with port-based facilities	6,08	Yes	No	No
Detect after attack that ALL pirates departed ship	6,00	Yes	No	No

ARENA User Requirement	Score from D2.1	Addressed by the ARENA solution	Implemented	Final demo
Identify the impact of mitigation tactics	5,75	No	No	No
Focus on either moving or stationary	4,25	Yes	Yes (stationary)	Yes (stationary)

6 ARENA Requirements based on DoW

The following table is a summary which gives a general overview on which of the system requirements taken from DoW are:

- mandatory to implementations (Must – Mandatory or Could – not mandatory),
- addressed by the generic ARENA concept,
- implemented within work on truck and vessel cases and
- demonstrated on final demo on truck case.

Requirements text	**Mandatory?**	**Addressed by the ARENA solution**	**Implemented**	**Final demo**
System should provide robust, proactive threat detection and recognition to security personnel	YES	Yes	Yes	Yes
System should provide autonomous monitoring and situational awareness of the environment surrounding mobile critical assets, in order to alert personnel to potential threats	YES	Yes	Yes	Yes

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
System should support protection of platforms in places where no security solutions such as CCTV monitoring systems are available	YES	Yes	Yes	Yes
System should enable the mobile assets to have the possibility to monitor the immediate surrounding area even if there is no other stationary monitoring system available	YES	Yes	Yes	Yes
Platforms with ARENA system should detect threats themselves	YES	Yes	Yes	Yes
System should help warn moving platforms from possible threats (and possibly backtrack to find out what did happen)	YES	Yes	Yes	Yes

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
System should produce a consistent operational picture around the platform using data association and fusion methods	YES	Yes	Yes	Yes
System should automatically review uncertainties and choose appropriate sensor types for fusion of the multiple sensor data	YES	Yes	Yes	Partially
System should provide adequate automatic assistance for threat recognition	YES	Yes	Yes	Yes
System should breaks down threats into a range of generic indicators of deviant or abnormal behaviour around mobile assets, which will be matched to object properties and their behaviours and interactions	YES	Yes	Yes	Yes

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
System should provide human-machine interaction with intuitive drill-down facilities to quickly assess the systems' hypotheses, by checking the situational picture, the object characteristics, and the sensor data leading to the threat assessment.	YES	Yes	Yes	Yes
System should provide muzzle flash (gunfire) detection	NO	Yes	No	No
System should use laser components which bring range information; laser illumination improves night vision and brings specific detection capability	NO	Yes	No	No

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
System should provide capability to detect noisy events or recognise specific spectra or sound sequences: motorised vehicle, gunfire or explosion	NO	Yes	No	No
System should provide capability to localise the sound source.	NO	Yes	No	No
System should provide capability to detect and analyse vibrations on the ground: moving vehicle, human walking, etc.	NO	Yes	No	No
System should provide capability to detect metallic objects	NO	Yes	No	No
System should support radars as very efficient detection device: day/night, robust to weather conditions, able to provide 360° surveillance	NO	Yes	Yes	No

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
System should support RFID for discriminating people from intruders.	NO	Yes	No	No
System should support passive electromagnetic sensor to detect and recognise potential EM emission from the threat (GSM, radio, …)	NO	Yes	No	No
System should use collaborative reporting systems to diffuse information on the state of collaborating actors	NO	Yes	No	No
System should provide high precision of localisation, and high discrimination capabilities: detect, track, count and discriminate small targets (e.g. human beings vs. animals)	NO	Yes	Yes	Yes
System should have low false alarm rate	YES	Yes	Yes	Yes

Requirements text	Mandat ory?	Addressed by the ARENA solution	Implemented	Final demo
System should optimise detection and recognition of threats in these various contexts while using a generic system architecture	YES	Yes	Yes	Yes
System should provide very high probability of threat detection	YES	Yes	Yes	Yes
Detection accuracy in the local sensors should be at least 60%	YES	Yes	Yes	Yes
Tracking continuity in the local sensors should be at least 60%	YES	Yes	Yes	Yes
Completeness of the common picture should be at least 65% and clarity should be at least 65%	YES	Yes	Yes	Yes
Completeness should be at least 70% and clarity should be at least 70%	YES	Yes	Yes	Yes
Threat classification correctness based on fused common picture > 70%	YES	Yes	Yes	Yes

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
Communication in the meaning of transmission time should be minimized because of a limited bandwidth and energy constraints in sensors	YES	Yes	Yes	Yes
System should be interoperable, in particular with other European detection and monitoring systems	YES	Yes	No	No
System should exploit existing and low cost sensor technologies for e.g. video surveillance (visual and thermal infrared), acoustic sensors, seismic sensors and radars	YES	Yes	Yes	Yes
System architecture should exploit in a plug-and-play manner the available sensors	YES	Yes	Yes	Yes

Requirements text	**Mandatory?**	**Addressed by the ARENA solution**	**Implemented**	**Final demo**
System should take into account existing current national and European safety regulations	YES	Yes	Yes	Yes
The system architecture should be adaptable to a range of mobile critical assets/platforms with a minimum of adjustments	YES	Yes	Yes	Yes
System should consider external information if it is available and e.g. fused with local sensor data to direct the monitoring and analysis to a more effective and fast investigation	YES	Yes	Yes (external ontologies; AIS)	Yes (external ontologies; AIS)
System should address robust detection through fusion of multiple modalities, including radar data, visible and IR images	YES	Yes	No	No
System should be scalable	YES	Yes	Yes	Yes
System should be affordable	YES	Yes	Yes	Yes

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
System architecture should be flexible and adaptable (no specialised set of sensors for an specific monitoring task)	YES	Yes	Yes	Yes
The system should be as much as possible technology independent	YES	Yes	Yes	Yes
The system should allow a decomposition of threats into an object assessment (properties) and a situation assessment (interactions and relations between objects)	YES	Yes	Yes	Yes
System should use open standard and technologies (including security related standards and algorithms)	YES	Yes	Yes	Yes
Threat recognition should be sensor-independend	YES	Yes	Yes	Yes

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
System should be easy to deploy	YES	Yes	Yes	No
System should be deployed on mobile asset itself	YES	Yes	Yes	Yes
System components should be deployed directly onto a mobile asset (not necessarily fixed)	YES	Yes	Yes	Yes
System should be deployable into wide area of environments	YES	Yes	Yes	No
System should reliably differentiate between real threats and false alarms across a range of environments and different types of mobile assets (platforms), such as trucks, trains, vessels and oil rigs	YES	Yes	Yes	No

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
The architecture should be able to interpret the environment even if one or more sensors in the sensor network does not work anymore or has been destroyed	YES	Yes	Partial (untested)	No
The system should be self-protecting concerning misuse of some of the elements of the system by e.g. hackers and terrorists	YES	Yes	No	No
System's wireless communication should bring adaptation and reconfiguration to the systems to cope with various mobile configuration	YES	Yes	No	No

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
The platform equipped with System should be able to protect itself even if there are no connections to external information sources during its movement or as it temporarily stops	YES	Yes	Yes	Yes
System should be autonomous (not depending on existence of any existing sensor or communications network; existing infrastructure will be exploited if available)	YES	Yes	Yes	Yes
The data architecture must allow data to be easily communicated between nodes for fusion and presentation	YES	Yes	Yes (presentation)	Yes (presentation)

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
The system has to provide communication for the individual system components. The system may be connected to the Internet, when that is possible (and in that case relevant information from the Internet will be used)	YES	Yes	Yes	Yes
Failure (of individual components) and difficulty of restoring functionality (i.e. autonomous reconfiguration with stolen or defect sensor) should not imply whole system failure.	YES	Yes	Partially	Partially
System should be built as multisensor wireless network	YES	Yes	Built as IP network including wireless	Demonstrated as wired network
It should be possible to deploy sensors in large area without protection	YES	Yes	Yes	Yes

Requirements text	**Mandatory?**	**Addressed by the ARENA solution**	**Implemented**	**Final demo**
System should address legal and ethical issues of monitoring, especially privacy	YES	Yes	Yes	Yes
System should operate in large, unpredictable environments (not specific sites such as public spaces)	YES	Yes	Yes	Yes
The network composed of mobile assets in large harsh environments (functional units and interfaces) should be secure in terms of identification, authentication, authorization and secure information exchange.	YES	Yes	No	No
System should be able to handle situation assessment in variable environments, as the platform may often change positions as well as be in motion itself	YES	Yes	Yes, through ontology service	Yes, through ontology service

Requirements text	Mandatory?	Addressed by the ARENA solution	Implemented	Final demo
System should be able to handle different types of objects (people, vehicles) as well as different light and weather conditions	YES	Yes	Partial	Partial
System should provide situation assessment for continuous, variable environment concerning light, weather and surrounding (when the platform is moving)	YES	Yes	No, only static platform implemented	No, only static platform demonstrated
System should operate in the land	YES	Yes	Yes	Yes
System should provide day and night observation capability based on combination of infrared and visible observation leads	NO	Yes	Yes	No
System should be integrated	YES	Yes	Yes	Yes

7 ARENA Use Cases

The consortium developed seven use cases to make the user requirements visible. However, the consortium decided that only the use cases 1 & 4 will be implemented and use case 1 will be shown at the final demo. The remaining use cases will however be considered during the definition of the ARENA generic architecture. Furthermore fulfillment of the requirements for use case 1 & 4 will also address some requirements of the remaining use cases, because the algorithms and implementation parts could also be used for them.

The following table is a summary which gives a general overview on which of the use cases are:

- addressed by the generic ARENA concept,
- implemented within work on truck and vessel cases and
- demonstrated at the final demo on truck case.

Use case number	**Use Case name**	**Addressed by the ARENA solution**	**Impleme nted**	**Final demo**
1	ARENA use case for cargo theft of parked truck	Yes	Yes	Yes (recorded data)
2	ARENA use case for threats towards a truck in motion	Yes	No	No
3	ARENA use case for threats towards cruise ship in port	Yes	No	No
4	ARENA use case for piracy attack on ship at sea	Yes	Yes	Yes (recorded

Use case number	Use Case name	Addressed by the ARENA solution	Impleme nted	Final demo
				data)
5	ARENA use case for hijacking of trains or service vehicles and hostage taking	Yes	No	No
6	ARENA use case for an oil rig terrorist attack	Yes	No	No
7	ARENA use case for a container security	Yes	No	No

8 Analysis of use cases and requirements

This chapter contains a table which maps requirements from the users defined in the description of work, to the use cases defined in D2.1. The table contains 123 requirements. The consortium decided that requirements marked as not mandatory (see section 6) and those which have been scored under 6/10 (see section 5) should not been taken into account.

After analyzing the relationship between the Use cases and a particular requirement it is clear that the consortium has:

- implemented 97% of requirements connected with Use Case 1 (stationary truck) and demonstrated 87% of them,
- implemented 70% of requirements connected with Use Case 4 (sailing vessel).

The remaining use cases have been addressed (it means that the requirements connected with this use cases have been implemented for UC1 & UC4) in the following way:

- Use Case 2 (truck in motion) – 88% addressed,
- Use Case 3 (vessel in port) – 73% addressed,
- Use Case 5 (Train hijack) – 89% addressed,
- Use Case 6 (Oil rig) – 87% addressed,
- Use Case 7 (Container theft) – 88% addressed.

The table contains the following columns:

- Requirement – statement which defines the requirement,
- Implemented (UC1 & UC4) – defines which requirements have been implemented for either truck and maritime case,
- Final demo (UC1) – defines which requirements have been demonstrated.

- Columns marked as UC1 – UC7 defines whether the requirement is connected to this use case or not.

The table below, because of its size, have the following shortcuts:

- UC1 – Use Case 1 Stationary Truck,
- UC2 – Use Case 2 Truck in motion,
- UC3 – Use Case 3 Vessel in port,
- UC4 – Use Case 4 Sailing Vessel,
- UC5 – Use Case 5 Train hijack,
- UC6 – Use Case 6 Oil rig,
- UC7 – Use Case 7 Container.

Requirement	**Implem. (UC1 & UC4)**	**Final demo (UC1)**	**UC 1**	**UC 2**	**UC 3**	**UC 4**	**UC 5**	**UC 6**	**UC 7**
Detect & recognise skiff at max range	Yes	Yes	No	No	Yes	Yes	No	Yes	No
To be friendly to the user	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Identify and confirm potential threats	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Detect vehicle abnormal/suspicious behaviour	No	No	No	Yes	No	No	No	No	No
Surveillance system which is sufficiently modular/flexible to adapt to different vessels -	Yes	No	No	No	No	Yes	No	Yes	No

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
plug 'n play sensors to match potential threats									
Low false alarm rate	Partial	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Identify mother ships at distance and avoid	No	No	No	No	No	Yes	No	Yes	No
Detection of mother ship	Yes	No	No	No	Yes	Yes	No	Yes	No
Recognize mother ships	No	No	No	No	Yes	Yes	No	Yes	No
Provide simple information from complex situation and multiple sensors to allow people under pressure to make the best decisions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Identify and avoid mother ships	No	No	No	No	Yes	Yes	No	Yes	No
Detect ships which are close and identify friend from foe	No	No	No	No	Yes	Yes	No	Yes	No
Any system to have low false alarms to be operationally viable	Partial	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Situation awareness with increasing resolution (near vessel)	No	No	No	No	Yes	Yes	No	Yes	No
Overlay intelligence regarding positions of mother ships or those without AIS signature and overlay on	Yes	Yes	No	No	Yes	Yes	No	Yes	No

Requirement	**Implem. (UC1 & UC4)**	**Final demo (UC1)**	**UC 1**	**UC 2**	**UC 3**	**UC 4**	**UC 5**	**UC 6**	**UC 7**
existing AIS mapping software									
Link information from surrounding vessels via arena to improve situational awareness	No	No	No	No	Yes	Yes	No	Yes	No
Integration and fusion of different sensors/systems, intelligent and autonomous surveillance aspect	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Warn of approach to vulnerable areas	No	No	No	Yes	No	Yes	No	No	No
Recognize pirate threats and terrorist threats	Yes	Yes	No	No	Yes	Yes	No	Yes	No
Identification, modelling and recognition of specific vessel behaviours (activity)	Yes	Yes	No	No	No	Yes	No	Yes	No
Threat can be wide range of boats - skiffs, larger vessels. mother ships: detection methods need to be relevant to current and foreseen tactics	No	No	No	No	Yes	Yes	No	Yes	No
The equipment to be for safe use with dangerous cargoes	No	No	No	No	No	Yes	No	Yes	No
Real-time detection of location, speed and direction	Yes	Yes	No	No	Yes	No	No	Yes	No

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
of vessels at different ranges									
Distributed system architecture (i.e. two or more ARENA systems working together and sharing information)	Partial	Partial	Yes	No	Yes	Yes	Yes	No	No
Detection of all attack modes, not just skiff vessels	No	No	No	No	Yes	No	No	Yes	No
Detect any breach of security around the ship	No	No	No	No	Yes	No	No	No	No
Know when threat is no longer there	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automatically communicate to others - vessels in area - authorities etc	No	No	No	No	Yes	Yes	No	No	No
Probing of vessel(s) - i.e. vessel detected, change ship course/speed, judge how other vessel responds	No	No	No	No	Yes	Yes	No	Yes	No
Immediate perimeter breach detection	No	No	No	No	Yes	Yes	No	Yes	Yes
Have a local monitoring and threat recognition system on the ship that also can cooperate with other ships' monitoring and threat	No	No	No	No	Yes	Yes	No	Yes	No

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
recognition systems									
Detect any suspicious movements at anchorages	No	No	No	No	Yes	No	No	No	No
Use of AIS data	Yes	Yes	No	No	Yes	Yes	No	Yes	No
Intrusion detection	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Work around privacy legislation issues	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Threat it may not always be a skiff	Yes	Yes	No	No	Yes	Yes	No	Yes	No
Environmental conditions modelling and monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Combine track and trace with close-in sensors	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Being able to continuously adapt to new threats or ways of attacking the ship	No	No	No	No	Yes	Yes	No	No	No
Lower cost than alternatives	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Detect tampering of cargo	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
Detect persons loitering around vehicle	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes
Detect malfunctioning of sensor	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Focus on ships	Yes	Yes	No	No	Yes	Yes	No	Yes	No
Portable surveillance system	Yes	No	Yes	Yes	No	No	No	No	Yes

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
Focus on 3 ranges of detection: close, medium and long	No	No	No	No	No	Yes	No	Yes	No
Detection of anomalous signatures <10m	No	No	No	No	Yes	Yes	No	Yes	No
Identify patterns of activity and link to threats	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Focus on 3 areas: cargo, vehicle and people	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
0-10m and 10-500m case	No	No	No	No	Yes	Yes	No	Yes	No
Record information for later intelligence and evidence	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Port/shore based attack detection	No	No	No	No	Yes	Yes	No	Yes	No
Directional sensors to monitor speed/direction of approaching vessels	No	No	No	No	Yes	Yes	No	Yes	No
Countermeasures for jamming and spoofing	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Also considering threats that can happen to the vessel in the port	Yes	Yes	No	No	Yes	Yes	No	No	No
Real-time video feed of an attack to assist response planning	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Countermeasures for jamming	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
Transmit alerts between vehicles	No	No	Yes	Yes	Yes	Yes	Yes	No	No
Detection of equipment on the approaching skiffs	No	No	No	No	Yes	Yes	No	Yes	No
Recognize vehicles following	No	No	No	Yes	No	No	No	No	No
Identify patterns of activity and link to mitigation tactics	No	No	No	No	No	Yes	No	Yes	No
Information can easily be transferred across national boundaries in quick time	No	No	No	Yes	No	Yes	No	No	Yes
Provide information on a "need-to-know" principle	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Communication with port-based facilities	No	No	No	No	Yes	Yes	No	Yes	No
System should provide robust, proactive threat detection and recognition to security personnel	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should provide autonomous monitoring and situational awareness of the environment surrounding mobile critical assets, in order to alert personnel to potential threats	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
System should support protection of platforms in places where no security solutions such as CCTV monitoring systems are available	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should enable the mobile assets to have the possibility to monitor the immediate surrounding area even if there is no other stationary monitoring system available	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Platforms with ARENA system should detect threats themselves	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should help warn moving platforms from possible threats (and possibly backtrack to find out what did happen)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should produce a consistent operational picture around the platform using data association and fusion methods	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
System should automatically review uncertainties and choose appropriate sensor types for fusion of the multiple sensor data	Yes	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should provide adequate automatic assistance for threat recognition	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should breaks down threats into a range of generic indicators of deviant or abnormal behaviour around mobile assets, which will be matched to object properties and their behaviours and interactions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should provide human-machine interaction with intuitive drill-down facilities to quickly assess the systems' hypotheses, by checking the situational picture, the object characteristics, and the sensor data leading to the threat assessment.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should have low false	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
alarm rate									
System should optimise detection and recognition of threats in these various contexts while using a generic system architecture	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should provide very high probability of threat detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Detection accuracy in the local sensors should be at least 60%	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tracking continuity in the local sensors should be at least 60%	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Completeness of the common picture should be at least 65% and clarity should be at least 65%	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Completeness should be at least 70% and clarity should be at least 70%	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Threat classification correctness based on fused common picture > 70%	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
Communication in the meaning of transmission time should be minimized because of a limited bandwidth and energy constraints in sensors	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should be interoperable, in particular with other European detection and monitoring systems	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should exploit existing and low cost sensor technologies for e.g. video surveillance (visual and thermal infrared), acoustic sensors, seismic sensors and radars	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System architecture should exploit in a plug-and-play manner the available sensors	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should take into account existing current national and European safety regulations	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
The system architecture should be adaptable to a range of mobile critical assets/platforms with a	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
minimum of adjustments									
System should consider external information if it is available and e.g. fused with local sensor data to direct the monitoring and analysis to a more effective and fast investigation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should address robust detection through fusion of multiple modalities, including radar data, visible and IR images	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should be scalable	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should be affordable	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System architecture should be flexible and adaptable (no specialised set of sensors for an specific monitoring task)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
The system should be as much as possible technology independent	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
The system should allow a decomposition of threats into an object assessment	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
(properties) and a situation assessment (interactions and relations between objects)									
System should use open standard and technologies (including security related standards and algorithms)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Threat recognition should be sensor-independend	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should be easy to deploy	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should be deployed on mobile asset itself	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System components should be deployed directly onto a mobile asset (not necessarily fixed)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should be deployable into wide area of environments	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should reliably differentiate between real threats and false alarms across a range of environments and different types of mobile assets (platforms), such as trucks,	Yes	No	No	No	Yes	Yes	Yes	Yes	No

Requirement	**Implem. (UC1 & UC4)**	**Final demo (UC1)**	**UC 1**	**UC 2**	**UC 3**	**UC 4**	**UC 5**	**UC 6**	**UC 7**
trains, vessels and oil rigs									
The architecture should be able to interpret the environment even if one or more sensors in the sensor network does not work anymore or has been destroyed	Partial	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
The system should be self-protecting concerning misuse of some of the elements of the system by e.g. hackers and terrorists	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System's wireless communication should bring adaptation and reconfiguration to the systems to cope with various mobile configuration	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
The platform equipped with System should be able to protect itself even if there are no connections to external information sources during its	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
movement or as it temporarily stops									
System should be autonomous (not depending on existence of any existing sensor or communications network; existing infrastructure will be exploited if available)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
The data architecture must allow data to be easily communicated between nodes for fusion and presentation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
The system has to provide communication for the individual system components. The system may be connected to the Internet, when that is possible (and in that case relevant information from the Internet will be used)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
Failure (of individual components) and difficulty of restoring functionality (i.e. autonomous reconfiguration with stolen or defect sensor) should not imply whole system failure.	Partial	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should be built as multisensor wireless network	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
It should be possible to deploy sensors in large area without protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should address legal and ethical issues of monitoring, especially privacy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should operate in large, unpredictable environments (not specific sites such as public spaces)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
The network composed of mobile assets in large harsh environments (functional units and interfaces) should be secure in terms of identification, authentication, authorization and secure	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Requirement	Implem. (UC1 & UC4)	Final demo (UC1)	UC 1	UC 2	UC 3	UC 4	UC 5	UC 6	UC 7
information exchange.									
System should be able to handle situation assessment in variable environments, as the platform may often change positions as well as be in motion itself	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should be able to handle different types of objects (people, vehicles) as well as different light and weather conditions	Partial	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should provide situation assessment for continuous, variable environment concerning light, weather and surrounding (when the platform is moving)	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System should operate in the land	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
System should be integrated	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

9 RoadMap

This chapter contains only the requirements which have not been implemented for any use case. The consortium has ranked them with priorities explaining which requirements should be implemented first in order to provide as soon as possible a functional system for most of the use cases. The ranking (priority) of the requirements have been done by taking into account how a particular requirement is connected with the use case:

- Must – requirements which should be implemented, because they are connected with at least 6 use cases,
- Should – requirements which should be implemented after finishing ”Must”, because they are connected with at least 3 use cases,
- Could – requirements which should be implemented in the end of the developing of the final system.

After an analysis it is clear that there are 10 ”Must” requirements, 17 ”Should” requirements and 23 ”Could” requirements. Note that the priority is made to keep the generic architecture. The priority might not be valid if the final system is specified for only one use case.

Requirement	**UC1**	**UC2**	**UC3**	**UC4**	**UC5**	**UC6**	**UC7**	**Priority**
Detect vehicle abnormal/suspicious behaviour	No	Yes	No	No	No	No	No	Could
Identify mother ships at distance and avoid	No	No	No	Yes	No	Yes	No	Could
Recognize mother ships	No	No	Yes	Yes	No	Yes	No	Should
Identify and avoid mother ships	No	No	Yes	Yes	No	Yes	No	Should
Detect ships which are close and identify friend from foe	No	No	Yes	Yes	No	Yes	No	Should

Requirement	UC1	UC2	UC3	UC4	UC5	UC6	UC7	Priority
Situation awareness with increasing resolution (near vessel)	No	No	Yes	Yes	No	Yes	No	Should
Link information from surrounding vessels via arena to improve situational awareness	No	No	Yes	Yes	No	Yes	No	Should
Warn of approach to vulnerable areas	No	Yes	No	Yes	No	No	No	Could
Threat can be wide range of boats - skiffs, larger vessels. mother ships: detection methods need to be relevant to current and foreseen tactics	No	No	Yes	Yes	No	Yes	No	Should
The equipment to be for safe use with dangerous cargoes	No	No	No	Yes	No	Yes	No	Could
Detection of all attack modes, not just skiff vessels	No	No	Yes	No	No	Yes	No	Could
Detect any breach of security around the ship	No	No	Yes	No	No	No	No	Could
Automatically communicate to others - vessels in area - authorities etc	No	No	Yes	Yes	No	No	No	Could
Probing of vessel(s) - i.e. vessel detected, change ship course/speed, judge how other vessel responds	No	No	Yes	Yes	No	Yes	No	Should
Immediate perimeter breach detection	No	No	Yes	Yes	No	Yes	Yes	Should
Have a local monitoring and threat recognition system on the ship that also can cooperate with other ships'	No	No	Yes	Yes	No	Yes	No	Should

Requirement	UC1	UC2	UC3	UC4	UC5	UC6	UC7	Priority
monitoring and threat recognition systems								
Detect any suspicious movements at anchorages	No	No	Yes	No	No	No	No	Could
Intrusion detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Must
Being able to continuously adapt to new threats or ways of attacking the ship	No	No	Yes	Yes	No	No	No	Could
Lower cost than alternatives	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Must
Detect malfunctioning of sensor	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Must
Focus on 3 ranges of detection: close, medium and long	No	No	No	Yes	No	Yes	No	Could
Detection of anomalous signatures <10m	No	No	Yes	Yes	No	Yes	No	Should
0-10m and 10-500m case	No	No	Yes	Yes	No	Yes	No	Should
Port/shore based attack detection	No	No	Yes	Yes	No	Yes	No	Should
Directional sensors to monitor speed/direction of approaching vessels	No	No	Yes	Yes	No	Yes	No	Should
Countermeasures for jamming and spoofing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Must
Countermeasures for jamming	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Must
Transmit alerts between vehicles	Yes	Yes	Yes	Yes	Yes	No	No	Should
Detection of equipment on the approaching skiffs	No	No	Yes	Yes	No	Yes	No	Should
Recognize vehicles following	No	Yes	No	No	No	No	No	Could
Identify patterns of activity and	No	No	No	Yes	No	Yes	No	Could

Requirement	UC1	UC2	UC3	UC4	UC5	UC6	UC7	Priority
link to mitigation tactics								
Information can easily be transferred across national boundaries in quick time	No	Yes	No	Yes	No	No	Yes	Should
Communication with port-based facilities	No	No	Yes	Yes	No	Yes	No	Should
System should be interoperable, in particular with other European detection and monitoring systems	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Must
System should address robust detection through fusion of multiple modalities, including radar data, visible and IR images	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Must
The system should be self-protecting concerning misuse of some of the elements of the system by e.g. hackers and terrorists	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Must
System's wireless communication should bring adaptation and reconfiguration to the systems to cope with various mobile configuration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Must
The network composed of mobile assets in large harsh environments (functional units and interfaces) should be secure in terms of identification, authentication, authorization and secure information exchange.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Must

Requirement	UC1	UC2	UC3	UC4	UC5	UC6	UC7	Priority
System should provide situation assessment for continuous, variable environment concerning light, weather and surrounding (when the platform is moving)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Must

10 Conclusions

All in all, ARENA has posed 135 requirements and 7 use cases. The requirements were split into two groups:

- requirements from DoW – 69 requirements from which 57 marked as mandatory,
- requirements from end users – 67 requirements from which 64 scored above 6/10.

The consortium has considered 57+64=121 requirements selected as described above.

The consortium has selected two use cases for the implementation and one of them for demonstration. This has led to the fact that not all of the requirements have been covered, because it was not needed to prepare only functionality connected with selected use cases. However all of the requirements have been considered during the preparation of the generic architecture which is compatible with them.

After the analysis made in section 8 it is clear that, because of the fact that the demonstrated/implemented part has some overlapping requirements, the developed solution could be in the future easily adapted to fulfil also other use cases. Because of that we have prepare three metrics to show how many of the initial goals the ARENA project has achieved:

- implemented – states how many percent of the requirements connected with a particular use case have been implemented,
- demonstrated – states how many percent of the requirements connected with a particular use case have been shown during final demo,
- addressed – states how many percent of the requirements connected with a particular use case have been solved/implemented for other use cases (we assume that this outcome could be used to solve the unimplemented use cases).

The result of the project is as follows:

- Use Case 1 – implemented 91%, demonstrated 87%
- Use Case 2 – addressed 88%,
- Use Case 3 – addressed 73%,
- Use Case 4 – implemented 70%,
- Use Case 5 – addressed 89%,
- Use Case 6 – addressed 87%,
- Use Case 7 – addressed 88%.

The next step and further work on this project could be done by transferring the knowledge and solutions developed in UC1 and UC4 to other use cases. This ensure that the other use cases will use the developed parts and reach the level of functionalities stated by *addressed* metric. The following project should also fulfill the requirements which have not been addressed/implemented. However, those remaining requirements are mostly not connected with the core functionalities (e.g. security and some additional functionalities which are connected with a particular use case). This means that they could be solved independently and do not withstands the preparation of demonstrators for the use cases.

The proposition of the RoadMap which defines the order of implementation of the remaining requirements has been given in section 9.