Future of Maritime Autonomy

Cybersecurity, Trust and Mariner’s Situational Awareness

Authors

Juan Dorje Palbar

Dr Rory Hopcraft

Dr Kimberly Tam

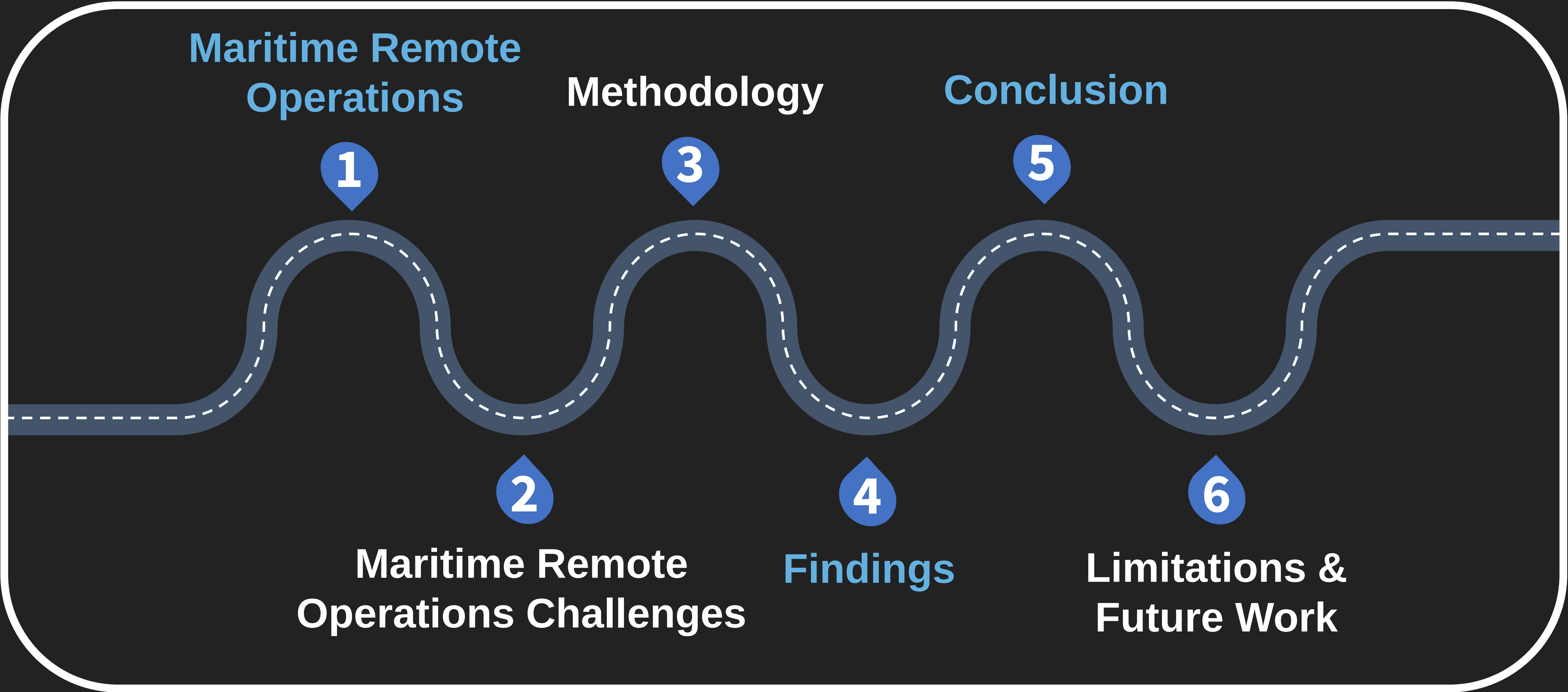
UNIVERSITY OF PLYMOUTH

Cyber-SHIP Lab
SECURING MARITIME

Cyber MAR

REARDON SMITH
NAUTICAL TRUST

Outline of the Presentation



1 Maritime Remote Operations

2 Maritime Remote Operations Challenges

3 Methodology

4 Findings

5 Conclusion

6 Limitations & Future Work

Maritime Remote Operations

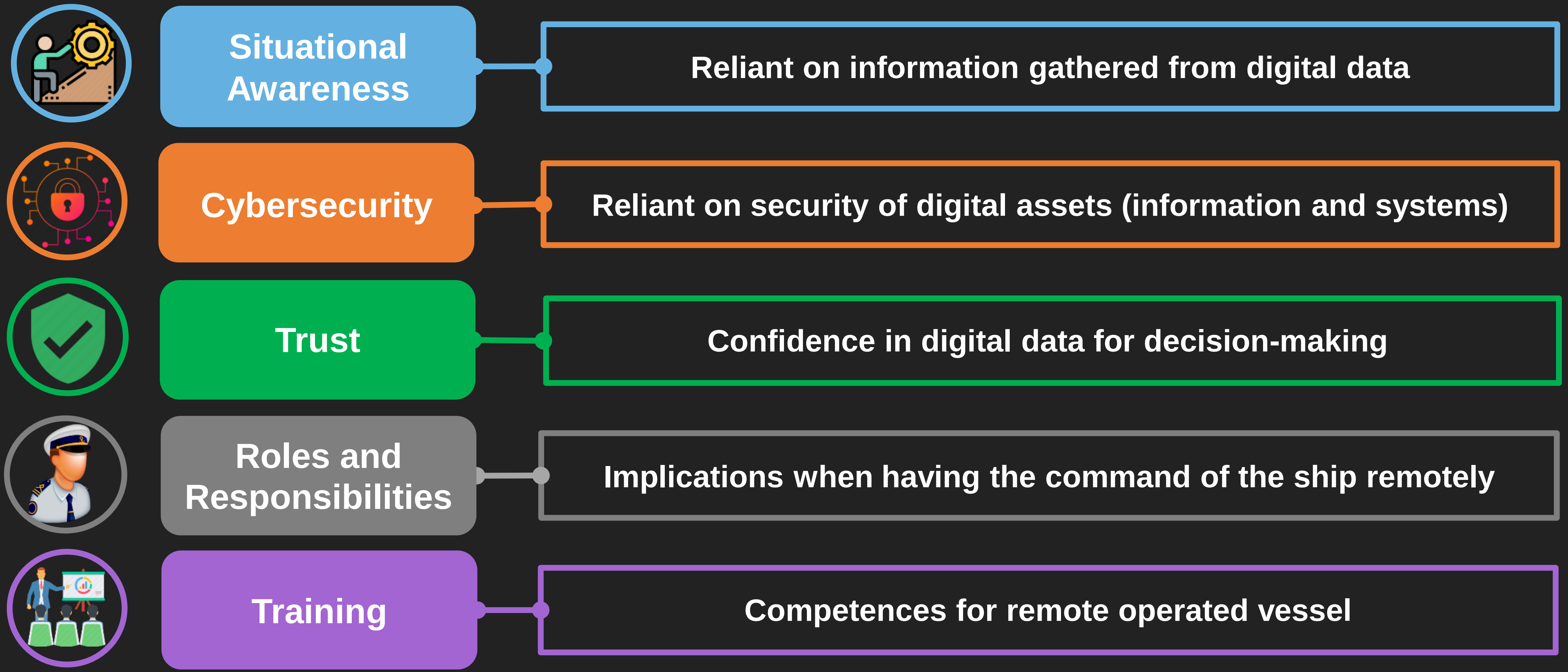
Source: (Kon, 2022)

- Remote operations reliant on **digital data**.
- The issue and the importance of the **human element** especially for remote operations.
- **New operational risks** are introduced.
- Misalignment between organisations innovation strategies to their **machine operator** work processes to achieve fully **autonomous vessels**.

Source: (Mtiinstruments, 2022)

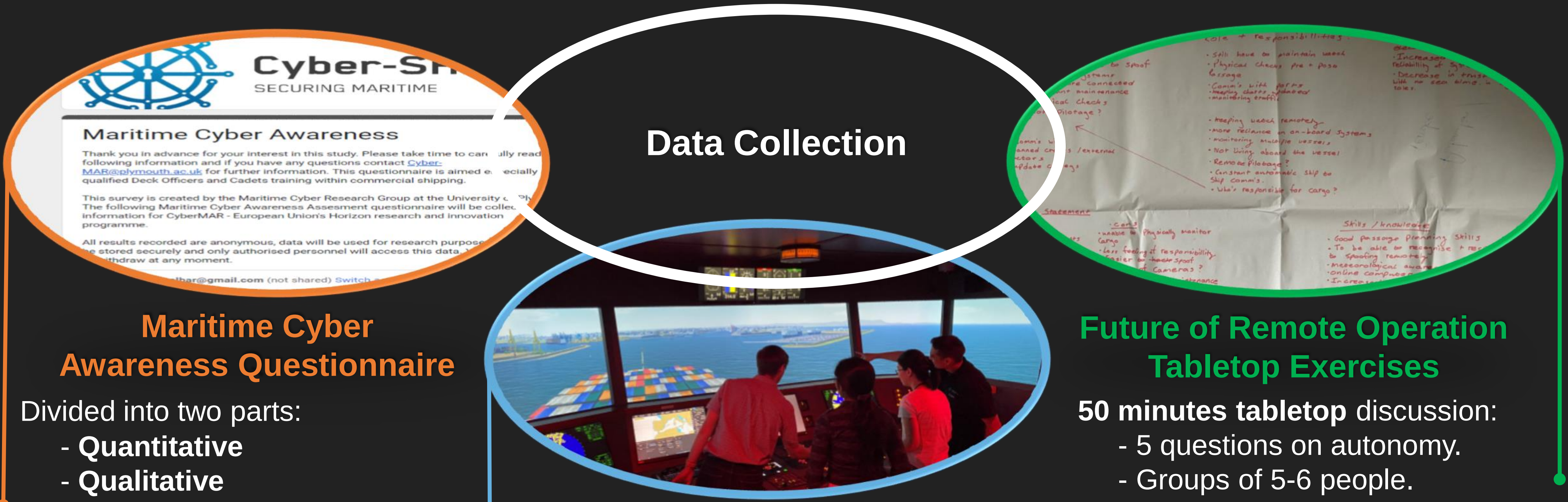
Automation Conundrum *or “****Human-in-the loop****”*

Maritime Remote Operations Challenges



Situational Awareness	Reliant on information gathered from digital data
Cybersecurity	Reliant on security of digital assets (information and systems)
Trust	Confidence in digital data for decision-making
Roles and Responsibilities	Implications when having the command of the ship remotely
Training	Competences for remote operated vessel

Methodology



Cyber-SH
SECURING MARITIME

Maritime Cyber Awareness

Thank you in advance for your interest in this study. Please take time to care ully read following information and if you have any questions contact Cyber-MAR@plymouth.ac.uk for further information. This questionnaire is aimed e ecially qualified Deck Officers and Cadets training within commercial shipping.

This survey is created by the Maritime Cyber Research Group at the University c Ply The following Maritime Cyber Awareness Assesment questionnaire will be collec information for CyberMAR - European Union's Horizon research and innovation programme.

All results recorded are anonymous, data will be used for research purpose e stored securely and only authorised personnel will access this data. ithdraw at any moment.

lbar@gmail.com (not shared) Switch a

Data Collection
Role + responsibilities
• Still have to maintain watch
• Physical checks pre + post passage
• Comm's with ports
• keeping charts updated
• monitoring traffic
• keeping watch remotely
• more reliance on on-board systems
• monitoring multiple vessels
• Not living aboard the vessel
• Remote Pilotage?
• Constant automatic ship to ship comm's.
• Who's responsible for cargo?
• Increased reliability of sy
• Decrease in trust
Statement
• Cons
• unable to physically monitor cargo
• Less feeling of responsibility
• Easier to hack spoof
Cameras?
Skills / knowledge
• Good passage planning skills
• To be able to recognise + re to spoofing remotely
• Meteorological awar
• online compute
• Increas

Maritime Cyber Awareness Questionnaire

Divided into two parts:

- **Quantitative**
- **Qualitative**

Full Bridge Cyber-attack Simulation Exercises

20-minute simulation exercises:

- **GNSS drift** in a TSS.
- **Loss** of **rudder** and **engine** control inbound passage to port.

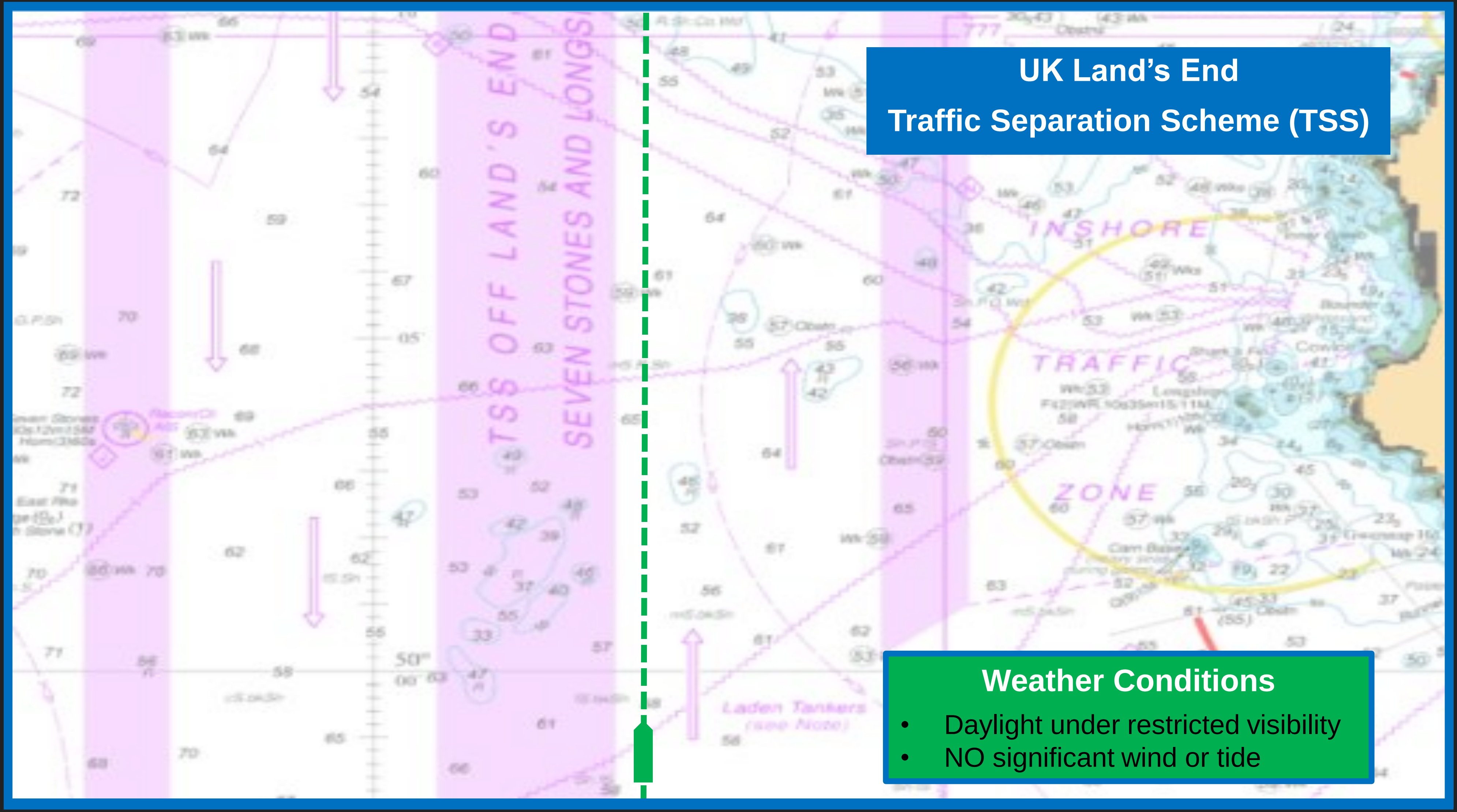
Future of Remote Operation Tabletop Exercises

50 minutes tabletop discussion:

- 5 questions on autonomy.
- Groups of 5-6 people.

Participants:
75 Navigators
(Cadet → Senior Officers)

1st Scenario – GNSS Spoofing



UK Land's End

Traffic Separation Scheme (TSS)

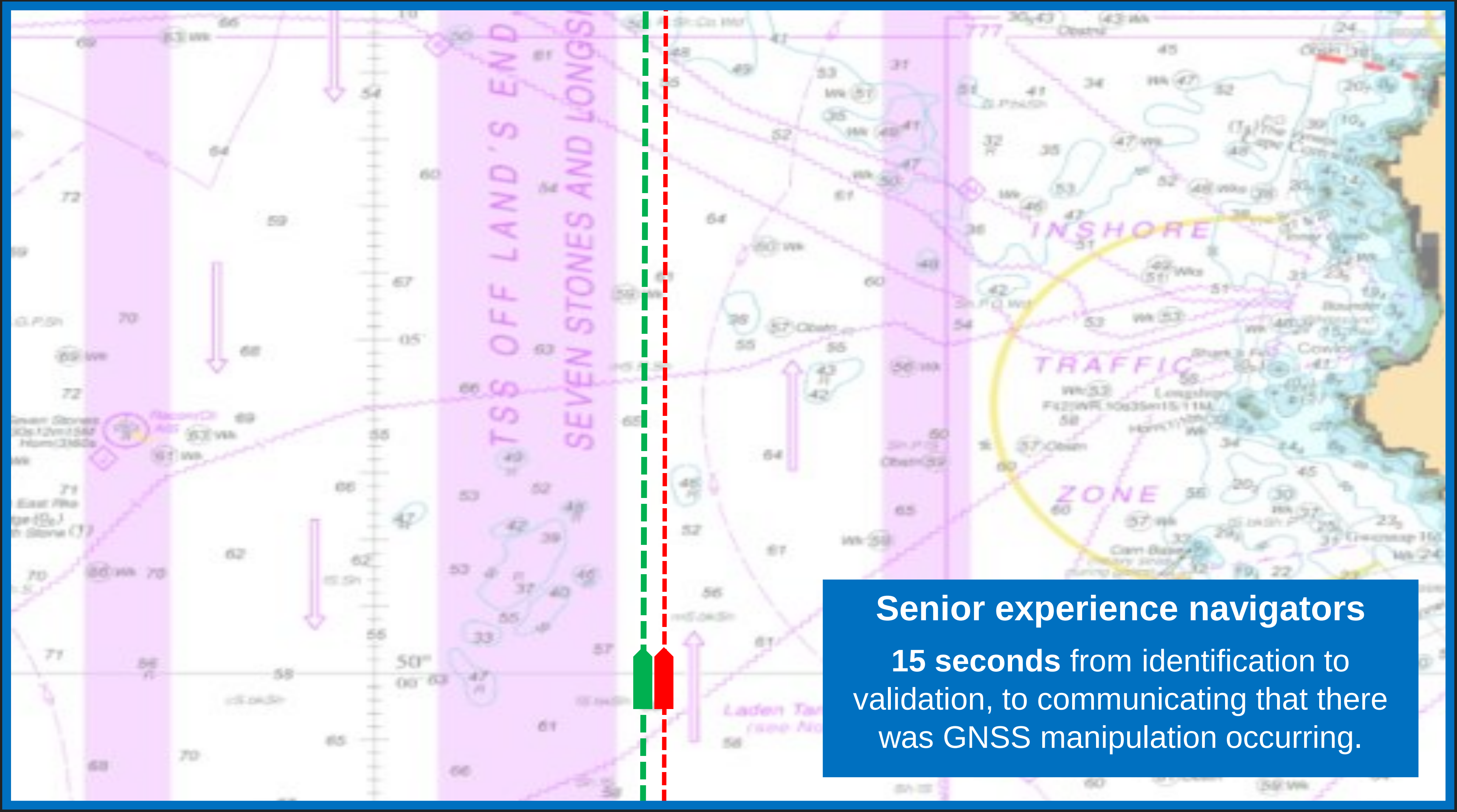
Weather Conditions

- Daylight under restricted visibility
- NO significant wind or tide

TIME

DRIFT

1st Scenario – GNSS Spoofing



Senior experience navigators

15 seconds from identification to validation, to communicating that there was GNSS manipulation occurring.

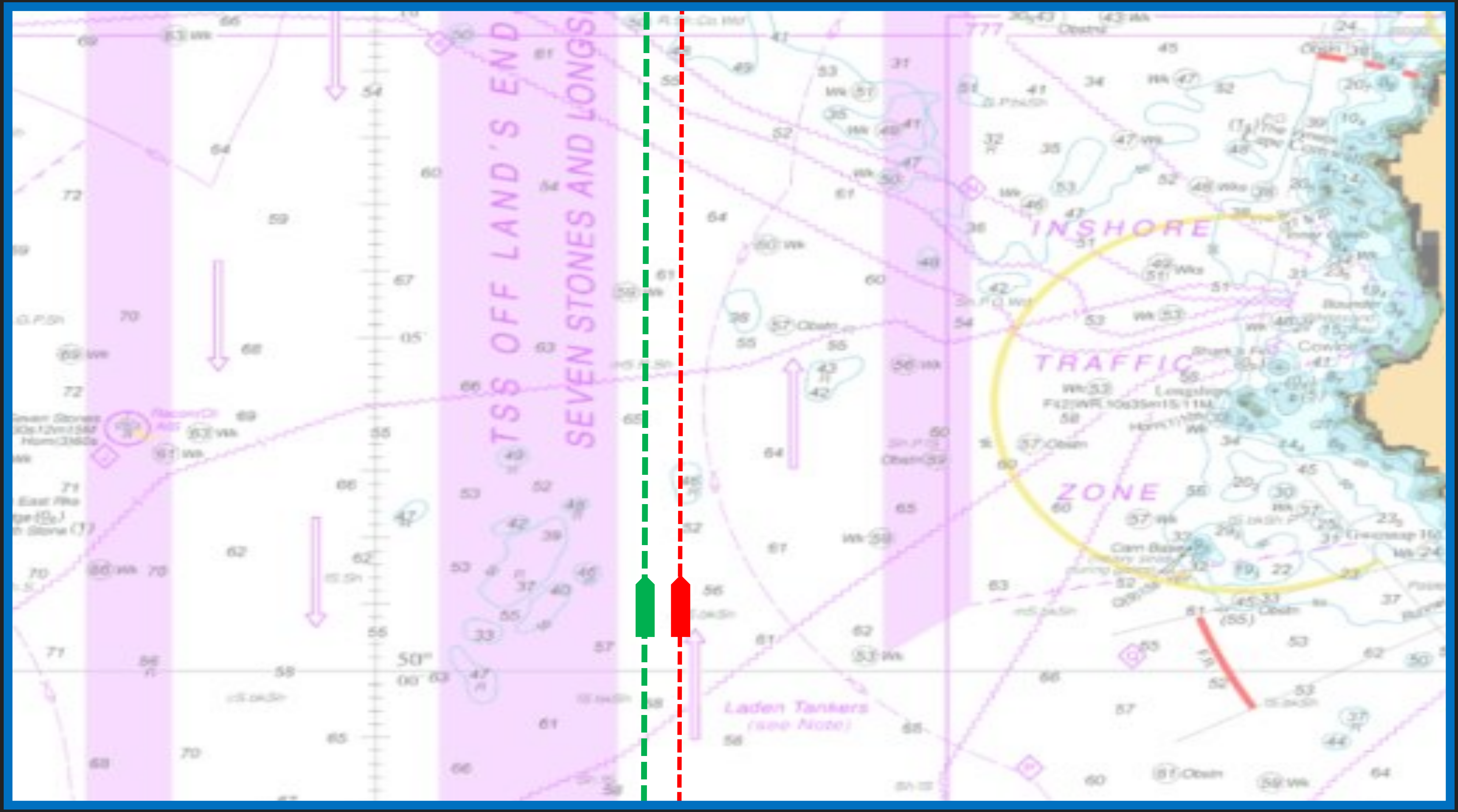
TIME

2 minutes

DRIFT

300m

1st Scenario – GNSS Spoofing



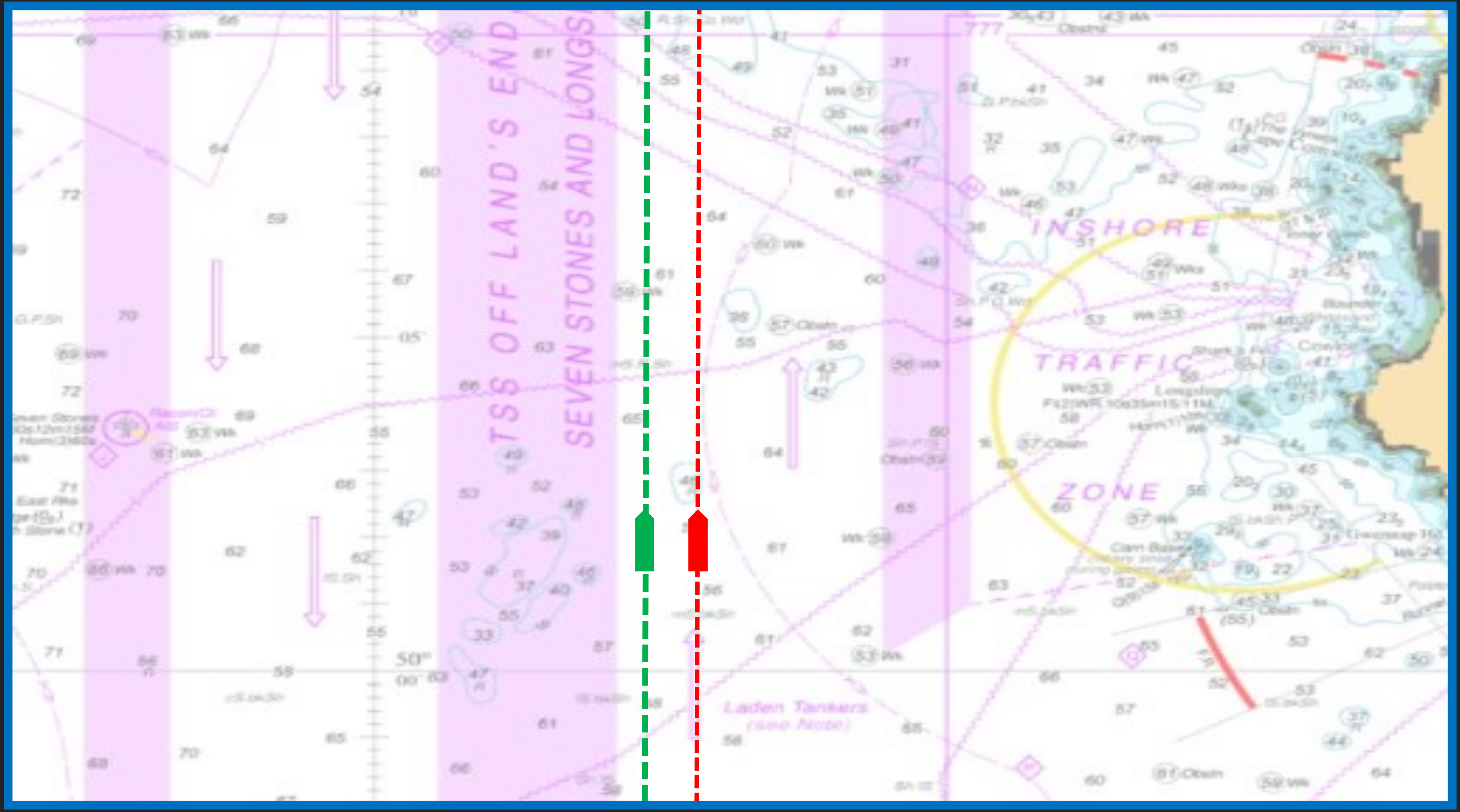
TIME

4 minutes

DRIFT

600m

1st Scenario – GNSS Spoofing



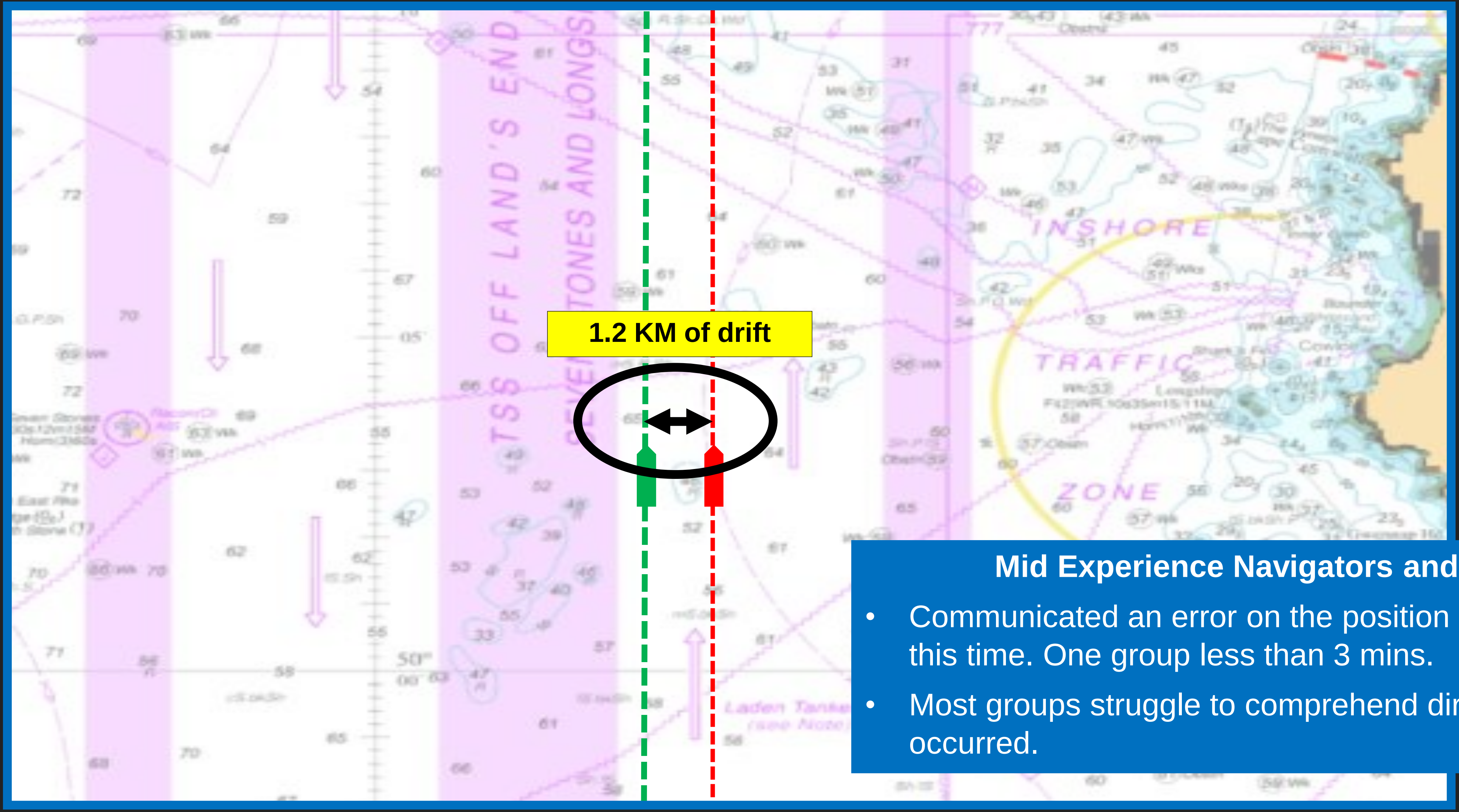
TIME

6 minutes

DRIFT

900m

1st Scenario – GNSS Spoofing



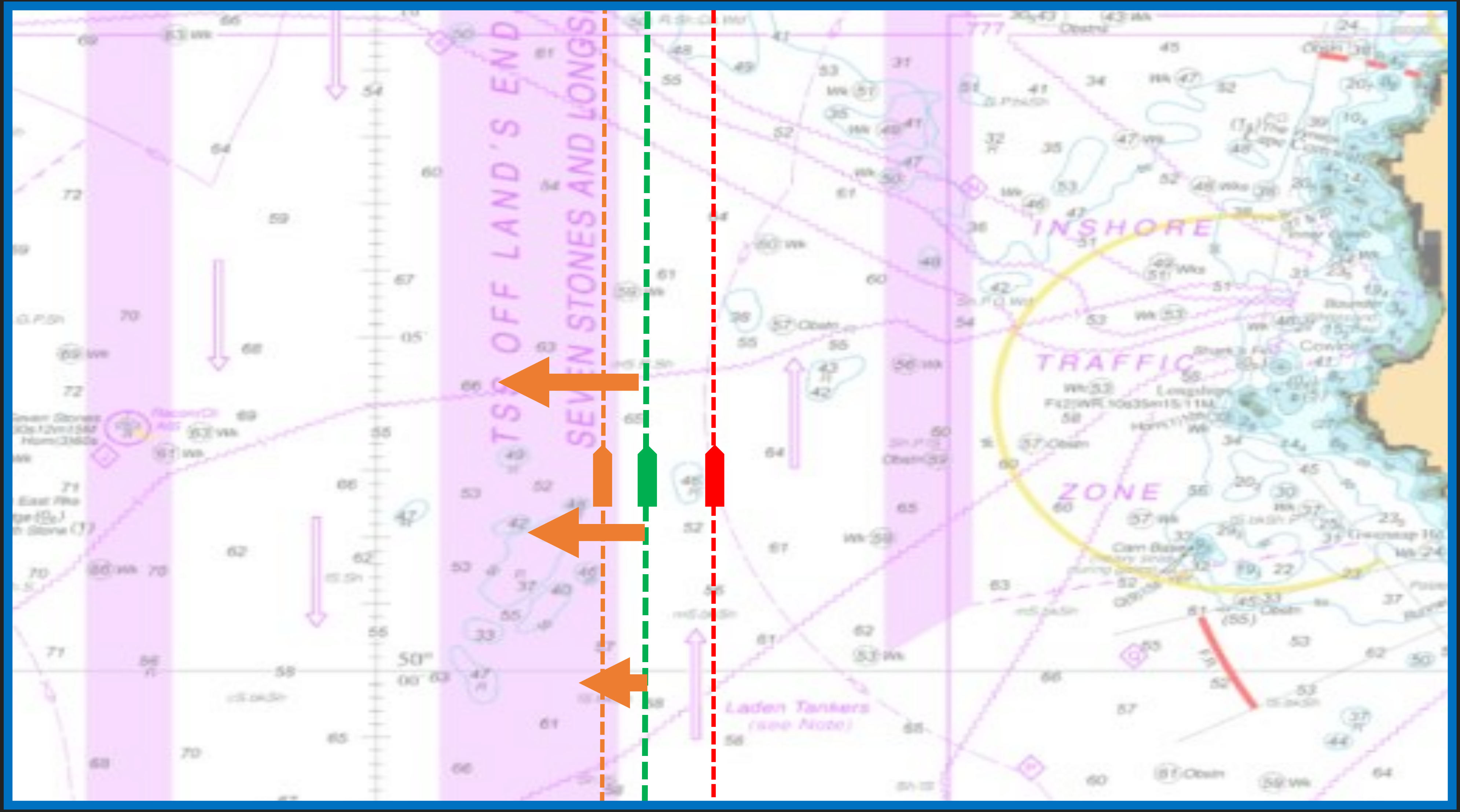
TIME

8 minutes

Mid Experience Navigators and Cadets

- Communicated an error on the position on average at this time. One group less than 3 mins.
- Most groups struggle to comprehend direction spoofing occurred.

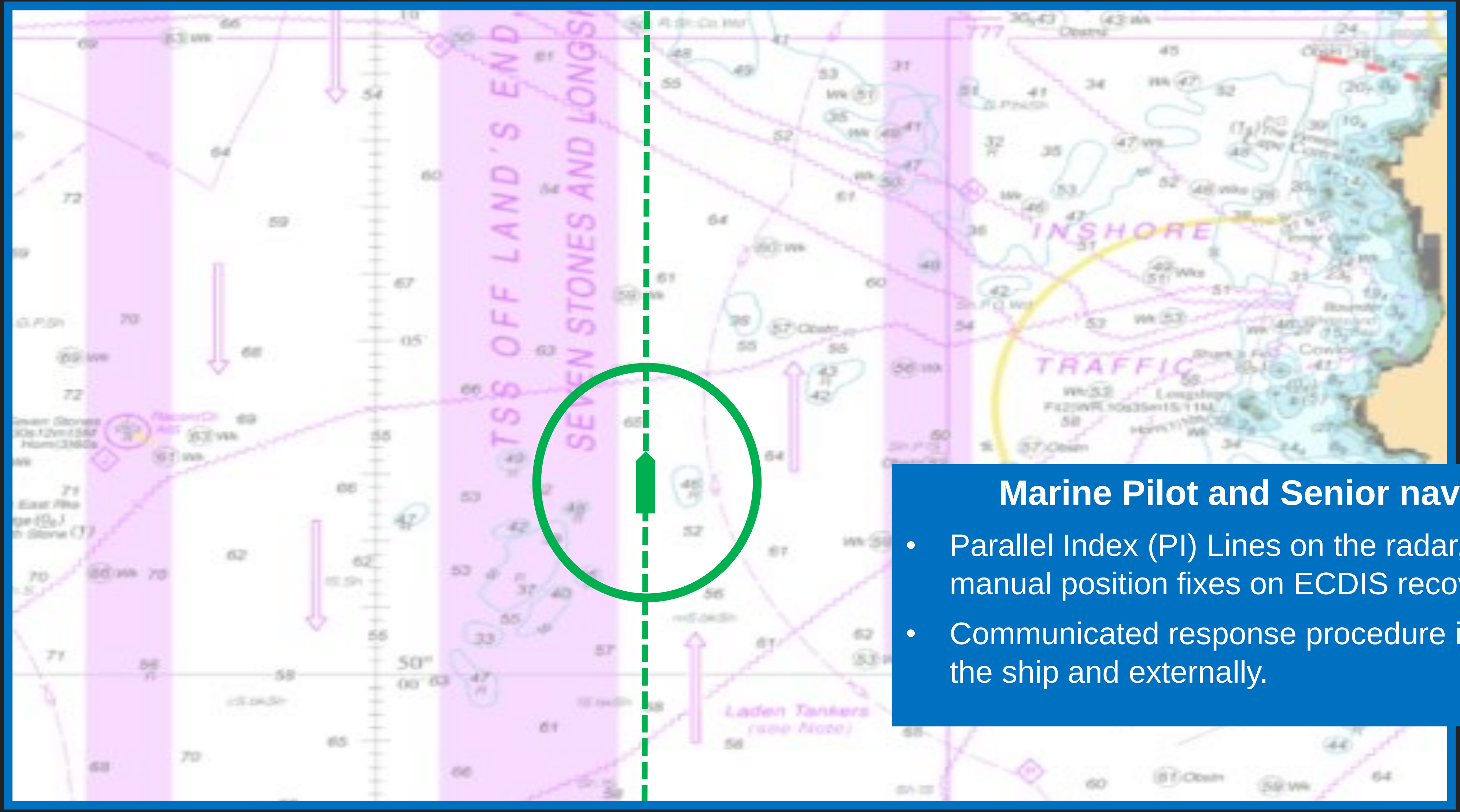
1st Scenario – GNSS Spoofing



TIME

8 minutes

1st Scenario – GNSS Spoofing



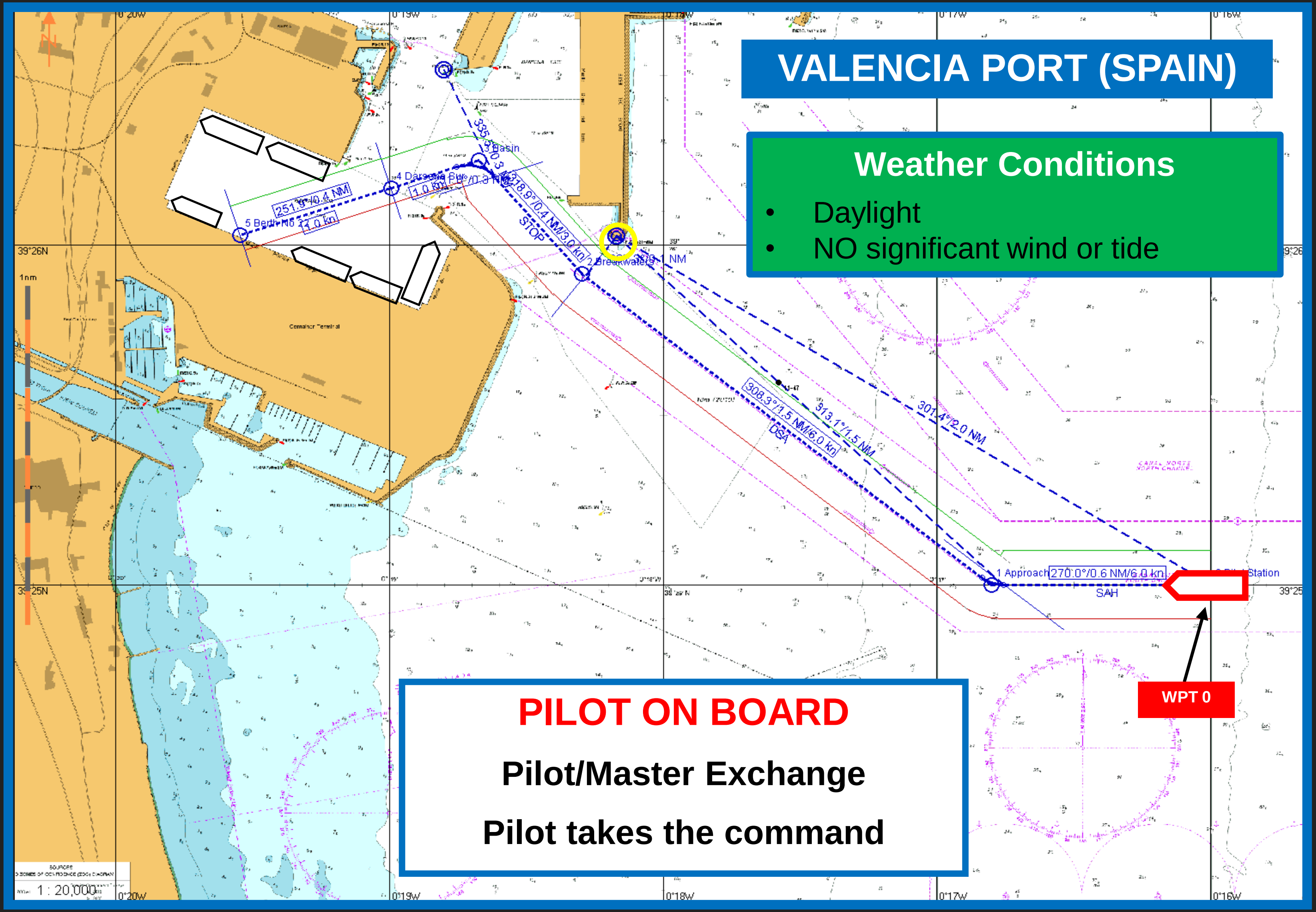
TIME

8 minutes

Marine Pilot and Senior navigators

- Parallel Index (PI) Lines on the radar, and taken manual position fixes on ECDIS recovering full SA.
- Communicated response procedure internally within the ship and externally.

2nd Scenario Rudder and Engine Jamming



VALENCIA PORT (SPAIN)

Weather Conditions

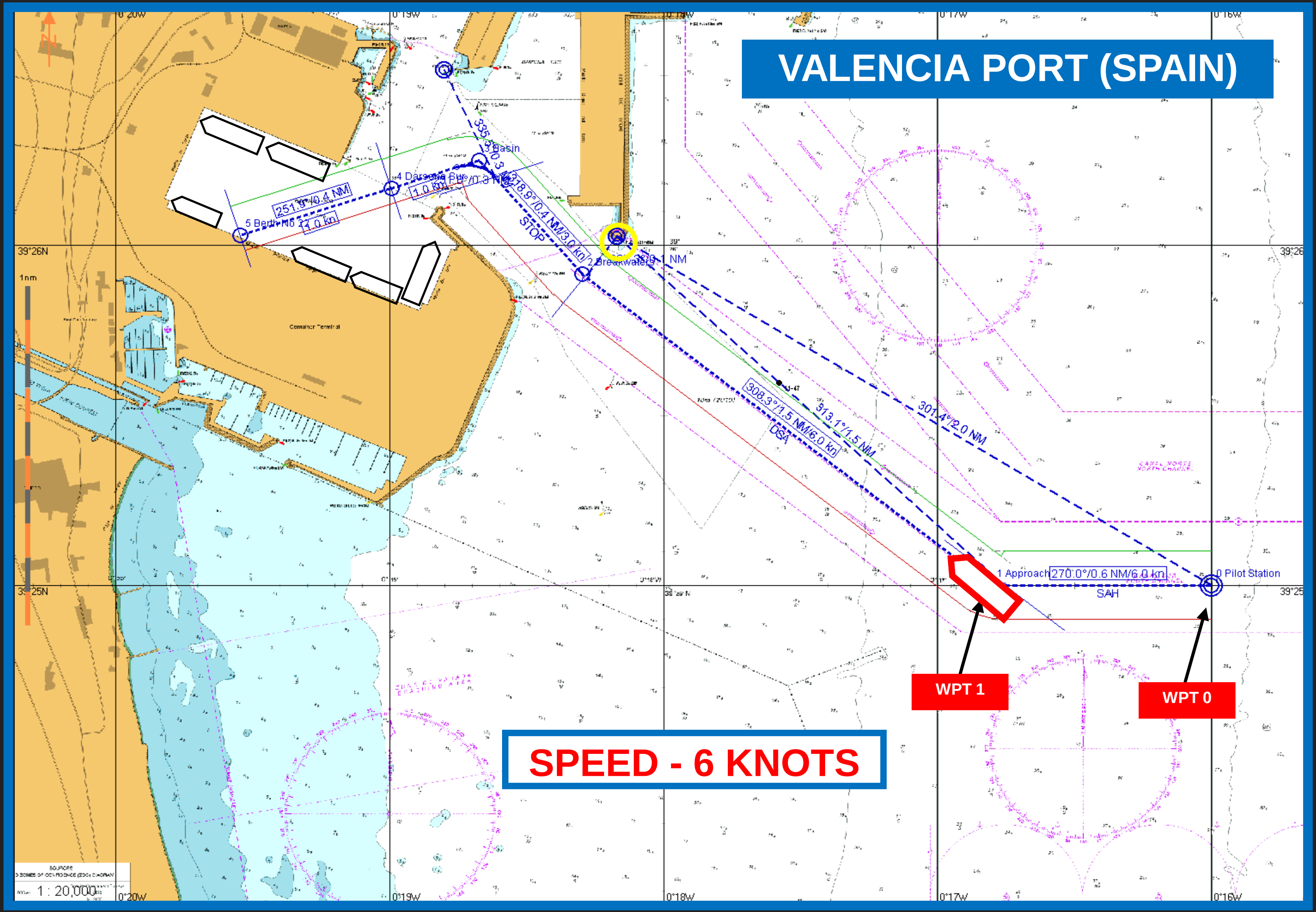
- Daylight
- NO significant wind or tide

PILOT ON BOARD

Pilot/Master Exchange

Pilot takes the command

2nd Scenario Rudder and Engine Jamming



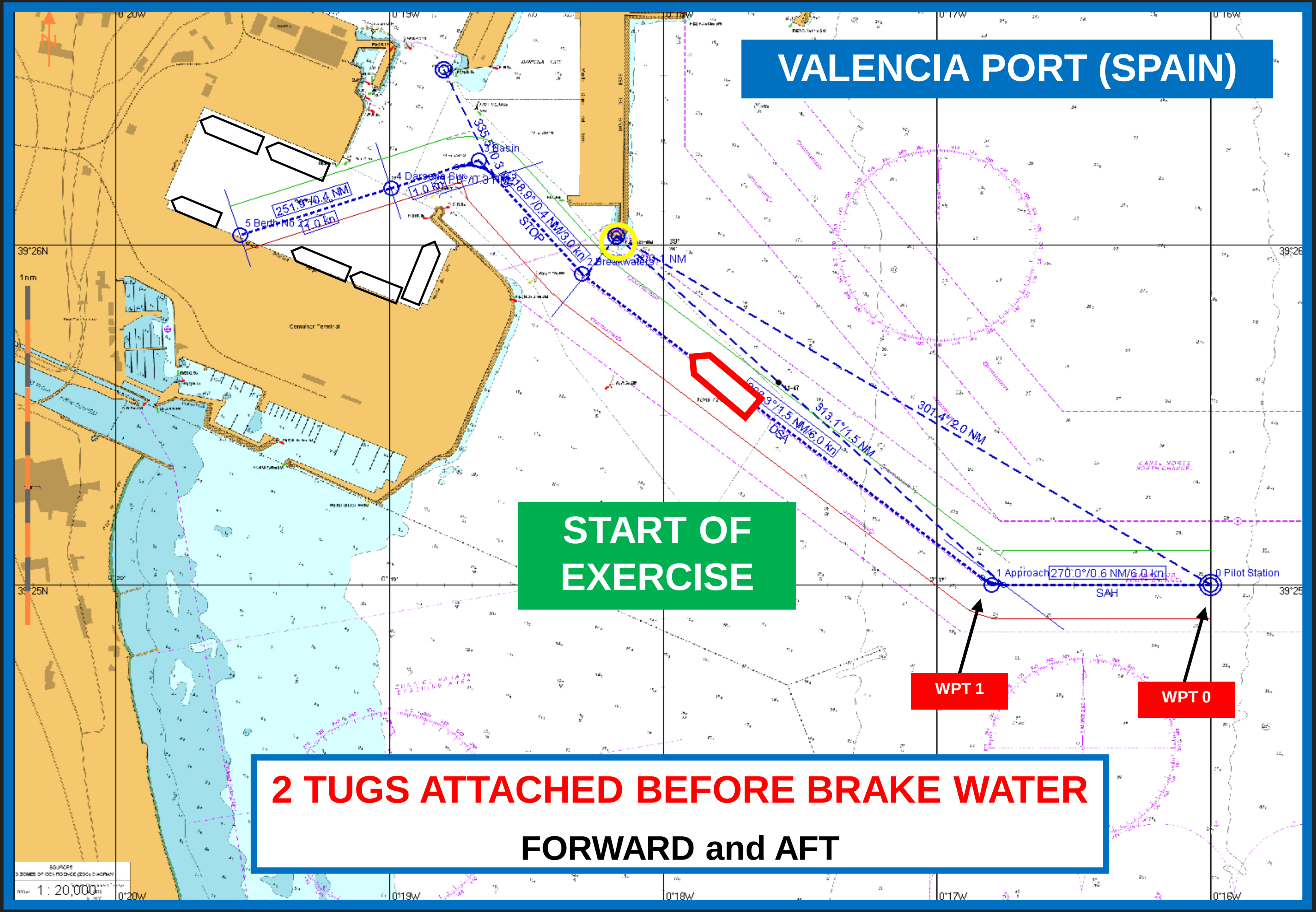
VALENCIA PORT (SPAIN)

SPEED - 6 KNOTS

WPT 1

WPT 0

2nd Scenario Rudder and Engine Jamming



VALENCIA PORT (SPAIN)

START OF EXERCISE

WPT 1

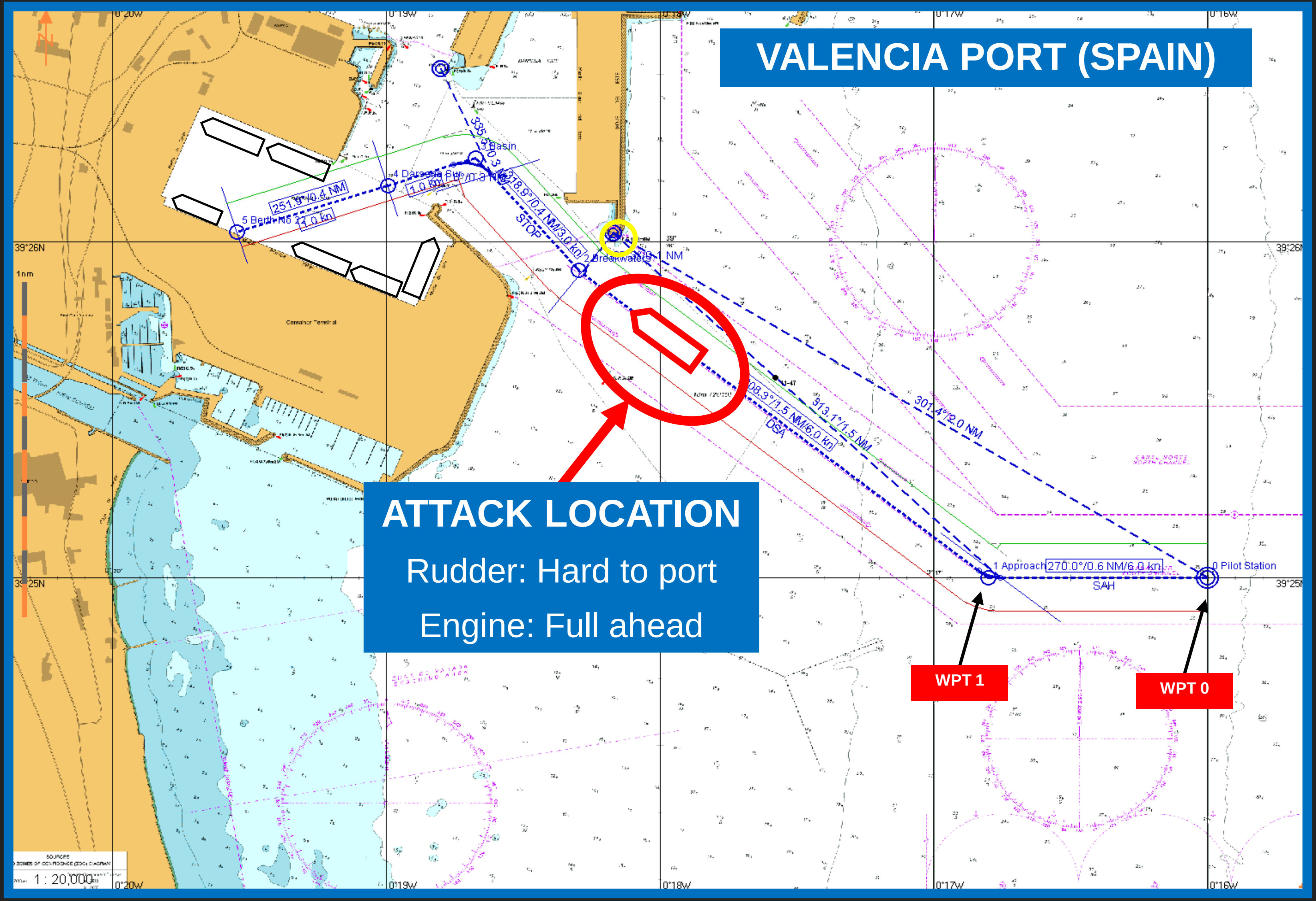
WPT 0

2 TUGS ATTACHED BEFORE BRAKE WATER

FORWARD and AFT

TIME

2nd Scenario Rudder and Engine Jamming



VALENCIA PORT (SPAIN)

ATTACK LOCATION

Rudder: Hard to port

Engine: Full ahead

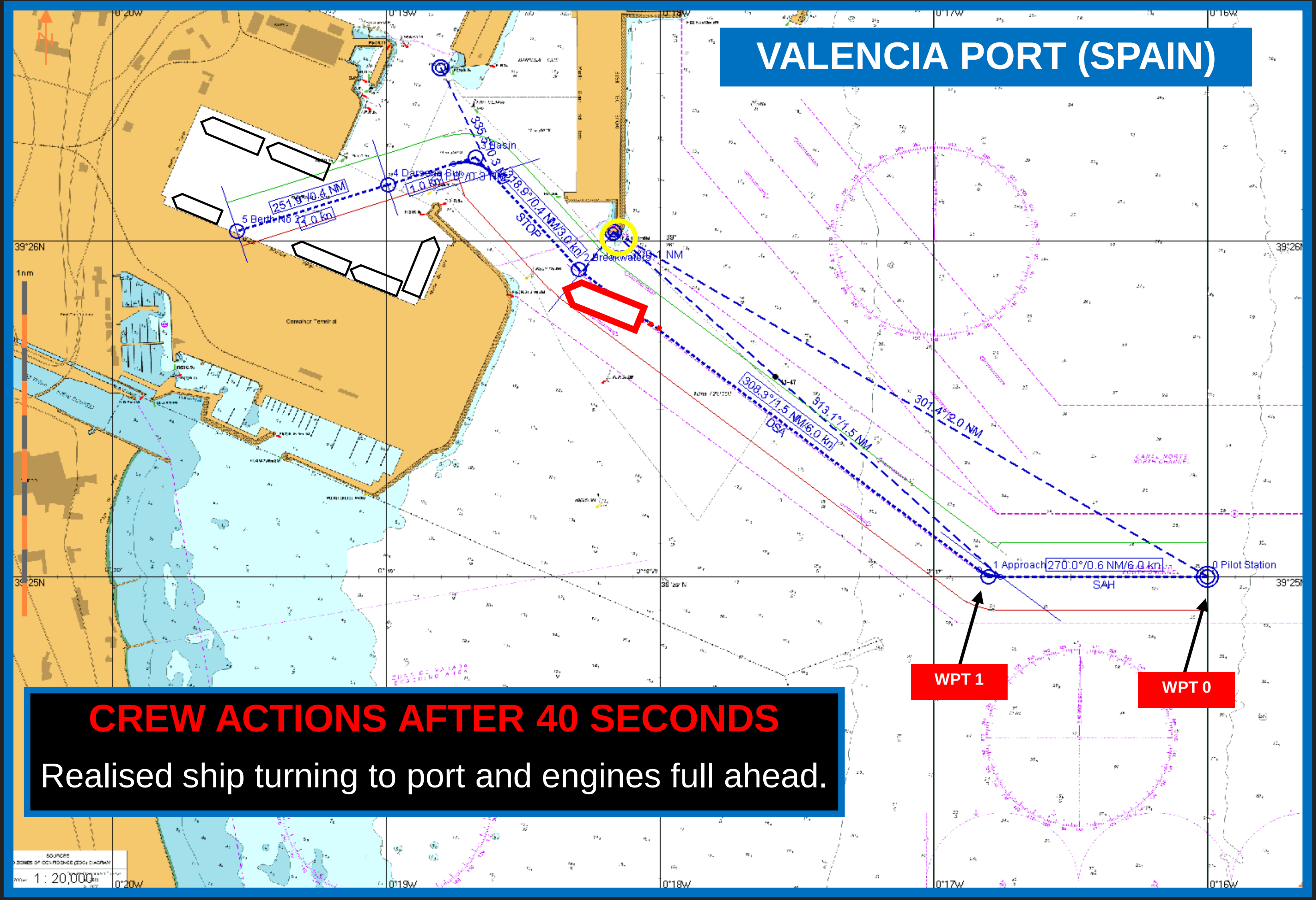
WPT 1

WPT 0

TIME

2 minutes

2nd Scenario Rudder and Engine Jamming



VALENCIA PORT (SPAIN)

WPT 1

WPT 0

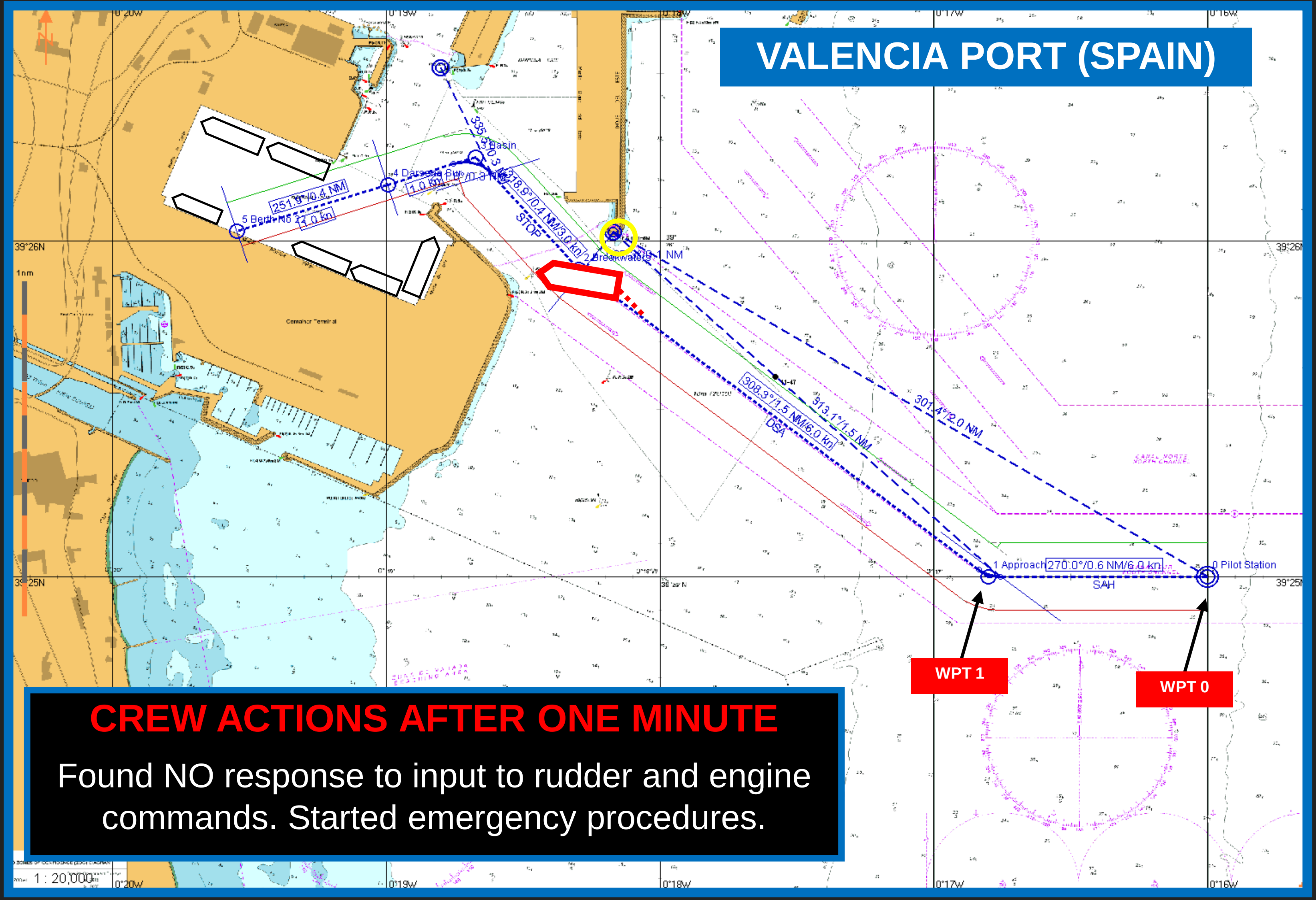
CREW ACTIONS AFTER 40 SECONDS

Realised ship turning to port and engines full ahead.

TIME

02:40

2nd Scenario Rudder and Engine Jamming



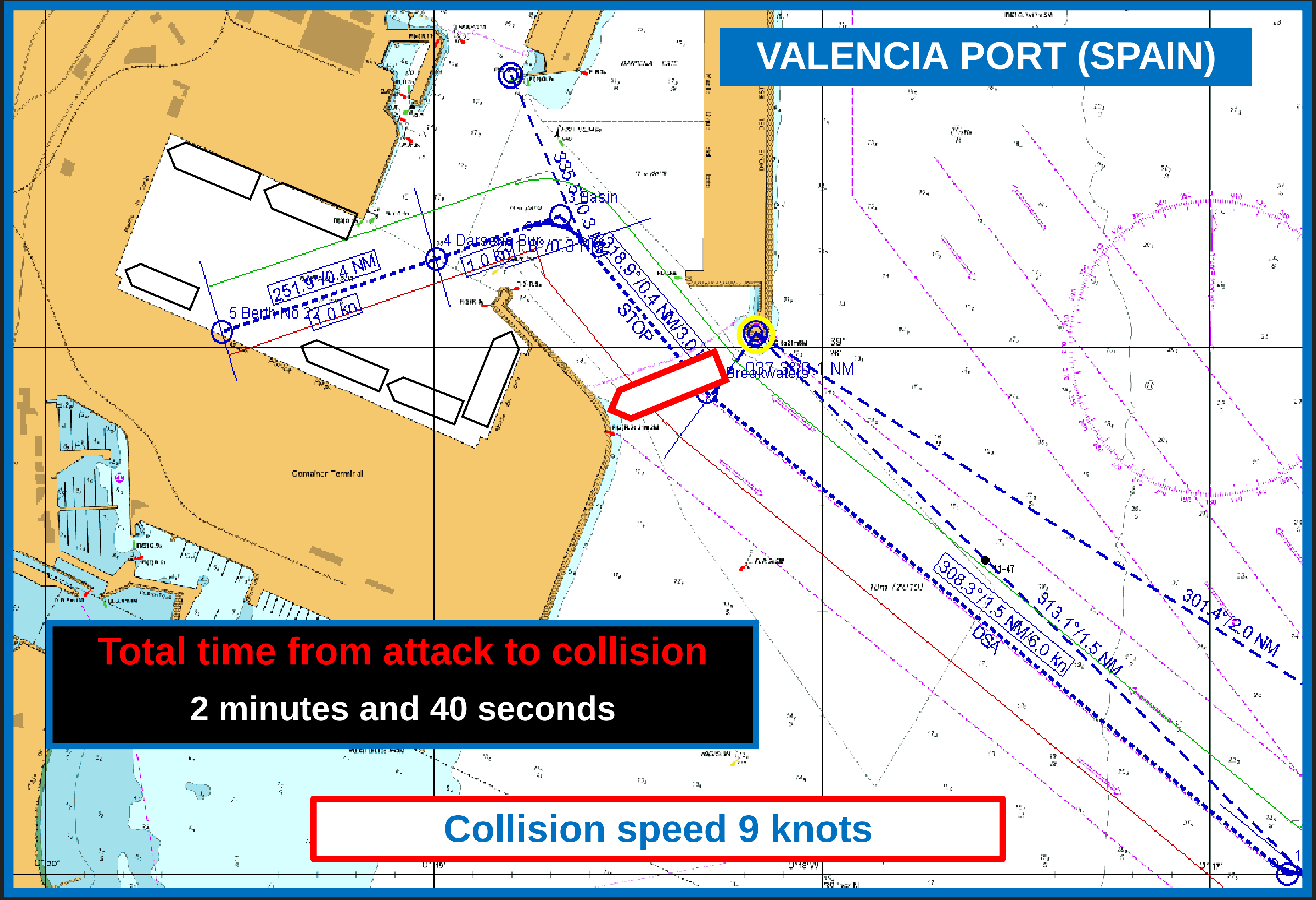
CREW ACTIONS AFTER ONE MINUTE

Found NO response to input to rudder and engine commands. Started emergency procedures.

TIME

03:00

2nd Scenario Rudder and Engine Jamming



VALENCIA PORT (SPAIN)

Total time from attack to collision

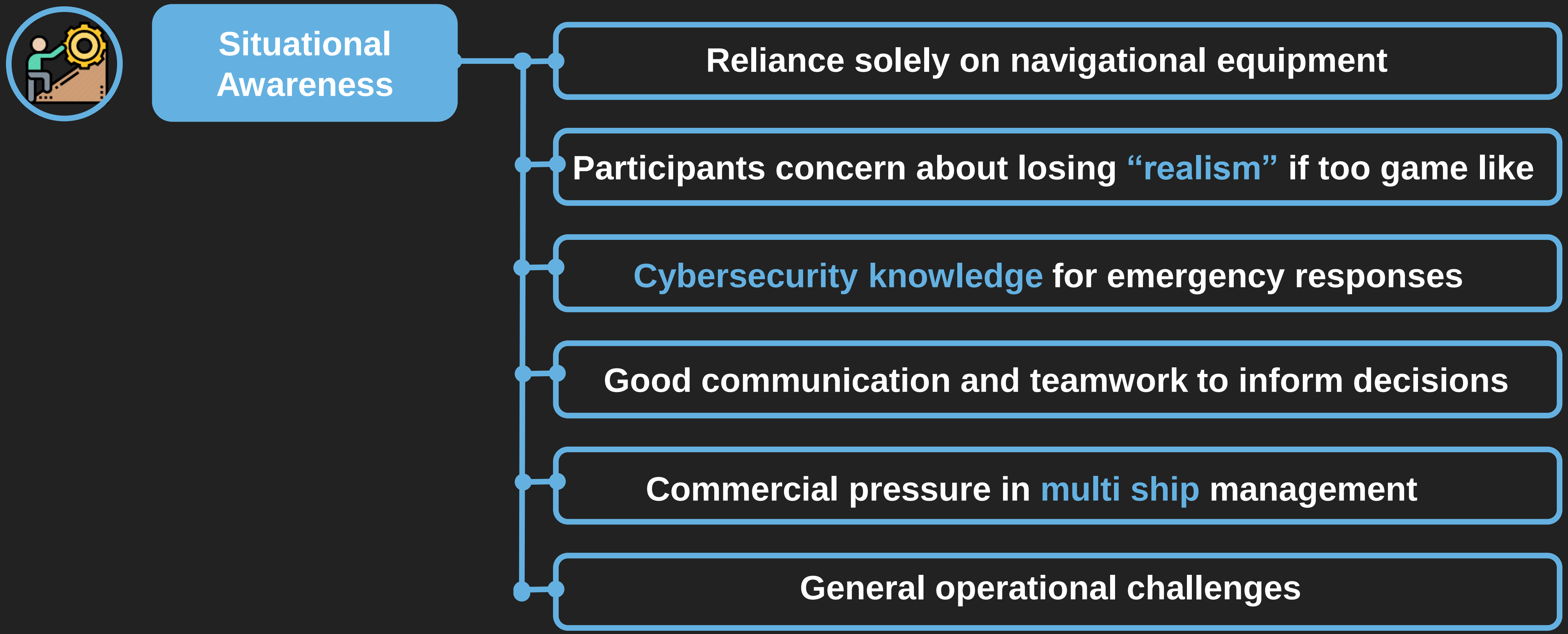
2 minutes and 40 seconds

Collision speed 9 knots

TIME

04:40

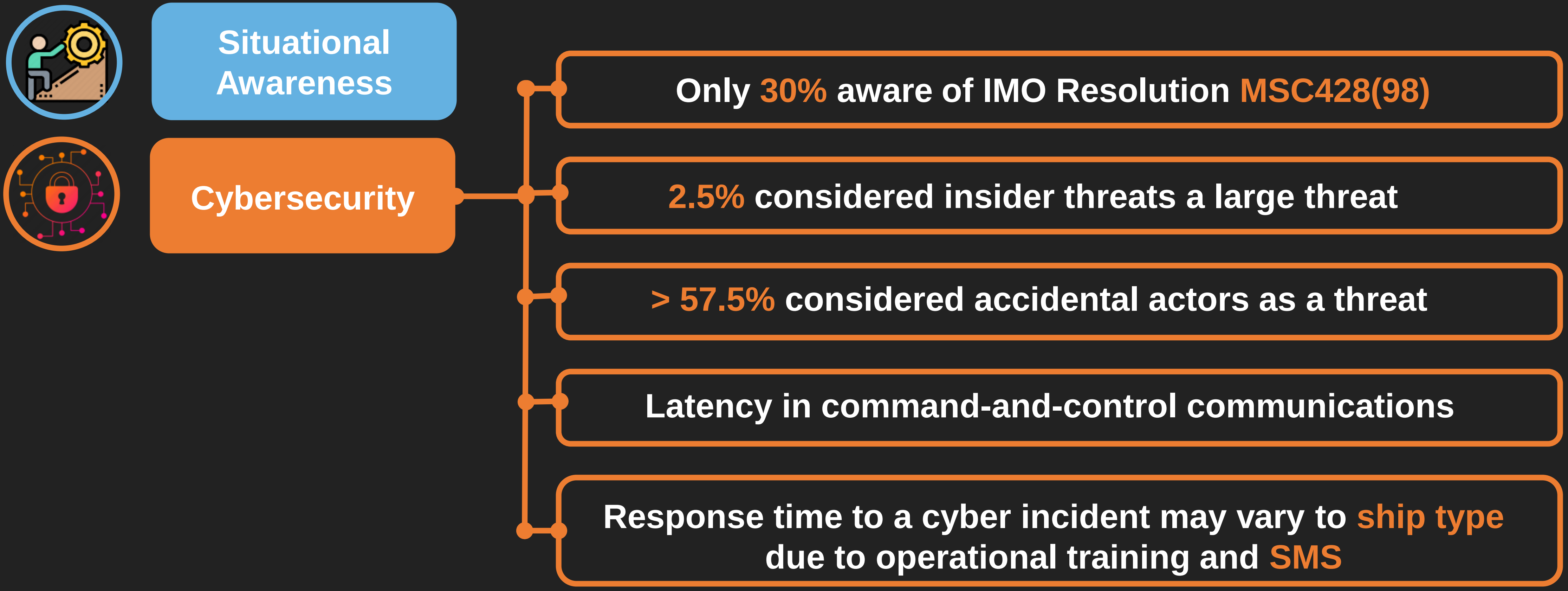
Findings



Situational Awareness

- Reliance solely on navigational equipment
- Participants concern about losing “realism” if too game like
- Cybersecurity knowledge for emergency responses
- Good communication and teamwork to inform decisions
- Commercial pressure in multi ship management
- General operational challenges

Findings

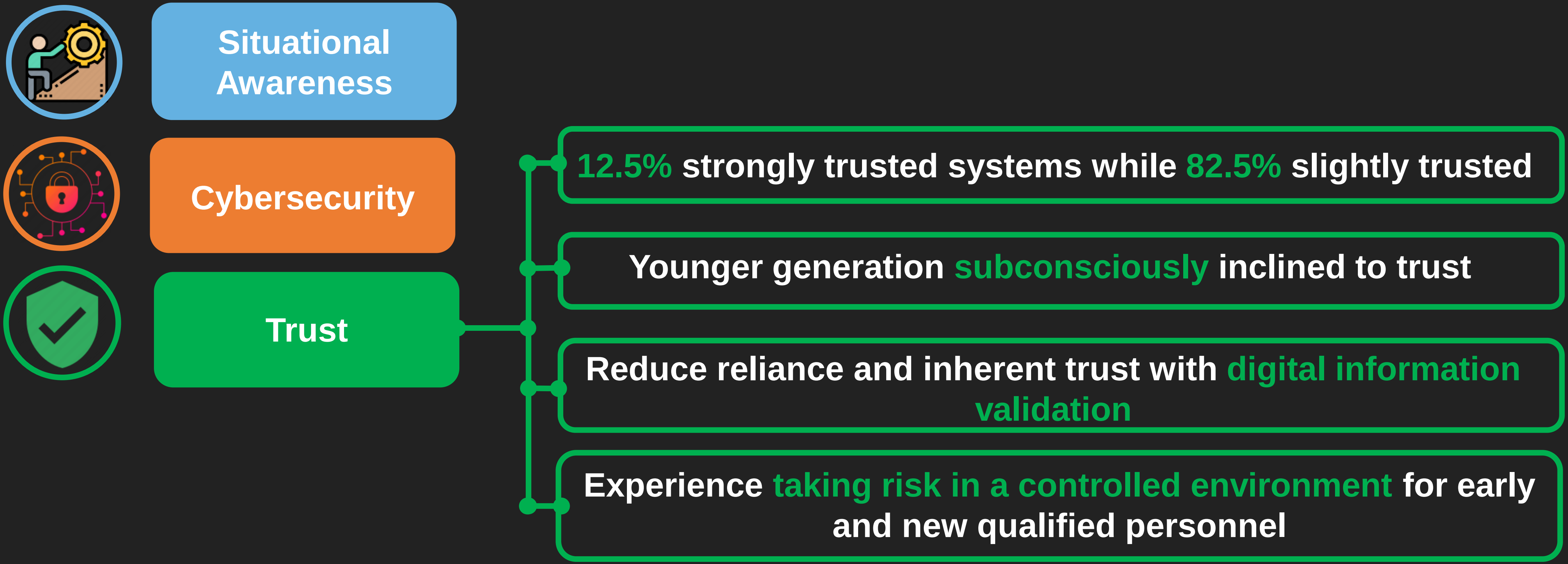


Situational Awareness

Cybersecurity

- Only 30% aware of IMO Resolution MSC428(98)
- 2.5% considered insider threats a large threat
- > 57.5% considered accidental actors as a threat
- Latency in command-and-control communications
- Response time to a cyber incident may vary to ship type due to operational training and SMS

Findings



Situational Awareness

Cybersecurity

Trust

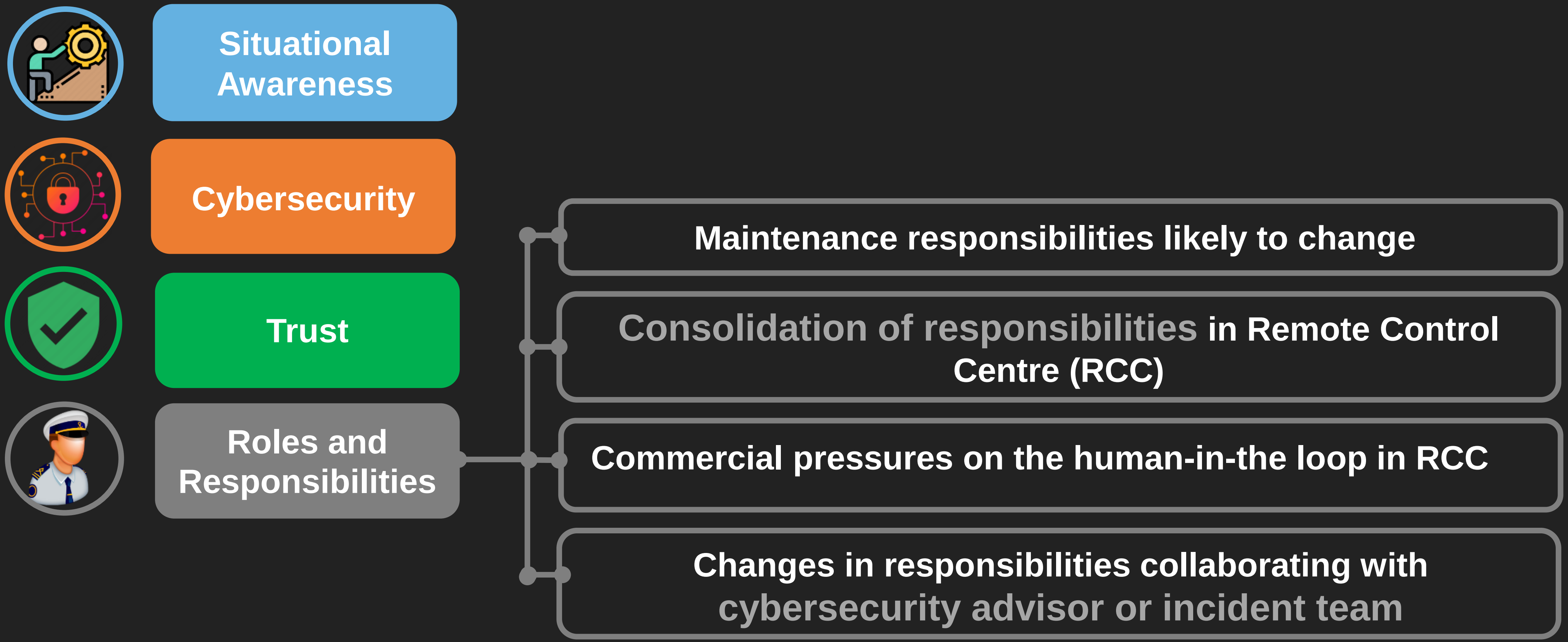
12.5% strongly trusted systems while 82.5% slightly trusted

Younger generation subconsciously inclined to trust

Reduce reliance and inherent trust with digital information validation

Experience taking risk in a controlled environment for early and new qualified personnel

Findings



Situational Awareness

Cybersecurity

Trust

Roles and Responsibilities

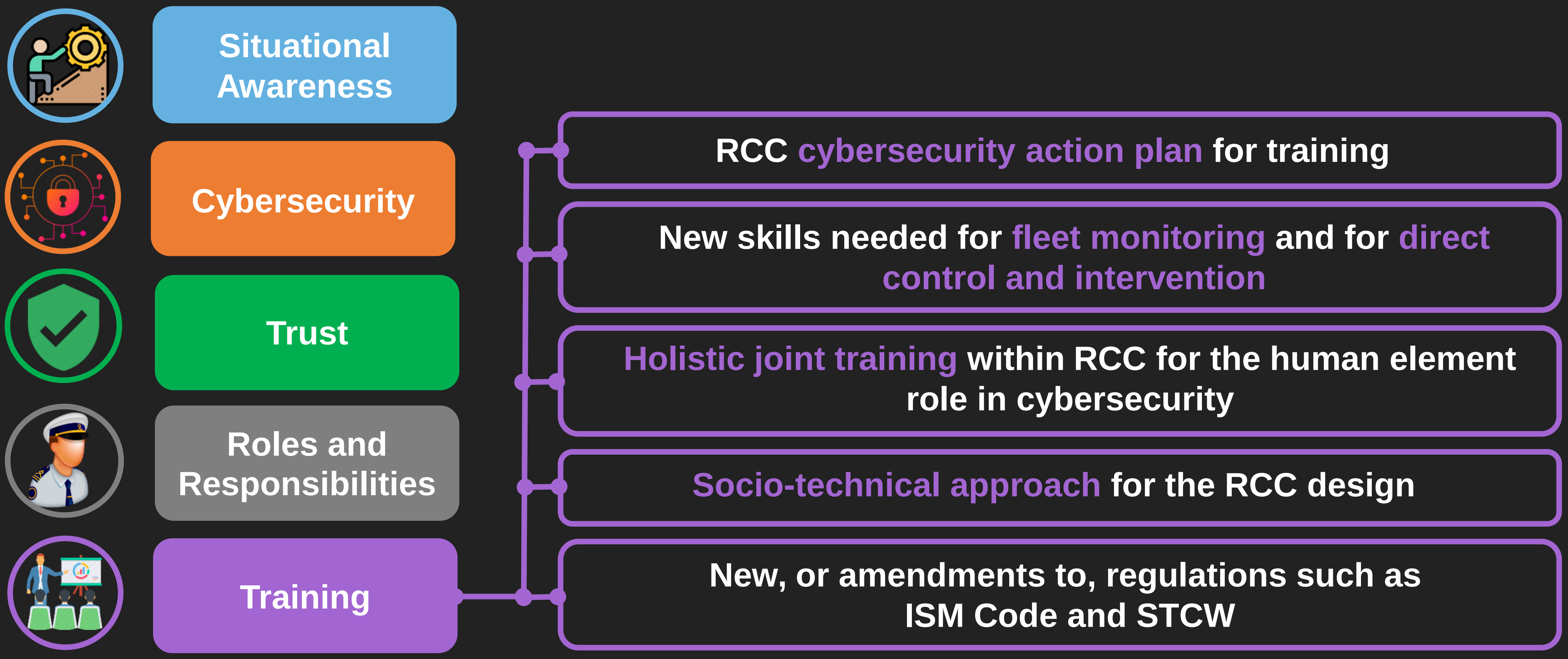
Maintenance responsibilities likely to change

Consolidation of responsibilities in Remote Control Centre (RCC)

Commercial pressures on the human-in-the loop in RCC

Changes in responsibilities collaborating with cybersecurity advisor or incident team

Findings



Situational Awareness

Cybersecurity

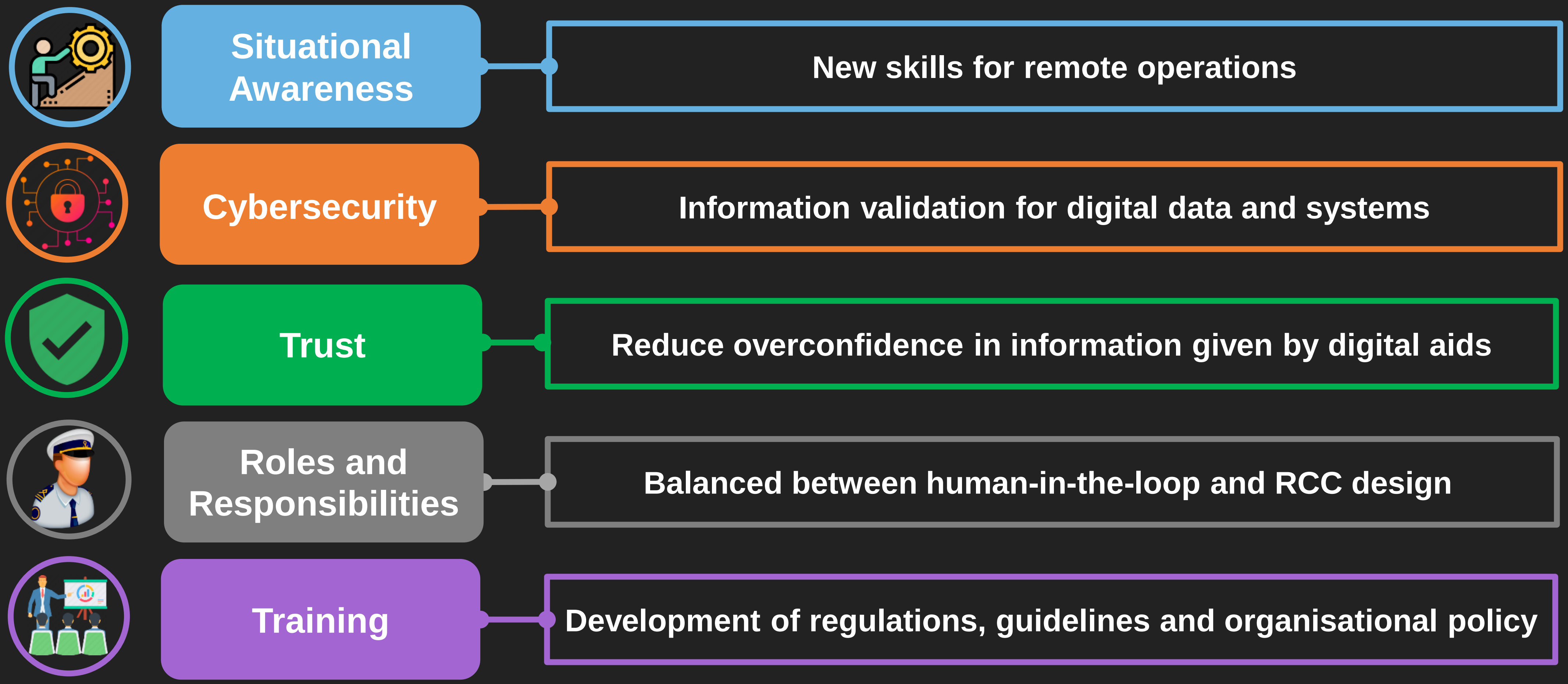
Trust

Roles and Responsibilities

Training

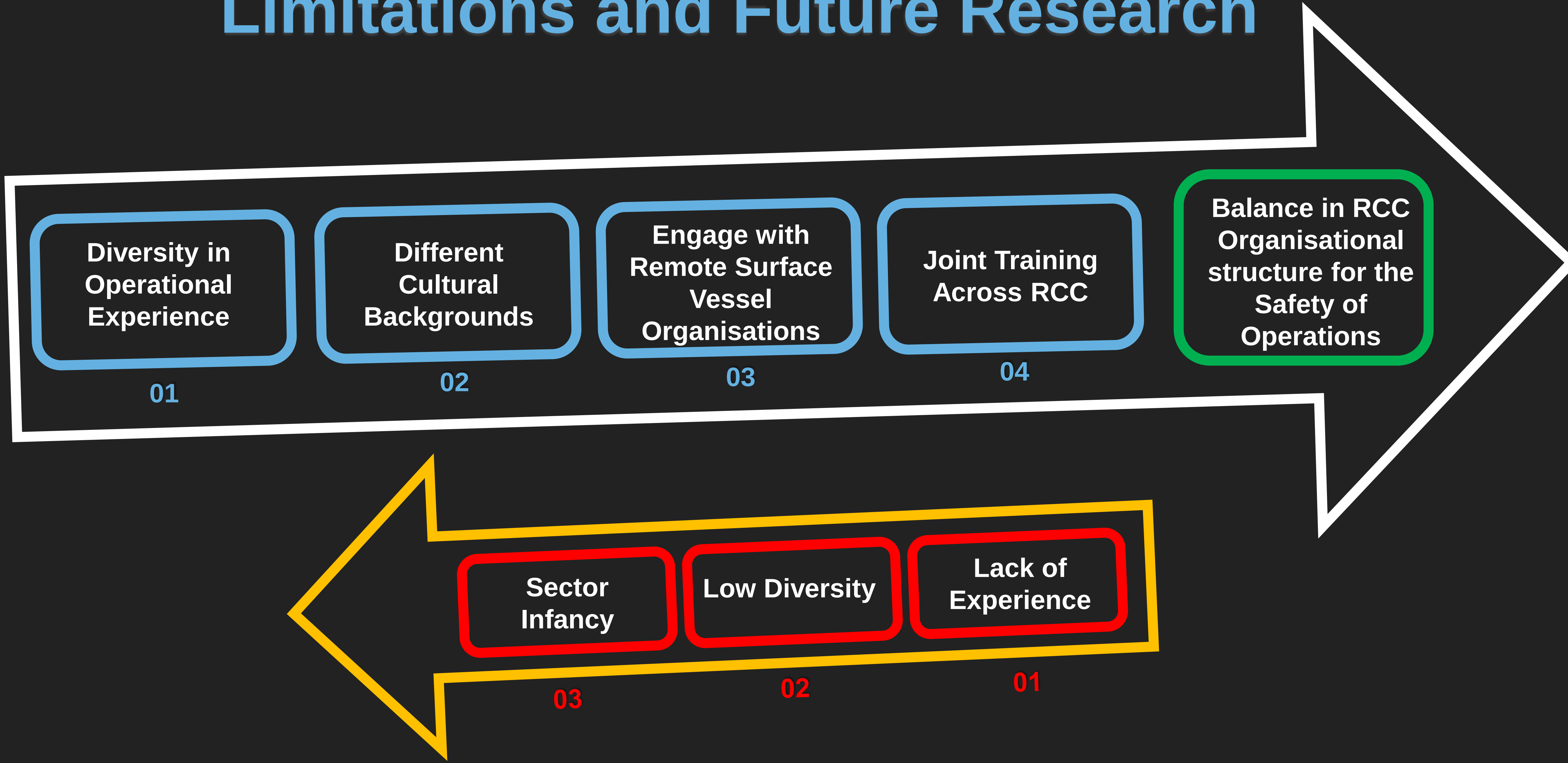
- RCC cybersecurity action plan for training
- New skills needed for fleet monitoring and for direct control and intervention
- Holistic joint training within RCC for the human element role in cybersecurity
- Socio-technical approach for the RCC design
- New, or amendments to, regulations such as ISM Code and STCW

Conclusion



Situational Awareness	New skills for remote operations
Cybersecurity	Information validation for digital data and systems
Trust	Reduce overconfidence in information given by digital aids
Roles and Responsibilities	Balanced between human-in-the-loop and RCC design
Training	Development of regulations, guidelines and organisational policy

Limitations and Future Research



Diversity in Operational Experience

01

Different Cultural Backgrounds

02

Engage with Remote Surface Vessel Organisations

03

Joint Training Across RCC

04

Balance in RCC Organisational structure for the Safety of Operations

Sector Infancy

03

Low Diversity

02

Lack of Experience

01

Thank You

Contact email: juan.palbarmisas@plymouth.ac.uk

Acknowledgements:

- Thank you to the **Reardon Smith Nautical Trust** for funding my PhD to do this research
- **Cyber-MAR project** has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No. 833389. Content reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.
- The authors would also like to thank **Prof. Kevin Jones**, **Mr. Tom Crichton, Mr. Tim Davies** and all the **participants**.

UNIVERSITY OF PLYMOUTH

Cyber-SHIP Lab
SECURING MARITIME

Cyber MAR

REARDON SMITH
NAUTICAL TRUST