D9.3 – Report on the Threat Scenarios Workshop

Due date of deliverable: 31/12/2014
Actual submission date: 05/01/2015

Organisation name of lead contractor for this deliverable: UCSC

Revision: 1.0

Grant Agreement N°: 607567
Project Acronym: IPATCH
Project Title: Intelligent Piracy Avoidance using Threat detection and Countermeasure Heuristics
Funding Scheme: SEC-2013.2.4-2
Start date of project: 01/04/2014
Duration: 36M

<table>
<thead>
<tr>
<th>Dissemination Level</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PU</td>
<td>Public</td>
</tr>
<tr>
<td>RE</td>
<td>Restricted to a group specified by the consortium (including the Commission Services)</td>
</tr>
</tbody>
</table>

Project co-funded by the European Commission within the 7th Framework Programme (2007-2013)
# Table of Contents

Executive Summary ............................................................................................................. 6

1 Introduction ..................................................................................................................... 7
   1.1 The IPATCH Project .................................................................................................... 7
   1.2 The On-board System Concept .................................................................................. 7
   1.3 This Document ......................................................................................................... 7

2 Organization of the workshop ........................................................................................... 8
   2.1 The agenda ............................................................................................................... 8
   2.2 The stakeholder group .............................................................................................. 8

3 Summary of the presentations ........................................................................................... 9
   3.1 Presentation of the user requirements analysis ............................................................ 9
   3.2 Presentation of the preliminary threat scenarios ......................................................... 9
      3.2.1 Macro-scenarios ................................................................................................. 9
      3.2.2 Micro-scenarios ............................................................................................... 10

4 Summary of stakeholders’ comments and workshop outcomes ......................................... 10
   4.1 IPATCH project aim ................................................................................................. 10
   4.2 IPATCH on-board system’s applications .................................................................. 11
   4.3 IPATCH on-board system development challenges .................................................... 11
   4.4 Issues on the data and information used .................................................................... 12
   4.5 Comments on anti-piracy measures ....................................................................... 12
   4.6 Threat scenario comments ...................................................................................... 13
      4.6.1 Macro-scenarios ............................................................................................... 13
      4.6.2 Micro-scenarios ............................................................................................... 13
   4.7 Comments on the proposed ‘Manual on Countermeasures’ (Deliverable 4.4) ............ 14

5 Conclusions ...................................................................................................................... 14
Document Summary Information

Authors and Contributors

<table>
<thead>
<tr>
<th>Initials</th>
<th>Name</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GB</td>
<td>Giulia Berlusconi</td>
<td>UCSC</td>
</tr>
<tr>
<td>MD</td>
<td>Marco Dugato</td>
<td>UCSC</td>
</tr>
<tr>
<td>CS</td>
<td>Cristina Soriani</td>
<td>UCSC</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Initials</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>15/12/2014</td>
<td>MD</td>
<td>Initial version</td>
</tr>
<tr>
<td>0.2</td>
<td>18/12/2014</td>
<td>ALL</td>
<td>Draft for internal review</td>
</tr>
<tr>
<td>0.3</td>
<td>27/12/2014</td>
<td>GB</td>
<td>Draft for internal release to Consortium</td>
</tr>
<tr>
<td>0.4</td>
<td>02/01/2015</td>
<td>GB</td>
<td>Draft for submission to EC (edited)</td>
</tr>
<tr>
<td>1.0</td>
<td>05/01/2015</td>
<td>TC</td>
<td>Final version for submission to EC</td>
</tr>
</tbody>
</table>

Quality Control

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Review</td>
<td>Stefano Caneppele</td>
<td>19/12/2014</td>
</tr>
<tr>
<td>Work Package Leader</td>
<td>Ernesto U. Savona</td>
<td>22/12/2014</td>
</tr>
<tr>
<td>Project Manager</td>
<td>Tom Cane</td>
<td>05/01/2015</td>
</tr>
</tbody>
</table>

Security Scrutiny Committee Review

<table>
<thead>
<tr>
<th>Comments</th>
<th>Recommended Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>This document does not contain any information which is not already in the public domain.</td>
<td></td>
</tr>
<tr>
<td>It is therefore suitable for public dissemination, as required by the DoW.</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>05/01/2015</td>
</tr>
</tbody>
</table>
Disclaimer

The content of the publication herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the IPATCH consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the IPATCH Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing, neither the IPATCH Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.
List of Tables

Table 1. Categories of stakeholders participating in the workshop......................................................... 9

List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFCAN</td>
<td>Association Française des Capitaines de Navires</td>
</tr>
<tr>
<td>BMP4</td>
<td>Best Management Practices for Protection against Somalia Based Piracy (Version 4 – August 2011)</td>
</tr>
<tr>
<td>HMI</td>
<td>Human-Machine Interface</td>
</tr>
<tr>
<td>IMB</td>
<td>International Maritime Bureau of the International Chamber of Commerce</td>
</tr>
<tr>
<td>PROMERC</td>
<td>Project ‘Protection Measures for Merchant Ships’, funded by the European Commission, 7th Framework Programme</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
</tbody>
</table>
Executive Summary

The Report on the Threat Scenarios Workshop (D9.3) presents the results of Task 9.3. In Task 9.3 a discussion workshop with maritime companies and other relevant stakeholders was organised to verify the data analysis results, discuss the use of countermeasures and develop realistic and pertinent threat scenario models. This Deliverable describes the preliminary results of Task 3.2 (Data Analysis) and Task 3.3 (Threat Scenarios and Countermeasure Definitions) as well as the main points discussed during the Threat Scenarios Workshop held in London on 3rd December 2014.

The outcome of the workshop is a long list of useful comments and suggestions that will inform the refinement of the threat scenarios (Task 3.3) as well as provide input regarding the manual on countermeasures (Task 4.4), the threat recognition algorithms (Task 6.2), and the decision support tool (Task 7.2).

In particular, the issue of underreporting was identified by the experts. IPATCH is in a position to contribute here by supporting the reporting process through standardisation of the data and automation of the report creation using the recorded data from the on-board system. Near misses, as well as successful attacks, can be reported in this way, vastly increasing the amount of incident data available to stakeholders. As well as saving the captain and crew time, the collected data can also be immediately sent to other nearby ships so they have the most up-to-date information for that area.

Another important area of focus for IPATCH will be the Human-Machine Interface (HMI), as this was identified by the experts as the “make or break” of the system. Ship crews already have many screens to monitor during voyages, so any additional information source must be carefully designed to give exactly the right information at exactly the right time. If the system is not intuitive, or if it creates extra work for the crew (e.g. through many false alarms), it will not be used and may even be turned off.

Finally, the Manual on Countermeasures (Deliverable 4.4) is seen as a good potential companion to BMP4 which could provide additional details on piracy risks (particularly for the West Africa region) and implications of countermeasures which are not present in the current BMP4 document.

More information on the IPATCH project can be found at www.ipatchproject.eu
1 Introduction

1.1 The IPATCH Project

Funded by the European 7th Framework Programme, the IPATCH project addresses Security Topic SEC-2013.2.4-2: Non-military protection measures for merchant shipping against piracy. The goal of the IPATCH project is three-fold:

1. To perform an in-depth analysis of the legal, ethical, economic and societal implications of existing counter piracy measures.
2. To produce well-founded recommendations to the industry in the form of a manual, extending and complementing the Best Management Practices document and to support the use and further development of countermeasures.
3. To develop an on-board automated surveillance and decision support system providing early detection and classification of piracy threats and supporting the captain and crew in selecting the most appropriate countermeasures against a given piracy threat.

The analysis performed under (1) will lead to recommendations for the use of countermeasures in a range of scenarios, structured as a manual (2), and development and implementation of an on-board surveillance and threat detection system (3). At the end of the project, the developed on-board system will be demonstrated in real-life maritime environments with simulated piracy attacks.

1.2 The On-board System Concept

In the second phase of the project, the main focus is the development of the on-board surveillance and threat detection system that can provide early detection and classification of piracy threats. Decision support tools will assist the captain and crew in selecting the most appropriate countermeasures that can be used against piracy threats. The IPATCH on-board system will consist of 3 elements:

- A sensor suite, incorporating existing surveillance capabilities of the vessel (e.g. radar, AIS) and extending and complementing them with the use of advanced visual and thermal infrared cameras.
- A threat recognition system which fuses data from the various sensors and employs new detection, tracking and situational awareness algorithms to give early warning of piracy threats to the captain and crew.
- A decision support tool which provides real-time information to the captain and crew and helps them select the most appropriate countermeasures and best course of action to take to protect the ship from potential piracy threats as they develop.

1.3 This Document

Within the IPATCH project, Work Package 3’s objective is to collect, systematise and analyse data on pirate attacks in order to assess their consequences and to develop a set of threat scenarios to be used in the development of the threat recognition and decision support modules.
In Task 3.3, a typology of pirate attacks will be developed based on criteria such as success, location, raiding party and raided vessel. Threat scenarios and countermeasures will be defined in terms of reduction/increase in the probability of threat and reduction/increase in potential harm. A discussion workshop with maritime companies and other relevant stakeholders (Task 9.3) has also been organised to verify the preliminary results of Task 3.2 (Data Analysis) and Task 3.3 (Threat Scenarios and Countermeasure Definitions).

The results of the discussion workshop will inform the refinement of the threat scenarios (Task 3.3), and they will provide input regarding the manual on countermeasures (Task 4.4), the threat recognition algorithms (Task 6.2) and the decision support tool (Task 7.2).

This report (Deliverable 9.3) provides a summary of the Threat Scenarios Workshop (Task 9.3), outlining the main topics and issues debated and the conclusions drawn. This workshop’s aim was to discuss with a wide range of representatives from maritime companies and other relevant stakeholders the data analysis results and state of the art in countermeasures, and to collect suggestions and feedback to develop accurate and reliable threat scenarios.

This report is organised as follows. Section 2 describes the organization of the workshop. Section 3 summarises the presentations that IPATCH consortium members gave in order to introduce the stakeholders to the User Requirements Analysis (Task 2.1) results along with the preliminary findings of the Data Analysis (Task 3.2) and Threat Scenarios and Countermeasure Definitions (Task 3.3). Finally, Section 4 describes the main discussion points and Section 5 concludes.

2 Organization of the workshop

2.1 The agenda

After a brief introduction explaining the IPATCH project’s goals and activities, the workshop consisted of two main parts. The first part was dedicated to discussing the User Requirements Analysis (Task 2.1) results, which brought together a group of end-users and other relevant stakeholders to define requirements for the manual on countermeasures (Task 4.4) and the on-board system (WP5-7). The second part presented the preliminary findings of the analysis of the data on piracy incidents (Task 3.2) – which were collected during the activities of WP3 and described in Deliverable 3.1 – and the first set of threat scenarios developed during Task 3.3 (Threat Scenarios and Countermeasure Definitions). Stakeholders were then asked to comment on these preliminary results and to provide feedback on the first set of threat scenarios. During the workshop, the stakeholders were also asked to complete a questionnaire regarding the installation and operational costs of a list of anti-piracy countermeasures.

2.2 The stakeholder group

A wide range of representatives from maritime companies and other relevant stakeholders independent from the project participated in the workshop. The workshop provided a tremendous opportunity to bring together experts from industry, research and technology organisations, and academia; representatives of industry organisations; and end users to discuss the issues relating to piracy as well as the development of new methods and technologies to address the challenges facing merchant shipping. Members of the IPATCH consortium were also present. Table 1 summarises the various categories of stakeholders who participated in the workshop.
**Summary of the presentations**

**3.1 Presentation of the user requirements analysis**

In this first presentation, the results of the User Requirements Analysis (Task 2.1) were presented. In particular, this initial analysis comprised all of those issues that could be used to support the IPATCH project, such as: information on the context of piracy in the two areas on which the project is focused (East Africa and West Africa); the state of the art of existing sensors and anti-piracy measures; and a functional description of the requirements for the IPATCH on-board system.

The analysis was based on existing literature on the topic and on a questionnaire administered to a sample of relevant stakeholders. The User Requirements Analysis highlighted the features that the IPATCH system should cover in order to provide effective support to existing anti-piracy measures and procedures. The IPATCH consortium presented the results of the analysis and asked the participants to express their points of view on the findings and eventually suggest new or different requirements to be considered.

**3.2 Presentation of the preliminary threat scenarios**

The consortium presented to the invited stakeholders a preliminary set of threat scenarios based on the analysis of the data on piracy incidents collected during Task 3.1 (Data Acquisition and Structuring). In particular, two types of threat scenarios were defined during Task 3.3 (Threat Scenario and Countermeasure Definitions): macro- and micro-scenarios.

**3.2.1 Macro-scenarios**

This first analysis aims to define the general conditions that are more likely to facilitate an attack. It is a preventive analysis of the risk associated with the characteristics of the attacks.
Different dimensions of the attacks have been considered in relation to the geographic area (where), the characteristics of the attack (how), the moment of the attack (when) and the characteristics of the targeted ship (who). For each dimension, several scenarios have been defined considering the different possible situations, and for each scenario, a probability of success was calculated based on the actual or attempted attacks. The scenarios presenting the highest probabilities of success have been considered as the actual threat scenarios highlighting the macro-conditions that are more likely to facilitate a positive result of an attack.

The first results and next steps of the analysis (e.g. considering also the likelihood of the scenarios, defining the probability of harm, considering the presence of countermeasures) were also briefly presented.

3.2.2 Micro-scenarios
This second part defines specific realistic situations which are representative of the pirates’ behavioural patterns during the attacks. These micro-scenarios were defined starting from the quantitative and qualitative evidence collected through consultation with experts and stakeholders (Task 2.1), the collection and analysis of data on piracy incidents (Task 3.2) and the review of literature on maritime piracy (Task 3.3).

The basic idea is to define the general patterns that pirates use when approaching and attacking an anchored or steaming ship. Then, these general patterns must be compared with ships’ normal conduct in order to highlight anomalous behaviours that the IPATCH system should recognize to generate an early warning.

Five micro-scenarios have been presented to the stakeholders asking them to evaluate their plausibility and to suggest other possible common patterns.

4 Summary of stakeholders’ comments and workshop outcomes
The following paragraphs summarise the main topics and conclusions of the discussion. For clarity, all of the comments, suggestions and criticalities collected have been categorised and summarised in seven thematic sections.

4.1 IPATCH project aim
- It has been clarified that project IPATCH’s main focus is to create an early warning system in order to provide information to crews by identifying risk factors and acting in response to anomalous behaviours.
- In this sense, the project will create a more reactive system and thus differs from a preventative project, such as the PROMERC project.
- Evaluation of the best strategies, countermeasures and procedures to be adopted once the ship has been boarded is out of the scope of this project.
4.2 IPATCH on-board system’s applications

- The IPATCH system will rely on a set of information about pirate behaviour that could be renewed on a regular basis so that it will use the most recent data for drawing conclusions and providing early warnings.

- The system will be developed to use the hardware already available on the ship and to improve its efficacy. In particular, the system will be built into the ship’s existing security and communication system, and it will provide a real-time operational picture of security situations in the area surrounding the ship. This information will be displayed on one interface (e.g., a map, radar screen).

- In the case of unexpected conditions or potentially dangerous factors, the IPATCH system will alert the captain and crew and provide critical information for assessing and mitigating the risk.

- The possibility of data-sharing is crucial for making the system more efficient and for improving existing knowledge. The system will integrate intelligence information (e.g., presence of friendly ships) sent directly to the system or to on-board crews and security teams (using radio or Web solutions). The system installed on a ship is, in principle, able to interact with other systems and share surveillance information. This aspect will probably not be tested during the project, but it is a designed function.

- In the case of an actual or attempted attack, the on-board crew could report it directly and automatically to some database. This report will include all of the information coming from the system, such as the characteristics of the attacks, the exact spatial and temporal location and the number of pirates’ boats and weapons used. The aim is to streamline the entire reporting process in order to improve the quality and quantity of the data on which the system depends.

- This will also guarantee a body of evidence (videos, voice recordings, etc.) that could be used in court proceedings so that ship owners and operators do not have to rely only on witness statements.

- The system is intended for use both at sea and in port areas, and could also be adapted to work on fixed platforms, such as oil and gas installations.

4.3 IPATCH on-board system development challenges

- Defining a reasonable warning time is difficult. Training of the crew is a fundamental factor. Even in the case of an early warning, every countermeasure’s efficacy and the response time to an alarm are strictly connected to the quality of the crew. The reaction time is also connected to the number of crew members and the ship size. In general, a well-trained crew is ready in about 10 minutes. The countermeasures’ efficacy will also depend on the ship speed: in the case of an attack against an anchored ship, the time between the warning and the actual attack is lower than the one against a moving target.

- The IPATCH system will not replace the security guards or the crew members. These individuals may use the system to gain pertinent information to complete their specific duties.

- The interaction between human actions and the system is crucial. The Human-Machine Interface (HMI) will be designed to be as intuitive as possible but of course all users would be trained to recognise early warning messages and actual threats. The crew members and the captain have to trust the IPATCH system. There is therefore a need to reduce false alarms so that they can accept the system as useful.
The IPATCH system cannot prevent the presence of hostile subjects on board. Like all on-board systems, it is also vulnerable when the ship is boarded so cyber security prevention measures and control for unauthorized access need to be put into place in order to prevent any misuse of the system.

4.4 Issues on the data and information used

- The IPATCH project covers data on both piracy attacks and armed robbery, as laid down in Article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS) and in Resolution A.1025 (26) adopted on 2 December 2009 at the 26th Assembly Session of the International Maritime Organisation (IMO), respectively.
- In the project, information on both actual and attempted attacks is considered. The latter are particularly interesting for evaluating the efficacy of the countermeasures used. However, available data’s incompleteness does not always allow for this kind of analysis.
- The statistics on piracy attacks coming from IMB cannot be considered complete because they comprise only attacks that private companies have communicated. The experts suggest using those data only as indicators of the phenomenon.
- Another issue regarding the data on the attacks is a lack of consistency in the reporting formula (e.g., the information that has to be provided or the classifications to be used).
- AFCAN, a French captains’ association, has been suggested for consideration as an additional source of reliable information.
- Underreporting is a fundamental problem. Some experts stated that only about 1 incident out of 10 is likely to be reported. Motivations for not reporting an attack can be varied: increase in insurance premiums; long and tedious procedures for reporting; bad publicity for the shipping company; unwillingness to declare the nature of the entire cargo; and costs of the loss due to the fact that the time spent on the report could be higher than the actual damage. The experts were asked if some specific patterns of the underreporting phenomenon could be found or if underreporting randomly affects all areas worldwide, but a clear answer on this topic was not reached in the workshop.
- Information on the vessels’ speed is often missing, but it may be crucial for the countermeasures’ effectiveness and the time needed for a useful early warning (cf. Section 4.2). Usually, the ships sail at full speed in high-risk areas. A pirate skiff normally sails at 25 knots.

4.5 Comments on anti-piracy measures

- The cost of countermeasures is relevant for making a choice to install or use them. Better technologies already exist, but they are currently unaffordable for shipping companies. As soon as they become cheaper, they could be implemented in the future. As an example, drones could be used for early detection of the pirates, or hostile vehicle mitigation (HVM) systems could be used to disable pirate skiffs.
- Travelling at high speed is an effective way to avoid attacks but is costly. In order to proceed at full speed, a 350-meter-long ship uses about 260 tonnes of fuel per day, whereas when sailing at service speed, it uses only about 50 tonnes of fuel per day. One tonne of fuel costs about 800 USD.
- Aluminium flaps can be added as a new effective countermeasure for avoiding pirates’ boarding.
Private maritime security companies (PMSCs) are one of the main effective countermeasures. Some stakeholders stated that most captains would like to have them on board and that a large reduction of the attacks in East Africa is due to the use of private guards on ships. However, the use of armed guards and other countermeasures can create some legal concerns because the guidelines are not always clear, and different states may have different legislations. Furthermore, security professionals are expensive, and the possibility for some shipping companies to fall back on cheaper and unexperienced guards could create serious problems.

The use of a citadel is widespread. However, having a citadel is a double-edged sword, as it provides temporary refuge but can also turn into a trap if no help arrives between 24 hours and 48 hours. This issue is becoming relevant especially in West Africa. In any case, a citadel should be considered as a last resort for the crew, and it is effective only if properly constructed and installed.

Almost all of the countermeasures depend on the crew skills. They must be able to protect the ship correctly without harming themselves, and in a short time. Apart from training, other crucial issues that may affect the crew's effectiveness in the security procedures are fatigue and availability. Safe manning is a crucial aspect. The tendency is to reduce the number of people on the ships, but this creates the problems of duplicate tasks and inefficiency in the response time to an alarm.

4.6 Threat scenario comments

4.6.1 Macro-scenarios

No specific comments on the macro threat scenarios have been advanced. Only some concerns arose about the reliability of the dataset for underreporting reasons (cf. Section 4.4). However, no suggestions about better sources of information were known to the experts.

4.6.2 Micro-scenarios

In general, the micro-scenarios appeared plausible to the stakeholders. Of course, the reality is always different, but common patterns can be identified. No relevant missing scenarios or situations have been highlighted.

Vessels rarely are at anchor in the high-risk areas, but in the same areas, fixed assets (e.g., oil platforms) can be found. The scenario should be applied to them, too.

The experts confirmed that, during ship-to-ship operations, the ships are incredibly vulnerable.

Some scenarios are more likely to affect certain types of ships than others. Ship type makes a difference, as the dimensions of the ships are different. As an example, ship-to-ship transfer is mainly relevant for tankers. The other scenarios are relevant for all other ship types.

Some ship characteristics (e.g., freeboard, type, service speed) should be added to the scenario descriptions.

The port scenario is relevant only for West Africa. In East Africa, the only port is in Somalia.

Some pirates may use a “friendly” ship to approach the target and test its reaction before the attack. Evidences of this pattern can be found particularly against stationary targets.
4.7 Comments on the proposed ‘Manual on Countermeasures’ (Deliverable 4.4)

- The manual should not be a new version of the BMP4 but rather a complementary document to aid in the usage and further development of counter-piracy measures. BMP4’s indications are often perceived as mandatory, and this sometimes creates conflict with the authority as well as liability of the captain, who has the responsibility to make the final decision. This last issue was mainly due to the insurance companies that consider compliance with these guidelines as a fundamental criterion for obtaining refunds.

- Although the project’s aim is not to train the captain and the crew, their behaviour during an attack can be considered part of the countermeasures that should be included in the manual. In particular, offering no resistance is often an efficient method for reducing the harm of the attack when pirates manage to board the ship.

- A section of the manual should be dedicated to analysing pirates’ possible responses to the countermeasures used and to what extent an action taken could provoke them, thus increasing the potential harm of the attack.

5 Conclusions

Within the IPATCH project, Task 3.3’s objective is to develop a typology of pirate attacks based on criteria such as success, location, raiding party and raided vessel. In order to verify the preliminary results of Task 3.2 (Data Analysis) and Task 3.3 (Threat Scenarios and Countermeasure Definitions), a discussion workshop with maritime companies and other relevant stakeholders (Task 9.3) was organised in London on 3rd December 2014.

The outcome of the workshop is a long list of useful comments and suggestions that will inform the refinement of the threat scenarios (Task 3.3) as well as provide input regarding the manual on countermeasures (Task 4.4), the threat recognition algorithms (Task 6.2), and the decision support tool (Task 7.2).

In particular, the issue of underreporting was identified by the experts. IPATCH is in a position to contribute here by supporting the reporting process through standardisation of the data and automation of the report creation using the recorded data from the on-board system. Near misses, as well as successful attacks, can be reported in this way, vastly increasing the amount of incident data available to stakeholders. As well as saving the captain and crew time, the collected data can also be immediately sent to other nearby ships so they have the most up-to-date information for that area.

Another important area of focus for IPATCH will be the Human-Machine Interface (HMI), as this was identified by the experts as the “make or break” of the system. Ship crews already have many screens to monitor during voyages, so any additional information source must be carefully designed to give exactly the right information at exactly the right time. If the system is not intuitive, or if it creates extra work for the crew (e.g. through many false alarms), it will not be used and may even be turned off.

Finally, the Manual on Countermeasures (Deliverable 4.4) is seen as a good potential companion to BMP4 which could provide additional details on piracy risks (particularly for the West Africa region) and implications of countermeasures which are not present in the current BMP4 document.