FORESIGHT

ADVANCED CYBER-SECURITY SIMULATION PLATFORM FOR PREPAREDNESS TRAINING IN AVIATION, NAVAL AND POWER-GRID ENVIRONMENTS

Grant Agreement: 833673

D5.3 – annex 3 of 3
Models for risk analysis and assessment (naval use-case)

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 833673.

Workshop n°1: Framing

(1 to 3 half-day sessions)

1 Study Objectives

- Identify platform runtime vulnerabilities & threats
- Provide rational inputs to generate scenarios for the Foresight naval pilot

Missions (i.e. raison d'être)

- Manage ferry navigation
- Ensure good transport conditions
- Recreational internet access

Time frame

Strategic cycle: ... years

Practical cycle: ... months

2 Asset owners, Main Primary Assets, and Security Needs

(confidentiality/privacy, integrity and availability)

Asset owners

- Shipowner
- Ship manager
- Service providers (incl. ISP)
- Regulators (e.g. IMO)
- PAX
- Captain
- CISO
- Equipment supplier maintenance operators
- Crew
- Ship vendor

Primary Assets

- Energy management A
- Energy management I
- I
- A
- Entertainment Internet access A
- Safety management IA
- Navigation management IA
- Other external communications A
- External VHF communications A
- Utilities management IA
- Propulsion management IA
- Software maintenance and patching A
- Software maintenance and patching I
- GNSS IA

Processes / services

Information

Security need

- Sensitive data (VDR, exploitation) C
- Customer data (incl. internet access history) P
- Sensitive data (VDR, exploitation) I
- External VHF communications I

C I A P

3 Existing / Regulatory Set of Security Controls

(i.e. applicable standards, possibly with restrictions)

Standard sources:

- ❑ ANSSI basic hygiene
- ❑ ANSSI PSSIE
- ❑ CIS security controls
- ❑ ISA/IEC 62443-3-3
- ❑ ISO 27002
- ❑ NIST SP800-53
- ❑ EUROCAE ED-203
- ☑ EU GDPR

Other sources:

Acronyms / Initialisms

- International Maritime Organization
- PAX: passenger
- Electronic Navigation Chart
- Voyage Data Recorder
- Electronic Chart Display and Information System
- Safety Management System
- Global Navigation Satellite System

Severity assessment of feared event impacts

(i.e. considering existing or already specified security measures)

2a

- Propulsion management ¬A
  - Accident
  - Immobilisation at sea >6h or during manoeuvre
  - Immobilisation at sea <6h or at port
- Propulsion management ¬I
  - Accident
  - Engine destruction
- Safety management ¬A
  - Accident + Uncontrolled incidents
- Safety management ¬I
  - Impaired decision-making
  - PAX accident (e.g. entrance in restricted area)
- Utilities management ¬A
  - Lack of critical resources >1 day
  - Fallback procedures
  - Lack of critical resources <1 day
- Utilities management ¬I
  - Crew health consequences (possibly leading to an accident)
  - PAX health consequences
  - Unhappy passengers
- Energy management ¬A
  - Accident (due to total blackout >1mn)
  - Energy limitations
- Energy management ¬I
  - System damage
- Navigation management ¬A
  - Accident (high traffic area or reduced visibility)
  - Unhappy passengers
  - Fallback procedures
- Navigation management ¬I
  - Accident

Reputation damage (in all columns, low severity)

Severity assessment of feared event impacts

(i.e. considering existing or already specified security measures)

2b

- Entertainment Internet access ¬A
  - PAX or crew complaints
- Customer data ¬P
  - Fine
- Sensitive data (VDR, exploitation) ¬C
  - Damaged reputation
- Sensitive data (VDR, exploitation) ¬I
  - No forensics
- GNSS ¬IA
  - Accident (high traffic area or reduced visibility)
  - Unhappy passengers
  - Fallback procedures
- Ext. VHF communications ¬I
  - Accident (high traffic area or reduced visibility)
  - Crew stress (if detected)
- Ext. VHF communications ¬A
  - Crew stress
  - Fallback procedures
- Other ext. communications ¬A
  - Crew stress
  - Fallback procedures
- Software maintenance and patching ¬A
  - Obsolete navigation charts (unknown)
  - Increased vulnerability
  - Obsolete navigation charts (known)
  - Entertainment issues
- Software maintenance and patching ¬I
  - Any critical system malfunction
  - Any non-critical system malfunction

4

Main supporting assets

System architecture

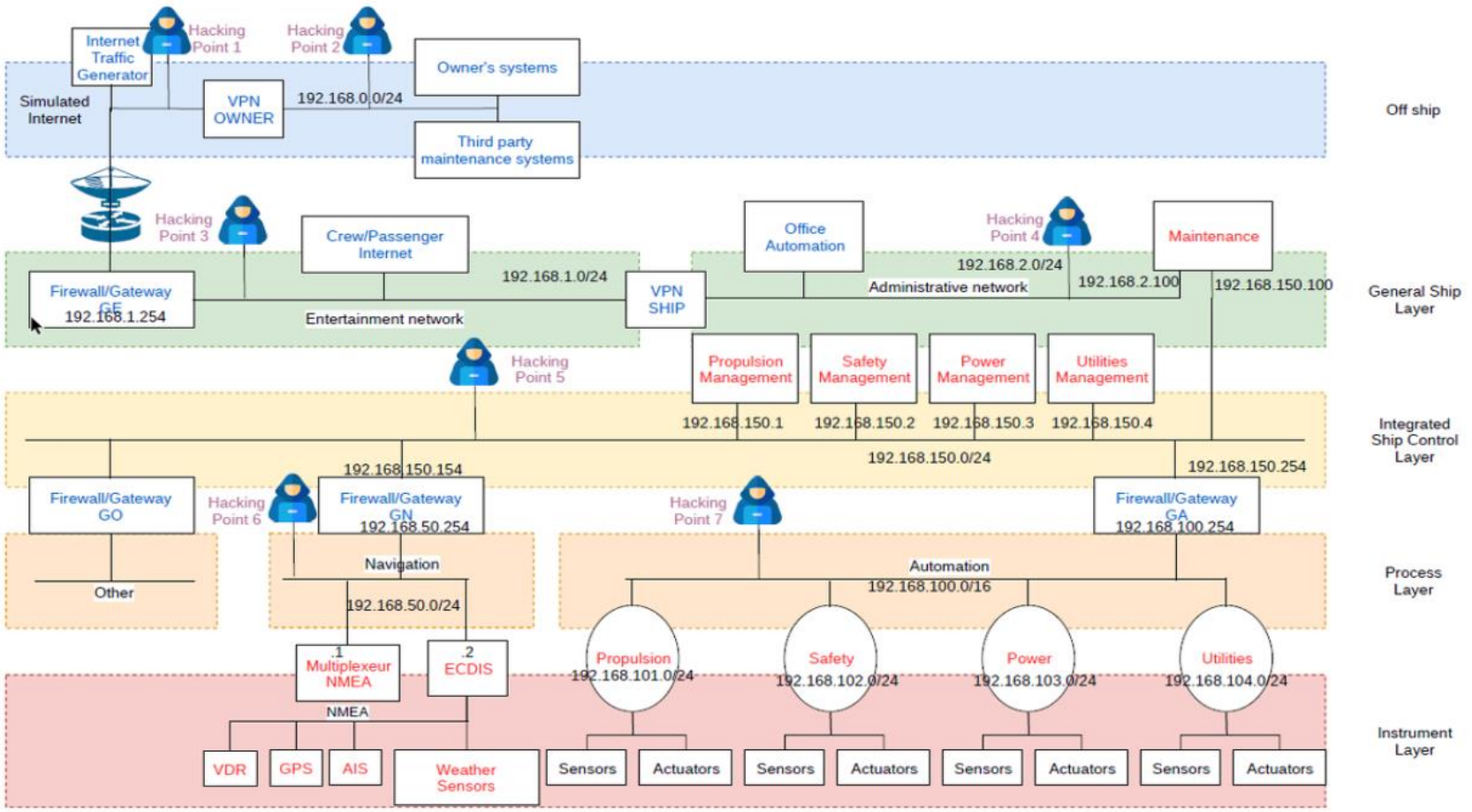
Captain

Crew

Organisation
(structure, human resources)

Information techn
(hardware, software, network

Crew BYOD



Information techn
(hardware, software, network

Physical
(premises, infrastructures)

Ship (premises)

5

Existing or already Specified Security Controls

(not part of previously mentioned Existing / Regulatory Set of Security Controls)

5

Existing or already Specified Security Controls on the Cyber-Range

(assessment of implementation status)

Technical protection measures	Procedural protection measures	Contingency management
R03 Secure management of confidential data	Physical network segregation	Visitors access control
	End-of-life equipment disposal, including data destruction	
R01/R02 Limitation to and control of network ports, protocols and services	R02 Secure password policy	R05 Ban visits to sensitive premises
R01/R02 Data recovery capability	R02 Cybersecurity awareness training	R01/R02 Secure upgrades and software maintenance (equipment)
R04 Customized web structure	R02/R07 Secure upgrades and software maintenance (malware)	Post-incidents cyber-investigation
R05 Physically block USB connector	Physical and removable media controls	Cyber-aware SMS
R06 Intrusion Detection System		
R02 Secure network physical layout	R05 Visitors accompanied in sensitive areas of ship	R02 Auditable events
R02 Email and web browser protection	R01/R02/R06/R07 Obtaining support from ashore and contingency plans	ALL Insurance coverage (for property damage and for liability)
R06 Secure satellite and radio communication	R04 Secure upgrades and software maintenance (web sites)	R06/R07 Crew takes manual control of the installation
R01/R02/R06 Network segmentation		R07 Crew switches off the PLCs
R01/R02/R07 Malware detection		R06 Crew cuts satellite connection
R04 Secure configuration for hardware and software		
CR Physical security (site perimeter fence, guards, locked door)	Registration upon site entrance	Visitors accompanied in restricted areas

Not implemente — Can be switched on or off at discretion — Fully implemented (cannot be switch off)

Not implemented — an be switched on or off at discretion — Fully lemented be switch off)

CR = Cyber-range only, not representative of ship conditions

Workshop n°2: Identification of adverse objectives

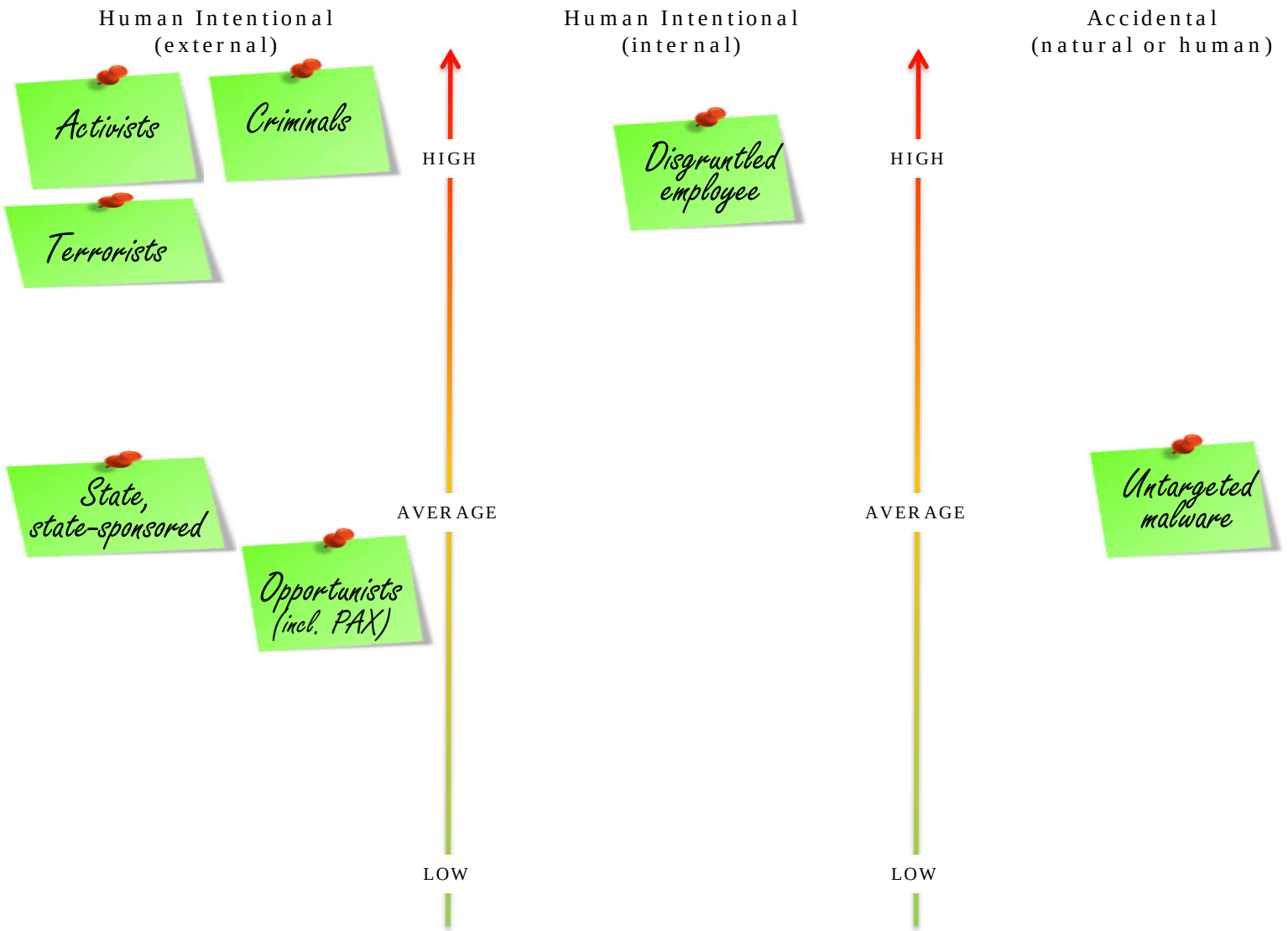
(2 hours to half-day session)

Rejected risk sources

Risk sources by attack likelihood

(considering motivation, current known activity, alternative easier attack paths, variety of risk source types...; ≠ attack success)

1



Rejected RS / TO

Retained Risk Source / Target Objectives

(i.e. considering security needs, and existing or already specified security measures)

2

(consider now)

- Criminals
  - Intelligence gathering
- Activists
  - R04 Publication of sensitive data
  - R03 Media attention
- Disgruntled employee
  - R04 Publication of sensitive data
  - R03 Media attention
- Criminals
  - R01/R02 Ransoming system operability
- Opportunists (incl. script kiddies)
  - R05 The challenge of getting through cyber security defenses
- Terrorists
  - R06/R07 Disruption to economies and critical national infrastructure

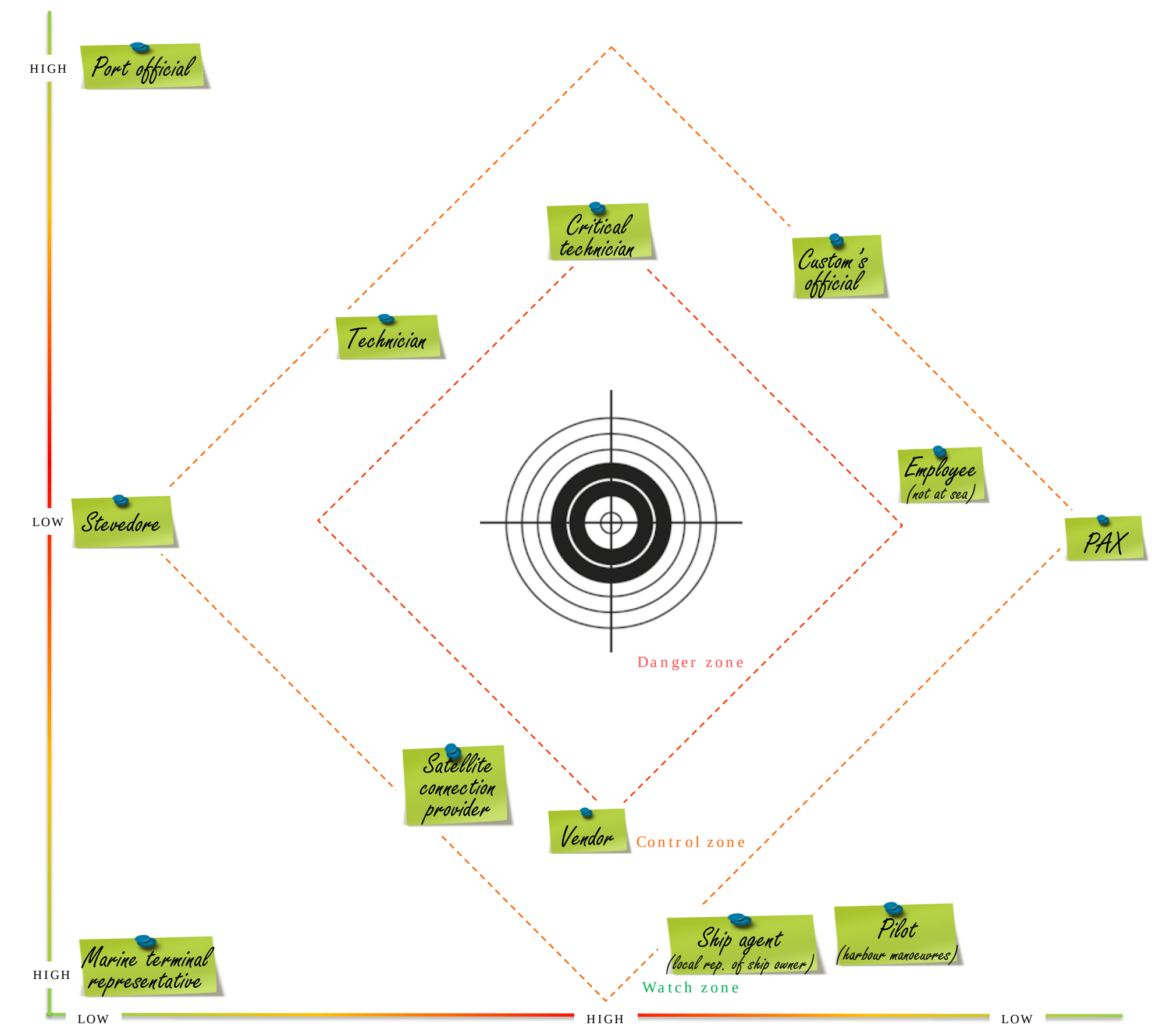
(consider later)

- Activists
  - Destruction of data
  - Denial of access to the targeted service or system
- Disgruntled employee
  - Destruction of data
  - Denial of access to the targeted service or system
- State, state-sponsored
  - Disruption to economies and critical national infrastructure
  - Political gain (through knowledge)
- Criminals
  - Arranging fraudulent cargo transportation
  - Selling stolen data
  - Ransoming stolen data
- Opportunists (incl. script kiddies)
  - Financial gain
- Terrorists
  - Political gain (through knowledge)
- Untargeted malware

1

Ecosystem

(i.e. dependency on participant, participant rights, participant maturity, trust in participant...)



3 Derived minimal set of security controls / security objectives on the ecosystem

(mitigation means based on security characterisation)

- ❑ ANSSI basic hygiene (standard)
- ❑ ANSSI basic hygiene (reinforced)
- ❑ ANSSI PSSIE
- ❑ CIS Controls
- ❑ ISA/IEC 62443-3-3 (SL1)
- ❑ ISA/IEC 62443-3-3 (SL2)
- ❑ ISA/IEC 62443-3-3 (SL3)
- ❑ ISA/IEC 62443-3-3 (SL4)
- ❑ ISO 27002
- ❑ NIST SP800-53 (low)
- ❑ NIST SP800-53 (moderate)
- ❑ NIST SP800-53 (high)

Expected from 3rd parties

R01/R07
Accreditation of technicians (checked by their company)

R06
Satellite provider security

Set by organisation under-study

IT control & registration of technicians' equipment (when boarding)

Weapons screening of PAX (when boarding)

2

Risks by impact severity

(i.e. high-level scenarios leading to the realisation of adverse objectives; cover all primary assets & all critical participants, no more than 3 per RO/TO pair)

Integrity

RO6 Terrorists create a major accident by taking remotely control of the ship **navigation** (via the satellite connection)

RO7 Terrorists create a major accident by triggering a logical bomb aboard the ship (**navigation** or **propulsion**) by leveraging the work of a critical technician

Availability

RO1 Criminals ransom an ICS operability (**navigation**, **propulsion**, **safety**, **utilities** or **energy**) by corrupting a technician to plant a ransomware

RO2 Criminals ransom an ICS operability (**navigation**, **propulsion**, **safety**, **utilities** or **energy**) by boarding as a PAX and planting a ransomware

RO5 For the challenge, an opportunist destroys an ICS (**navigation**, **propulsion**, **safety**, **utilities** or **energy**) by planting corrupted hardware (e.g. USB killer)

Confidentiality

RO3 A disgruntled employee accesses and discloses **sensitive data** by taking pictures of screens, or accessing files

Privacy

RO4 Activists attract media attention by publishing crew-related **sensitive data** by attacking the web-site

(consider now)
(consider later)

Postponed risks

Rejected risks

Cyber kill chain

System mode: *Operational*

R01

Ext. recognition	Intrusion	Int. recognition	Move laterally	Exploitation
Success likelihood: L3	Likelihood: L3	Likelihood: L2	Likelihood: L1	Likelihood: L1
Threat actors	Criminal	Technician	Ransomware	Ransomware	Ransomware
Existing measures	Accreditation of technicians (checked by their company)	Physical security	Network segmentation Malware detection	Obtaining support from ashore and contingency plans Insurance coverage (for property damage and for liability)
Scenarios	Social engineering OSINT on ship design OSINT on ship crew Criminal corrupts technician to plant a ransomware	Plant ransomware on IT network	Map network, find route to ICS network	Move to ICS network	Encrypt PLC software Encrypt bridge HMI
Proposed measures			Limitation to and control of network ports, protocols and services	Secure upgrades and software maintenance (equipment) Data recovery capability

System mode: *Maintenance / operational*

R05

Ext. recognition	Intrusion	Int. recognition	Move laterally	Exploitation
Success likelihood: ...%	Likelihood: L3	Likelihood: ...%	Likelihood: ...%	Likelihood: L3
Threat actors		Opportunist (maintainer or PAX)			USB killer
Existing measures		Physical security Visitors accompanied in sensitive areas of ship		Insurance coverage (for property damage and for liability)
Scenarios		Participate to a ship visit Plug a USB killer on the maintenance computer		Destroy the maintenance computer
Proposed measures		Ban visits to sensitive premises		Physically block USB connector

Workshop n°4: Risk evaluation at technical-level

(1 to 3 half-day sessions)

Cyber kill chain

System model: Operational

R02

Ext. recognition	Intrusion	Int. recognition	Move laterally	Exploitation
Success likelihood: L4	Likelihood: L3	Likelihood: L2	Likelihood: L2	Likelihood: L2

Threat actors

- Criminal
- Crew
- Criminal
- Criminal
- Ransomware

Existing measures

- Malware detection
- Email and web browser protection
- Auditable events
- Network segmentation
- Auditable events
- Obtaining support from ashore and contingency plans
- Malware detection
- Insurance coverage (for property damage and for liability)

Scenarios

- Board as a passenger
- OSINT on ship design
- Phishing
- Mail poisoning
- Gain insight on equipment specifications & crew authorisations
- Blackmail crew to get credentials to admin network
- Access to the entertainment network
- Eavesdrop then brute-force credentials
- Access to the administrative network (maintenance position)
- Scan network
- Access to the automation network
- Encrypt PLC software
- Encrypt bridge HMI

Proposed measures

- Secure upgrades and software maintenance (malware)
- Secure password policy
- Cybersecurity awareness training
- Physical network segregation
- Limitation to and control of network ports, protocols and services
- Data recovery capability
- Secure upgrades and software maintenance (equipment)

Cyber kill chain

System mode: Operational

R03

Ext. recognition | Intrusion | Int. recognition | Move laterally | Exploitation

Success likelihood: | Likelihood: L4 | Likelihood: | Likelihood: | Likelihood: L4

Threat actors: | Disgruntled employee | | | Disgruntled employee

Existing measures: | Physical security; Auditable events | | Auditable events | Insurance coverage (for property damage and for liability)

Scenarios: Take pictures of software versions, emails, pwds, architecture, whiteboards, papers... | Record discussions | Copy files, steal physical documents... → Disclose sensitive data

Proposed measures: Secure management of confidential data

System mode: Operational

R04

Ext. recognition | Intrusion | Int. recognition | Move laterally | Exploitation

Success likelihood: L4 | Likelihood: L3 | Likelihood: L3 | Likelihood: L2 | Likelihood: L2

Threat actors: Activists | Activists | Crawler | Activists | Activists

Existing measures: Secure configuration for hardware and software | Secure upgrades and software maintenance (web sites)

Scenarios: Gather information on web-site → Exploit web-site vulnerability → Crawl web-site → Explore unreferenced pages → Disclose crew-related sensitive data

Proposed measures: Customized web structure

Cyber kill chain

System mode: Operational (e.g. manoeuvring in port)

R06

Ext. recognition → Intrusion → Int. recognition → Move laterally → Exploitation

	Ext. recognition	Intrusion	Int. recognition	Move laterally	Exploitation
Success likelihood / Likelihood	L4	L2	L2	L1	L1
Threat actors	Terrorist	Terrorist	Terrorist	Terrorist	Terrorist
Existing measures		Satellite provider security Secure satellite and radio communication	Network segmentation	Crew takes manual control of the installation * Crew cuts satellite connection Obtaining support from ashore and contingency plans	
Scenarios	OSINT on ship	Connect to the ship via satellite connection system	Map the networks, find a path to the bridge	Move to the bridge Take control of ship	Send ship against a wharf or another ship
Proposed measures		Intrusion Detection System			Insurance coverage (for property damage and for liability)

System mode: Maintenance then Operational (e.g. manoeuvring in port, or at sea in a rocky area)

R07

Ext. recognition → Intrusion → Int. recognition → Move laterally → Exploitation

	Ext. recognition	Intrusion	Int. recognition	Move laterally	Exploitation
Success likelihood / Likelihood	L2	L2			L2
Threat actors	Terrorist	Critical technician			Logical bomb
Existing measures	Accreditation of technicians (checked by their company)	Malware detection		Obtaining support from ashore and contingency plans Crew switches off the PLCs Crew takes manual control of the installation *	Insurance coverage (for property damage and for liability)
Scenarios	OSINT on ship and crew Corrupt critical technician Find/adapt malware	Install script on maintenance PC that infinitely switches on/off the PLCs Change PLC firmware		Self-activate script based on ship position / speed, time, email... Malfunction or destruction of actuators	Accident
Proposed measures		Secure upgrades and software maintenance (equipment, malware)			

*: in the future, this may not be an option anymore.

List of risks

(include at least threat source, primary asset, feared event, supporting asset, and exploited vulnerability inside risk description)

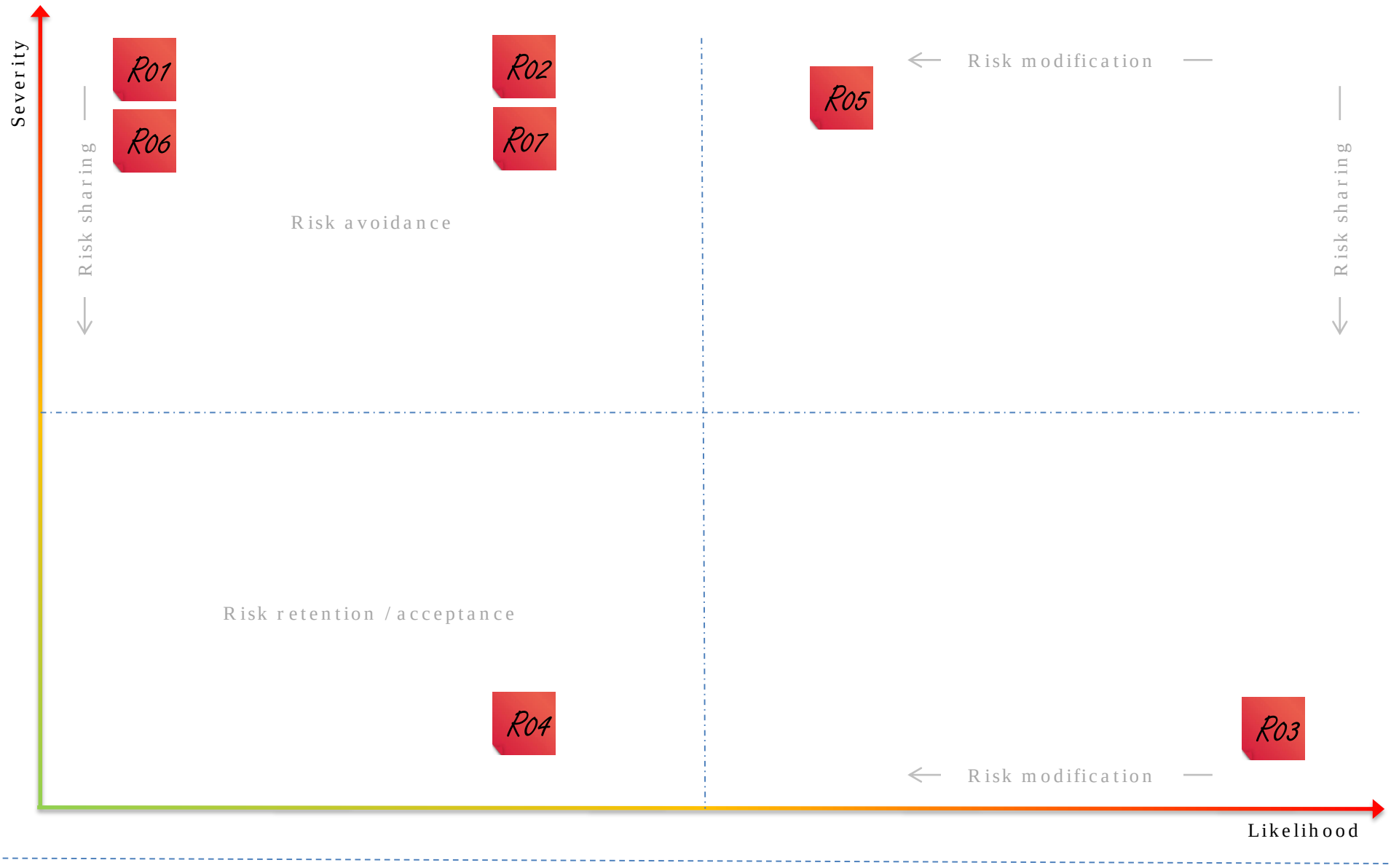
Risk n°	Risk description	Risk owner	Comment
R01	Rather unlikely that criminals corrupt a technician so that the latter plants a ransomware, leading to the loss of an ICS operability (navigation, propulsion, safety, utilities or energy) and thereof high severity impacts (i.e. accident)	Ship manager	High severity Rather unlikely
R02	Likely that criminals board as PAX and plant a ransomware, leading to the loss of an ICS operability (navigation, propulsion, safety, utilities or energy) and thereof high severity impacts (i.e. accident)	Ship manager	High severity Likely
R03	Certain that a disgruntled employee accesses sensitive operational data, e.g. by taking pictures of screens, or accessing files, and then discloses this information, damaging the ship's reputation	Ship manager	Low severity Certain
R04	Likely that activists attack the web-site and disclose crew-related sensitive data to attract media attention	Ship manager	Compromises privacy Low severity Likely
R05	Very likely that, for the challenge, an opportunist destroys an ICS by planting corrupted hardware (e.g. USB killer)	Ship manager	High severity Very likely
R06	Rather unlikely that, when the ship is manoeuvring in port, terrorists take remote control of the ship (navigation), via the satellite connection, to create send the ship against a wharf or another ship	Ship manager	High severity Rather unlikely
R07	Likely that, when the ship is manoeuvring in port, or at sea in a rocky area, terrorists trigger a logical bomb aboard the ship (by leveraging the work of a critical technician), to create an accident	Ship manager	High severity Likely

Operational scenario likelihood scale

SCALE	DEFINITION
L4 – CERTAIN OR ALREADY OCCURRED	The risk origin will certainly reach its target objective by one of the considered methods of attack OR such a scenario has already occurred within the organisation (incident history).
L3 – VERY LIKELY	The risk origin will most probably reach its target objective by one of the considered methods of attack.
L2 – LIKELY	The risk origin is able to reach its target objective by one of the considered methods of attack.
L1 – RATHER UNLIKELY	The risk origin has little chance of reaching its objective by one of the considered methods of attack.

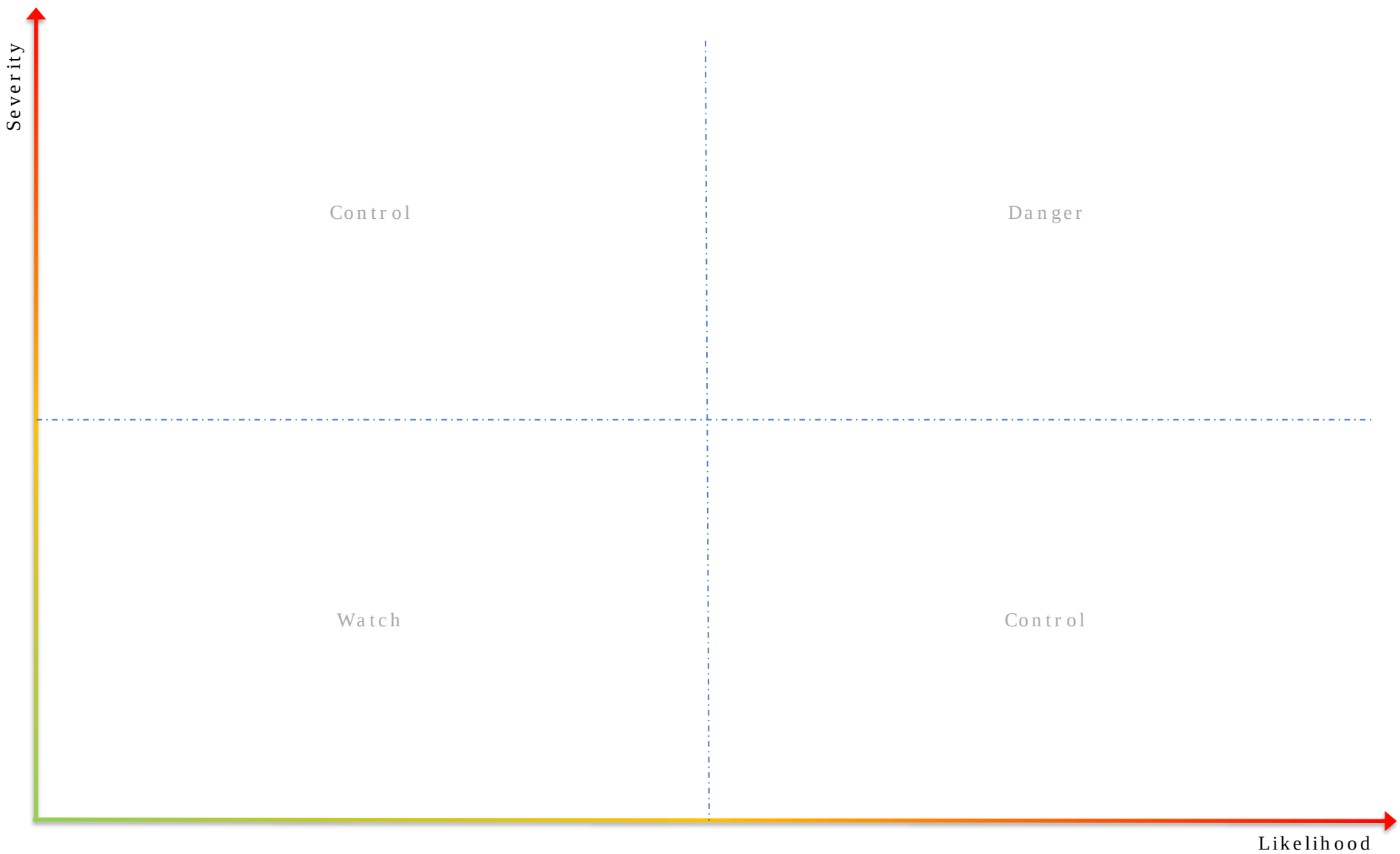
Synthesis of inherent / initial risks

1



Synthesis of residual risks

3



Conclusions

- The key business assets all relate to the ferry navigation mission, with integrity and availability security needs. Business assets related to good transport conditions and recreational internet access appear as secondary concerns.
- The synthesis of existing security controls was not easy to draw because it was unclear whether the synthesis should be representative of Ecole Navale's cyber-range, or a typical ferry boat or the best-of-class ferry. The current synthesis is representative of Ecole Navale's cyber-range, capturing: (i) the unavoidable security controls, i.e. the controls related to the military premises where the cyber-range is installed; (ii) the security controls that can be switched on or off at will on the cyber-range; and (iii) the security controls that may exist on certain ships but are not implemented in the scope of the cyber-range. Colour coding is used to specify if the security controls were considered as existing or not in the attack scenarios (see workshop 4).
- The risk sources (RS) that have been identified as the most relevant are criminals, terrorists, activists, and disgruntled employees. Activists and disgruntled employees were grouped, the hypothesis being that they have similar goals, centred on private or confidential data, i.e. not targeting the integrity or availability of the ferry navigation supporting assets. Even though significantly less relevant, an attack by an opportunist was short-listed, because assumed to use radically different attack techniques. To allow for a quick first iteration, only 5 target objectives (TO) were selected, whilst 9 others were identified but postponed to a later risk assessment iteration. This selection allows for a pretty good coverage of the business assets.
- The mapping of the ecosystem shows no critical participant. However, the ship is highly dependent on some participants, in particular (critical) technicians, the satellite connection provider and ICS vendors. Very few security controls were defined on the ecosystem, most of which relate to physical security. It seems that the security of the participants is left to the participants themselves. There is room here for significant improvement in the naval business.
- Based on the 5 RS/TO couples, 7 strategic scenarios were defined, 5 of which have a high severity. The 2 others have a low severity, and unsurprisingly relate to the activists / disgruntled employees.
- Attack scenarios triggered by criminals (R01, R02) were found to have a low to medium-low likelihood of success, because they target navigation-related supporting assets, which are difficult to access, both physically and remotely. The attack scenario triggered by the disgruntled employee (R03) was found to have a high likelihood of success, because of the insider nature of the attacker, providing him both with trust and multiple opportunities to act; the same scenario run by an activist would be significant less likely, and has therefore been dismissed. The attack scenario triggered by an activist (R04) was found to have a medium-low likelihood of success, because of the difficulty of finding relevant sensitive data; by contrast, the same scenario run by a disgruntled employee would be significant more likely, but has been dismissed due to its similarity to R03. The attack scenario triggered by the opportunist (R05) was found to have a medium-high likelihood of success, however, in the synthesis of inherent risks, the overall likelihood is degraded to medium-low, due to the medium-low relevance of this risk source (see workshop 2). Finally, the attack scenarios triggered by terrorists (R06, R07) are similar to R01 & R02 in that they target navigation-related supporting assets, which are difficult to access. This closes the 1st goal of this study, i.e. to identify platform runtime vulnerabilities & threats.
- To proceed with the 2nd goal of this study, i.e. provide rational inputs to generate scenarios for the Foresight naval pilot, it was decided to short-list the 4 most critical risks, i.e. R02, R03, R05 and R07. The follow-up work is to be performed as part of WP8.

Contributors

David BROSSET (EN); Clet BOUDEHENNE (EN); Nicolas PELISSERO (EN); Douraid NAOUAR (EN); Maxence LANNUZE (EN); Mickael BERVAS (EN), Olivier JACQ (EN), Stéphane PAUL (Thales)