CyBOK: Teachability Feasibility Study

Multiplying the reach and impact of CyBOK via safety MSc

Dr Emma Taylor CISSP CEng FIMechE FSaRS

Royal Academy of Engineering Visiting Professor

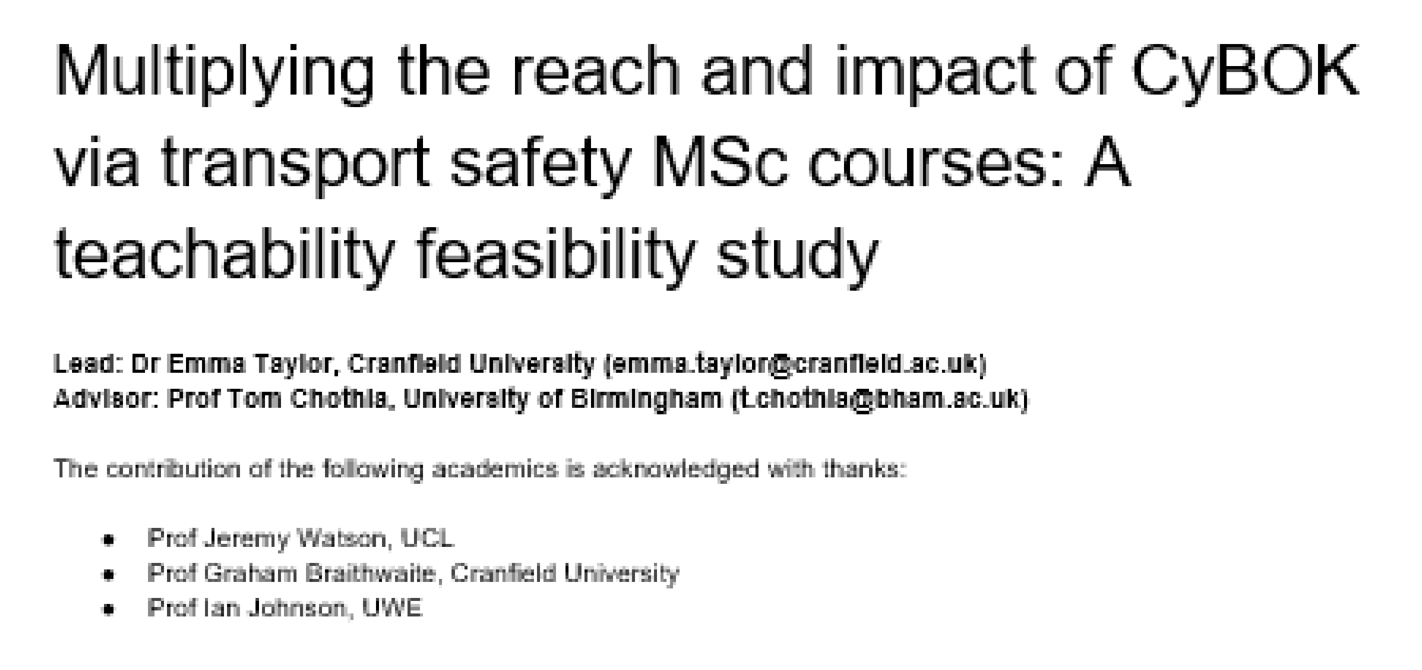
Presentation Deliverable to CyBOK, 2nd August 2024

Overview of deck

- Part 1: Context for work
- Part 2: Introduction and study methodology
- Part 3: Comparison of (safety) accident investigation and cybersecurity CyBOK themes
- Part 4: Identification of teachable scenarios
- Part 5: Priority ranking of scenarios (cybersecurity and safety perspectives)
- Part 6: Assessment of teachability through gamification, and pedagogical approaches
- Part 7: Results and analysis of consultation with the safety community
- Part 8: Deaf awareness
- Part 9: Recommendations for further work

Part 1: Context for work

This presentation accompanies the final report



Multiplying the reach and impact of CyBOK via transport safety MSc courses: A teachability feasibility study

Lead: Dr Emma Taylor, Cranfield University (emma.taylor@cranfield.ac.uk)
Advisor: Prof Tom Chothia, University of Birmingham (t.chothia@bham.ac.uk)

The contribution of the following academics is acknowledged with thanks:

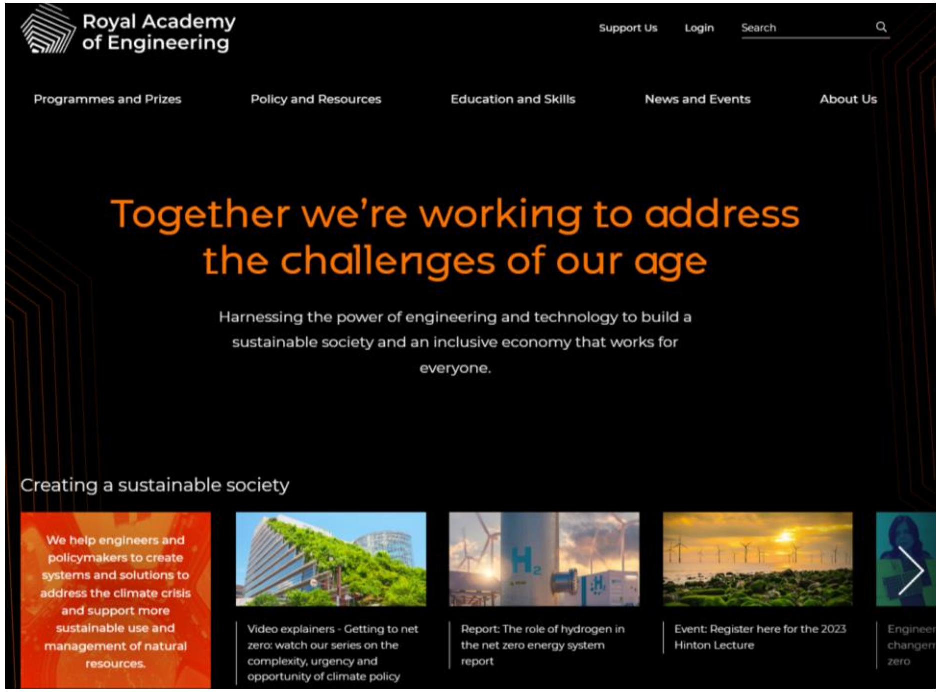
- Prof Jeremy Watson, UCL
- Prof Graham Braithwaite, Cranfield University
- Prof Ian Johnson, UWE

Context for work

Royal Academy of Engineering Visiting Professorship in Digital Safety and Security (2022-2025)

Royal Academy of Engineering Visiting Professors are focussed on:

- Teaching the engineers to 2030 and beyond
- Embedding engineering habits of mind
- Improving, systems thinking, adapting, problem-finding, creative problem solving, visualising
- Nurturing a questioning mindset, ethical consideration
- Embedding inclusion, inclusive engineering



Together we're working to address the challenges of our age

Harnessing the power of engineering and technology to build a sustainable society and an inclusive economy that works for everyone.

Creating a sustainable society

We help engineers and policymakers to create systems and solutions to address the climate crisis and support more sustainable use and management of natural resources.

Video explainers - Getting to net zero: watch our series on the complexity, urgency and opportunity of climate policy

Report: The role of hydrogen in the net zero energy system report

Event: Register here for the 2023 Hinton Lecture

Engineer changem zero

Part 2: Introduction and methodology

Why is incorporating cybersecurity into (safety) accident investigation key?

What is the rationale for this project, why has CyBOK funding been sought?

- Broadening accident investigation to incorporate cybersecurity is needed as safety-related incidents (or near misses) with a suspected cyber element are anticipated to occur in greater numbers as networks and systems become more connected, with changes in use cases and increasing system complexity leading to a wider range of unexpected emergent properties
- Increasing regulatory scrutiny and lower levels of maturity for combined safety and cybersecurity management systems create a challenging and changing environment
- Perception of one discipline by another e.g. “cybersecurity is a process not an event”, “safety is static not dynamic”, but safety specialists will say “safety is a process not an event” (note that “safety” is a much broader scope than safety-critical systems)
- The current maturity of both the field of (safety) accident investigation incorporating cyber and the teaching of accident investigation is still developing
- CyBOK material and cyber pedagogical experience may provide opportunities to fast-track the development of both competencies and teaching delivery

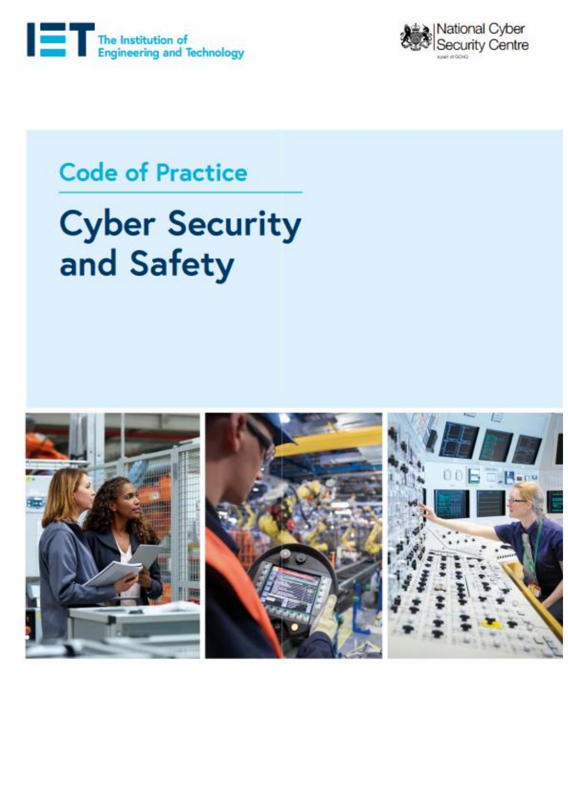
Problem statement

(Safety) accident investigation academic resources and syllabus time is limited requiring a targeted approach to the use of CyBOK themes

- Safety does not map well onto cybersecurity (IET Code of Practice in Safety and Security) and best practice is still emerging, with limited case studies which are distributed and understood
- As a result (future) skills development of (safety) accident investigators is impaired, potentially leading to additional hurdles when investigating incidents incorporating digital technologies.
- Given the lack of existing capabilities and/or time resources in the student (and academic) cohort, and MSc accident investigation syllabus time available for cybersecurity, a targeted and tailored approach is needed when evaluating opportunities for use of CyBOK material
- A case for the time needed will need to be made (e.g. a 1-2 day addition to a 3 week programme) it is not sufficient simply to say that “cyber needs to be taught”. This will prepare the ground for a scenario-based hybrid safety/cybersecurity (Digital Safety) module add-on proposal
- Teachable scenario approach, incorporating reasonably foreseeable scenarios, credible to those without a cyber background, and potentially using elements of gamification, are assumed to provide the best starter for ten approach. This will need to be trialled in the field to confirm this.

Material challenges exist when working to incorporate safety and cybersecurity

These have been summarised and distributed across industry, they represent some baseline limitations involved in teaching cyber into safety

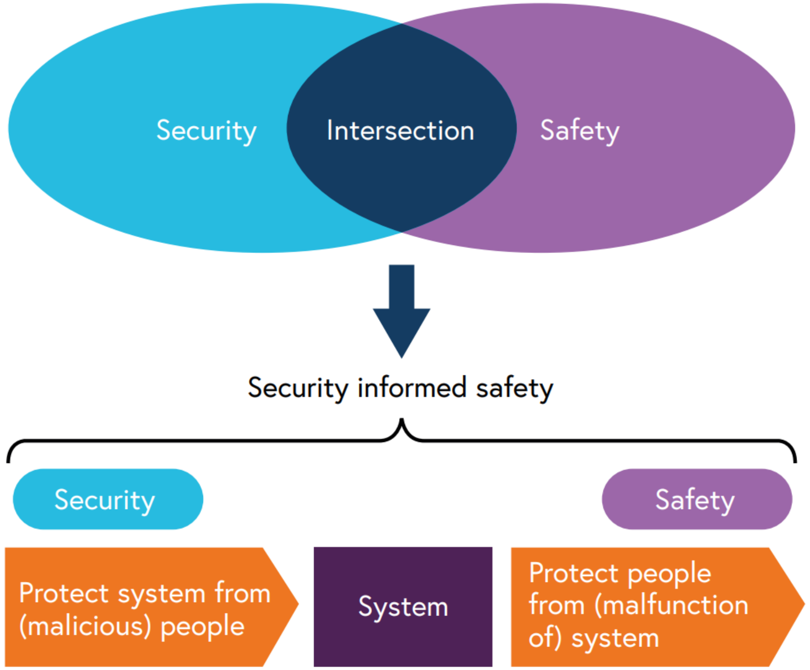


IET The Institution of Engineering and Technology

National Cyber Security Centre
a part of GCHQ

Code of Practice

Cyber Security and Safety



Security

Intersection

Safety

Security informed safety

Security

Safety

Protect system from (malicious) people

System

Protect people from (malfunction of) system

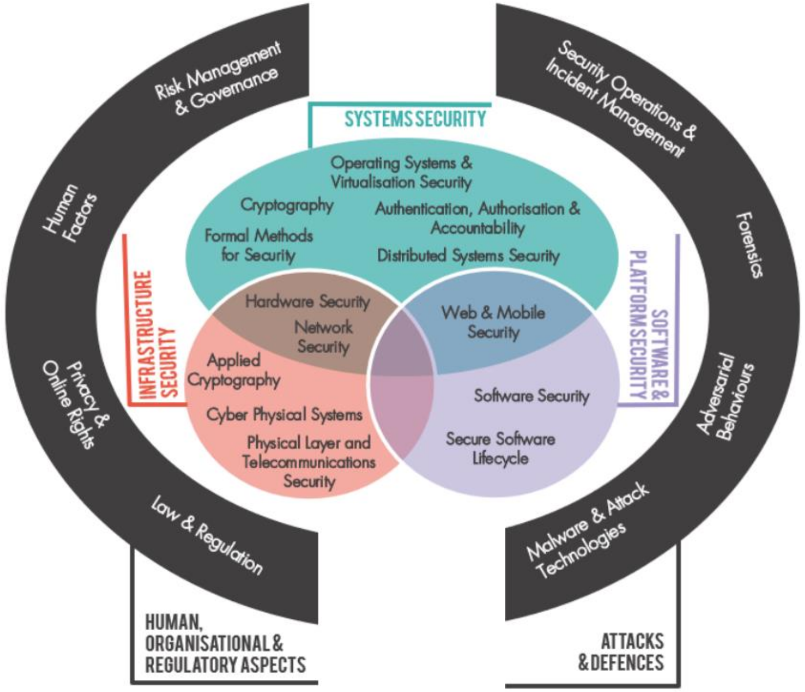
Part 3: Comparison of safety and cybersecurity

- Analysis and screening of CyBOK themes against (safety) accident investigation modules to identify opportunities for teaching cybersecurity into accident investigation (as well as challenges e.g. due to technical skill levels required)
- Evaluation of the structure of safety risk management and the types of controls to further refine the topic areas and approaches for teachable scenarios, identify priorities and limitations
- Create and apply a ranking structure for teachability of the 5 CyBOK themes, build development of scenario themes using the results of the high-level screening
- Some additional opportunities for short lectures to fill certain topic area gaps were also identified

CyBOK topic areas

CyBOK resources are grouped into five themes, these represent a pool of resources for teaching cybersecurity in (safety) accident investigation

1. Human Organisational and Regulatory Aspects
2. Attacks and Defences
3. Infrastructure Security
4. Systems Security
5. Software and Platform Security



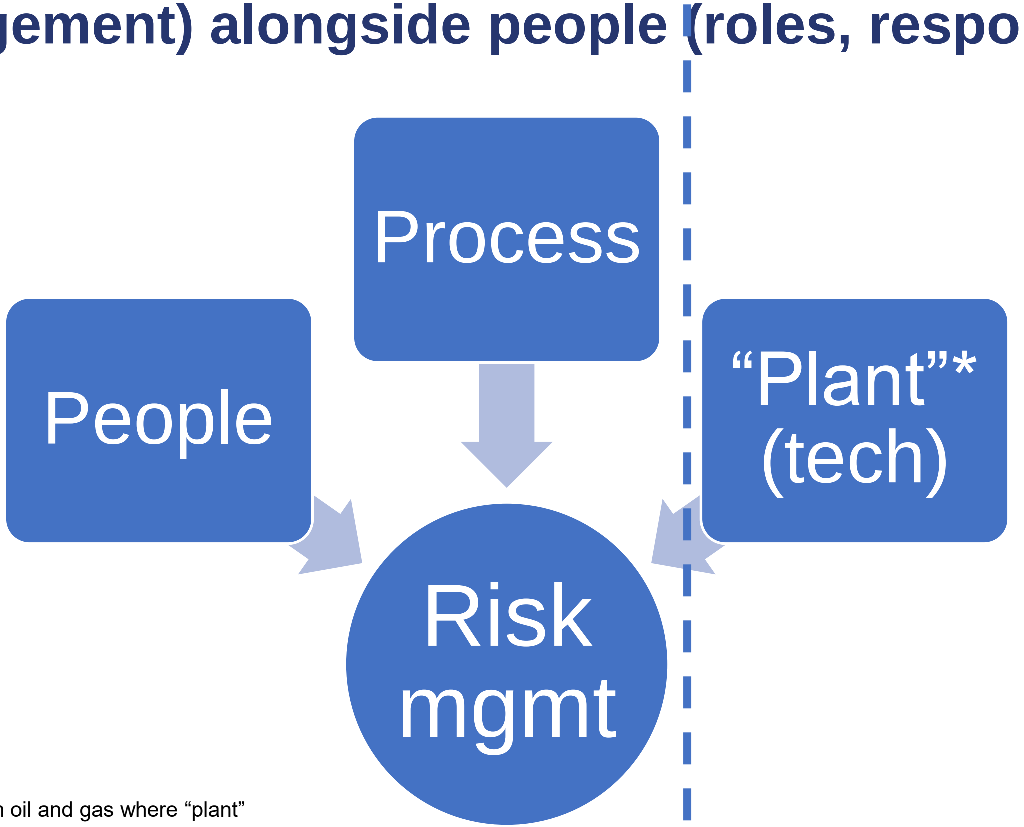
Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
Cryptography
Authentication, Authorisation & Accountability
Formal Methods for Security
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Applied Cryptography
Cyber Physical Systems
Physical Layer and Telecommunications Security
Web & Mobile Security
Software Security
Secure Software Lifecycle
SOFTWARE & PLATFORM SECURITY
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

Safety risk management structure and controls (3 types: people, “plant”, process)

Industry regulators scrutinise safety management systems (process, organisation, management) alongside people (roles, responsibilities)

Hierarchy of controls (i.e. which type should be used first) is set by legislation/regulation (MHSWR)

Technical controls may be selected over administrative controls in this hierarchy

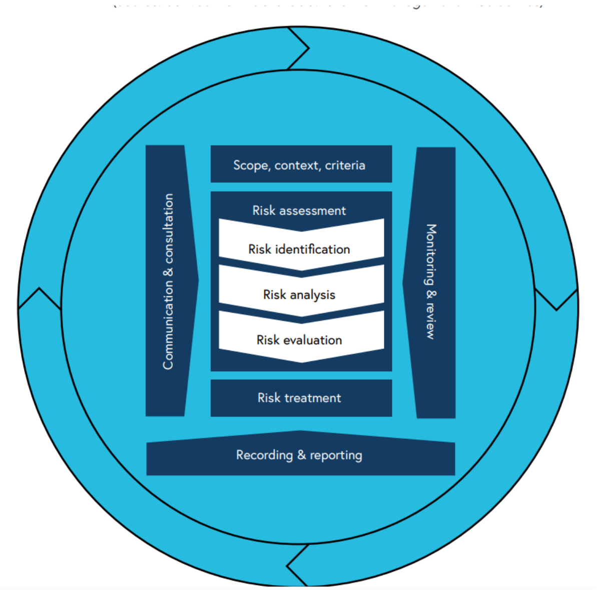


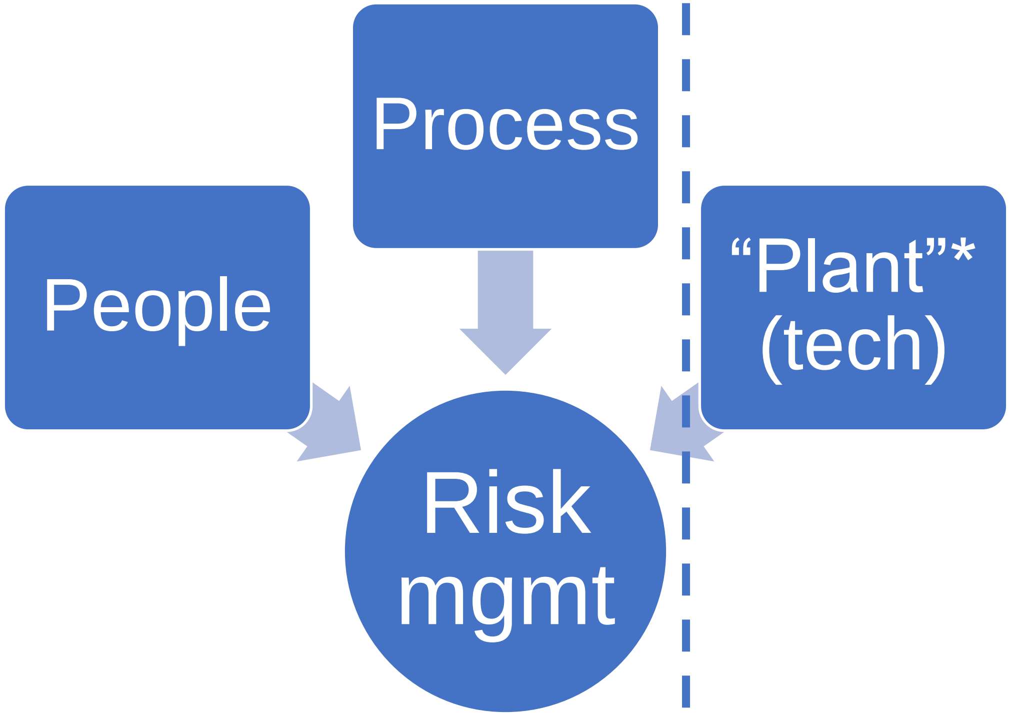
The discipline of cybersecurity (as mapped by CyBOK) is strongly technology based. Understanding the role of people (e.g. attack/defend) and data (e.g. incident management, forensics) requires technological skills.

* Naming of three categories of controls originally from oil and gas where “plant” refers to process control equipment (valves, pipework, vessels, control systems). Plant = technology (hardware, software…)

Safety risk management structure (people, “plant” and process)

Controls are identified through the implementation of a risk management process



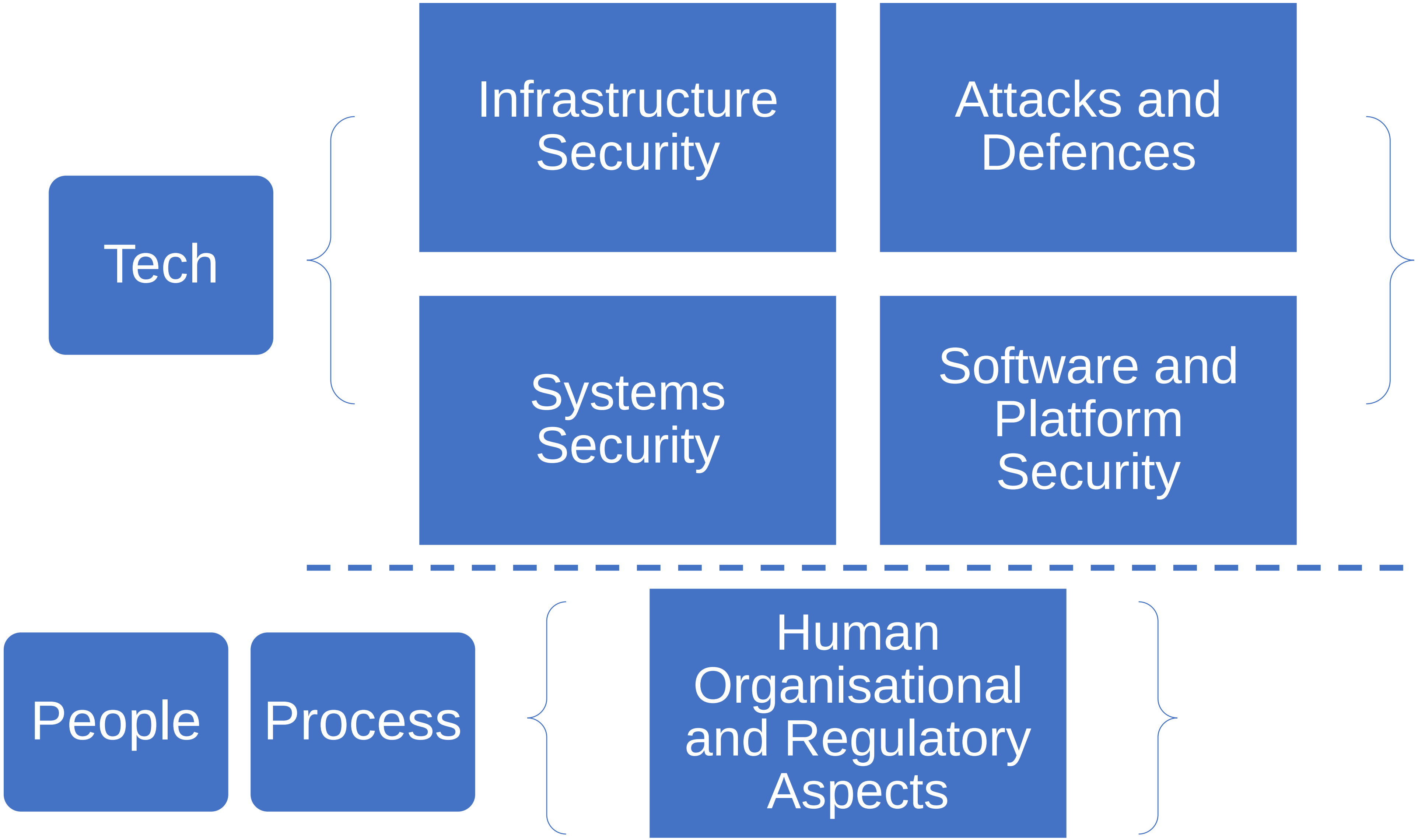


Safety accident investigators of course focus on all three categories of controls and where they have failed

In recent digital technology incidents (e.g. Rail Accident Investigation Branch Cambrian ERTMS where integrity and availability of data was not maintained the difficulty of gathering and understanding the data clearly bounds the investigation process and report content.

Investigators will focus where they can. Scenarios are needed to encourage a focus on tech elements despite difficulty in gathering data

Five CyBOK themes, the majority of which are linked to primarily “technical” controls



Tech

Infrastructure Security

Attacks and Defences

Systems Security

Software and Platform Security

People

Process

Human Organisational and Regulatory Aspects

Accident investigation syllabus opportunities for alignment

Overview based on access to multiple MSc courses, including Fundamentals of Accident Investigation and Applied Marine Accident Investigation

- Teaching (safety) MSc Accident investigation is management-centric and people-led
- Human factors are considered in context of management systems, both investigation management and management of organisation being investigated
- Focus on selected technical elements primarily directly relevant to incident investigation, case studies discussed
- Significant proportion of course time is spent on applied exercises, in the field

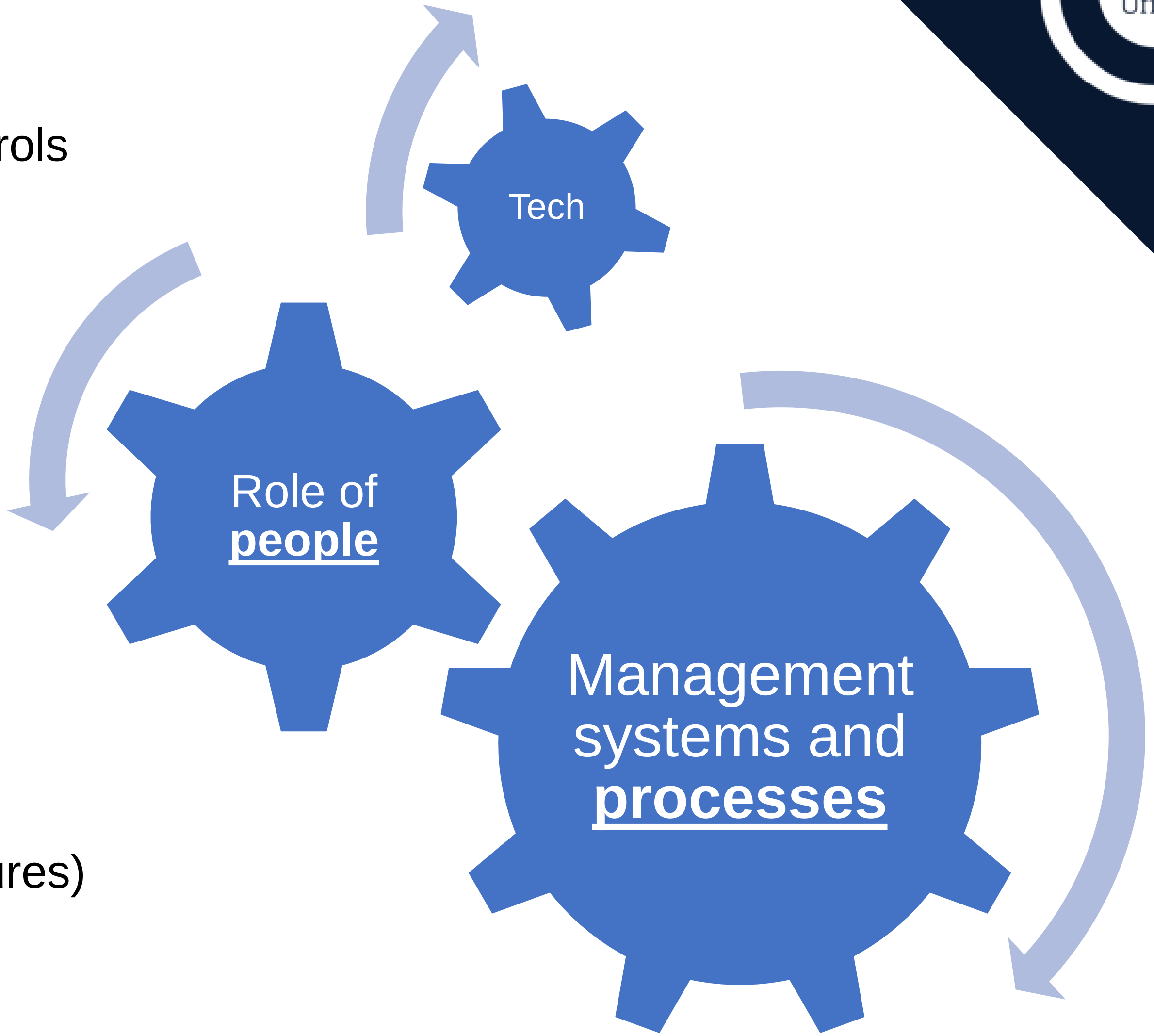
Syllabus analysis shows majority of teaching time (including exercises) on two out of three of the controls (people, processes), less focus on the third (tech)

General:

- Accident site investigation procedures and practicalities
- Investigation of human factors and organisations
- Accident site investigation, procedures and practicalities
- Interviewing people (e.g. witnesses, participants)
- Legal and regulatory context

Marine specific:

- Marine accident investigation process
- International perspective (co-ordination and cultures)
- National and international regulations and codes



Ranking of CyBOK themes for alignment with (safety) accident investigation (1/2)

CyBOK material needs to be screened to identify “implementability” within a (safety) accident investigation teaching context

- The alignment scale is qualitative and relative and characterises the degree of alignment of each the five CyBOK themes to the relevant accident investigation modules.
  - Assessment is carried out within the current syllabus framework provided by the MSc in Fundamentals in Accident Investigation (with the specialist modules in Applied Maritime Accident Investigation)
- It is not defining whether the topics covered by CyBOK would be called on in a cybersecurity-led investigation but how close (or not) the CyBOK topic areas fit into the accident investigator mindset and skillset developed through the MSc module study and the nature of opportunities for.

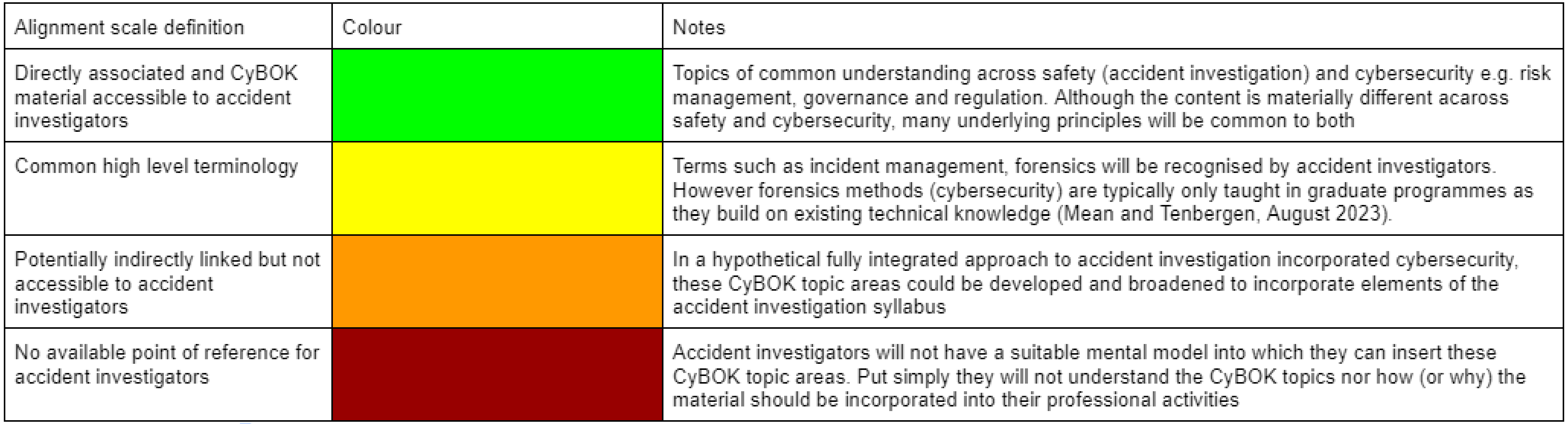
Ranking of CyBOK themes for alignment with (safety) accident investigation (2/2)

CyBOK material needs to be screened to identify “implementability” within a (safety) accident investigation teaching context

- Colloquially, it’s a ranking of whether an accident investigator will pick up a CyBOK document index and be able to
  - (green - directly associated) understand the content, read and absorb and then assess how it might be integrated into their professional practice, through to the opposite end of the scale
  - (red - no available point of reference) where the index page won’t be understood nor seen as relevant to accident investigation and there is no evident pathway through which to teach the material within the context of scenario-based gamification, given the various constraints (available syllabus, student cohort skillset)
- The CyBOK topic themes assessed as red are not incorporated into the development of the scenarios which are then assessed for their priority and teachability and implemented through pedagogical approaches.

Ranking scale developed for study

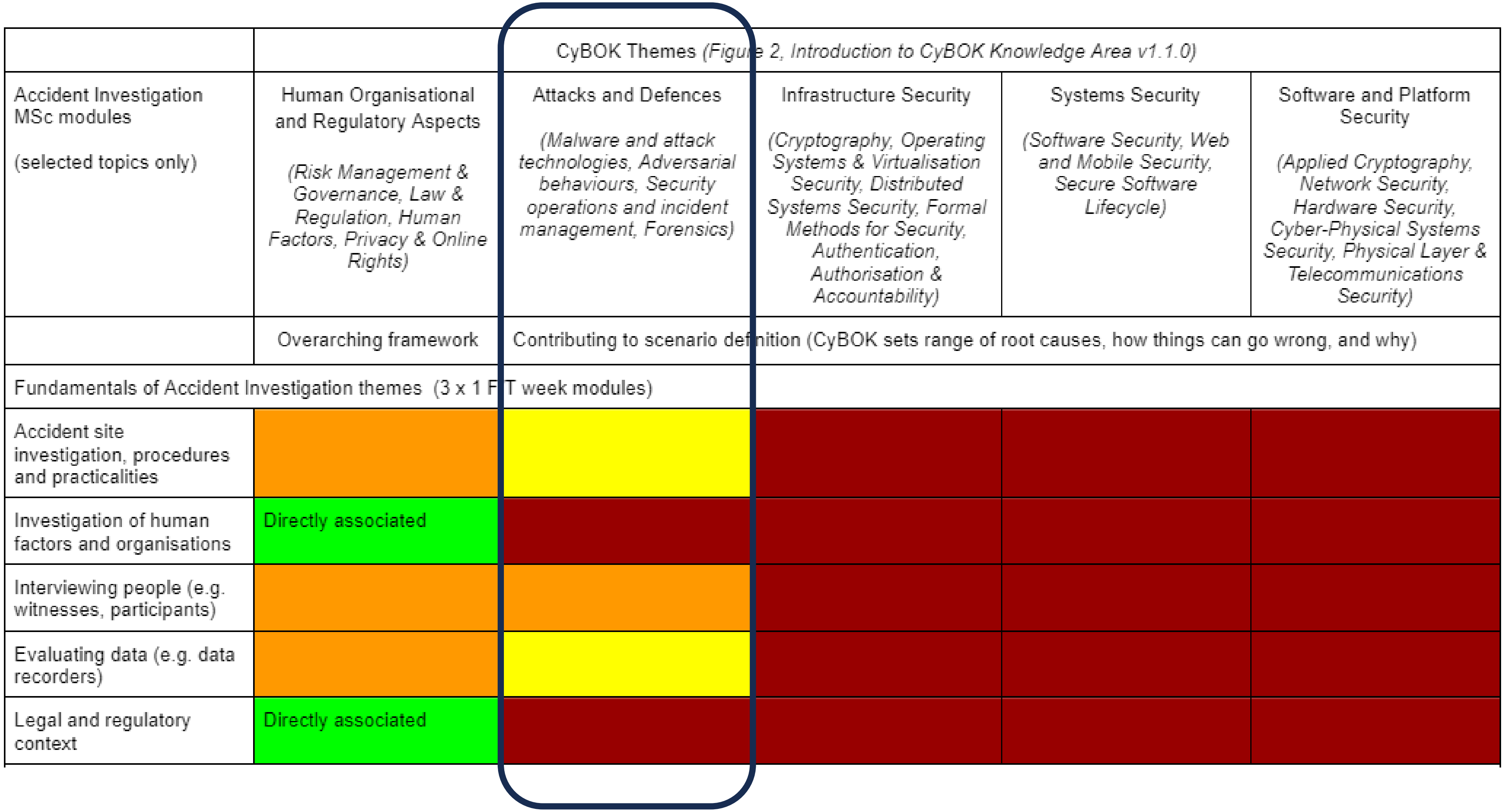
Applied to Accident Investigation syllabus modules (general and maritime specialist modules)



Alignment scale definition	Colour	Notes
Directly associated and CyBOK material accessible to accident investigators	🟩	Topics of common understanding across safety (accident investigation) and cybersecurity e.g. risk management, governance and regulation. Although the content is materially different acaross safety and cybersecurity, many underlying principles will be common to both
Common high level terminology	🟨	Terms such as incident management, forensics will be recognised by accident investigators. However forensics methods (cybersecurity) are typically only taught in graduate programmes as they build on existing technical knowledge (Mean and Tenbergen, August 2023).
Potentially indirectly linked but not accessible to accident investigators	🟧	In a hypothetical fully integrated approach to accident investigation incorporated cybersecurity, these CyBOK topic areas could be developed and broadened to incorporate elements of the accident investigation syllabus
No available point of reference for accident investigators	🟥	Accident investigators will not have a suitable mental model into which they can insert these CyBOK topic areas. Put simply they will not understand the CyBOK topics nor how (or why) the material should be incorporated into their professional activities

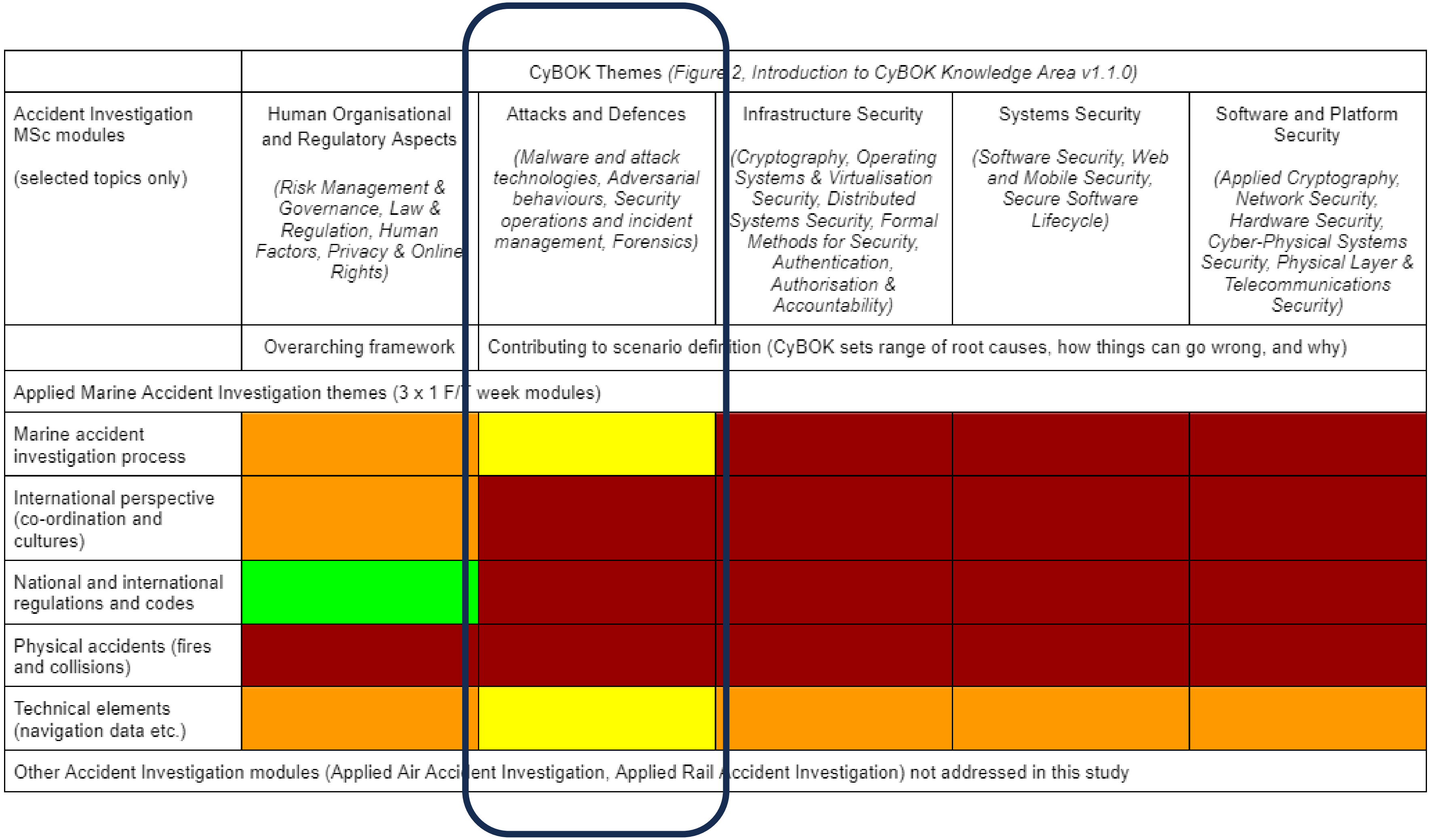
Full breakdown of syllabus and scope not publishable in its entirety (IP and copyright)

Mapping of CyBOK themes to selected Accident Investigation modules (1/2)



	CyBOK Themes *(Figure 2, Introduction to CyBOK Knowledge Area v1.1.0)*				
Accident Investigation MSc modules (selected topics only)	Human Organisational and Regulatory Aspects *(Risk Management & Governance, Law & Regulation, Human Factors, Privacy & Online Rights)*	Attacks and Defences *(Malware and attack technologies, Adversarial behaviours, Security operations and incident management, Forensics)*	Infrastructure Security *(Cryptography, Operating Systems & Virtualisation Security, Distributed Systems Security, Formal Methods for Security, Authentication, Authorisation & Accountability)*	Systems Security *(Software Security, Web and Mobile Security, Secure Software Lifecycle)*	Software and Platform Security *(Applied Cryptography, Network Security, Hardware Security, Cyber-Physical Systems Security, Physical Layer & Telecommunications Security)*
	Overarching framework	Contributing to scenario definition (CyBOK sets range of root causes, how things can go wrong, and why)			
Fundamentals of Accident Investigation themes (3 x 1 F/T week modules)					
Accident site investigation, procedures and practicalities	🟧	🟨	🟥	🟥	🟥
Investigation of human factors and organisations	🟩 Directly associated	🟥	🟥	🟥	🟥
Interviewing people (e.g. witnesses, participants)	🟧	🟧	🟥	🟥	🟥
Evaluating data (e.g. data recorders)	🟧	🟨	🟥	🟥	🟥
Legal and regulatory context	🟩 Directly associated	🟥	🟥	🟥	🟥

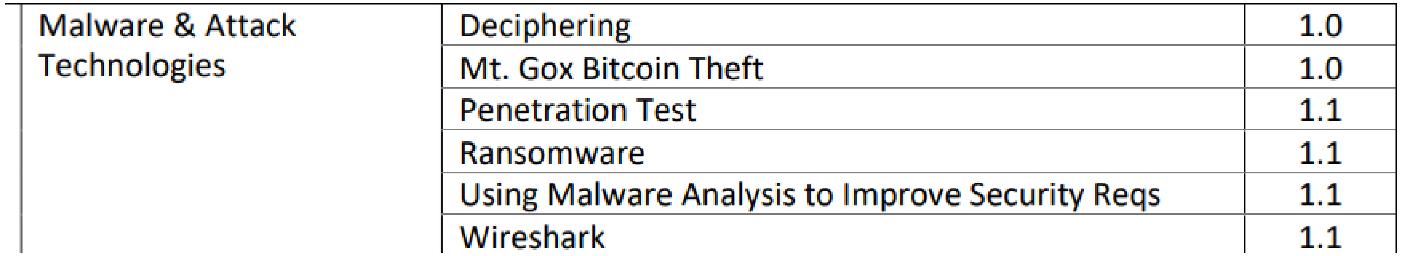
Mapping of CyBOK themes to selected Accident Investigation modules (2/2)



	CyBOK Themes *(Figure 2, Introduction to CyBOK Knowledge Area v1.1.0)*				
Accident Investigation MSc modules (selected topics only)	Human Organisational and Regulatory Aspects *(Risk Management & Governance, Law & Regulation, Human Factors, Privacy & Online Rights)*	Attacks and Defences *(Malware and attack technologies, Adversarial behaviours, Security operations and incident management, Forensics)*	Infrastructure Security *(Cryptography, Operating Systems & Virtualisation Security, Distributed Systems Security, Formal Methods for Security, Authentication, Authorisation & Accountability)*	Systems Security *(Software Security, Web and Mobile Security, Secure Software Lifecycle)*	Software and Platform Security *(Applied Cryptography, Network Security, Hardware Security, Cyber-Physical Systems Security, Physical Layer & Telecommunications Security)*
	Overarching framework	Contributing to scenario definition (CyBOK sets range of root causes, how things can go wrong, and why)			
Applied Marine Accident Investigation themes (3 x 1 F/T week modules)					
Marine accident investigation process	🟧	🟨	🟥	🟥	🟥
International perspective (co-ordination and cultures)	🟧	🟥	🟥	🟥	🟥
National and international regulations and codes	🟩	🟥	🟥	🟥	🟥
Physical accidents (fires and collisions)	🟥	🟥	🟥	🟥	🟥
Technical elements (navigation data etc.)	🟧	🟨	🟧	🟧	🟧
Other Accident Investigation modules (Applied Air Accident Investigation, Applied Rail Accident Investigation) not addressed in this study					

CyBOK Attacks and Defences represents CyBOK material best suited to teaching

Elements of CyBOK resources can be passed directly to students (sections on malware etc.)



Malware & Attack Technologies	Deciphering	1.0
	Mt. Gox Bitcoin Theft	1.0
	Penetration Test	1.1
	Ransomware	1.1
	Using Malware Analysis to Improve Security Reqs	1.1
	Wireshark	1.1

<u>Attacks and Defences is best suited for (safety) accident investigation, creation of teachable scenarios</u>
This CyBOK theme represents the cornerstone material that is anticipated to be easiest (relatively) and most appropriate for application within a (safety) accident investigation curriculum, based on the results of the initial screening (previous two slides)

Recommendations for additional lectures (1/2)

The comparison between (safety) accident investigation syllabus themes and CyBOK themes also identified a few gaps potentially requiring targeted lectures. This is in addition to material specific to Attacks and Defences

- 1 hour lecture summarising cybersecurity based organisational and regulatory factors including scope and impact on (i) the normal operation of an organisation (ii) incident response, including data privacy breaches as well as operational impacting safety [CyBOK resources]
  - This will introduce the students to the existence of a parallel large and complex ecosystem of management, organisational "processes" (one of the three categories of control) that will need to be taken into account as part of their investigation
- 1 hour lecture on human factors from the cybersecurity perspective, covering a range of topics including (i) users of the system and the broader ecosystem and the role of the human (ii) types of attackers, their motivations (iii) (three types of vulnerabilities: NCSC 2016)
  - This will introduce the safety community to the significantly increased role that malicious actors play when considering disruptions of digital technologies, which is not something that is always prioritised in a safety-led accident investigation

Recommendations for additional lectures (2/2)

The comparison between (safety) accident investigation syllabus themes and CyBOK themes also identified a few gaps potentially requiring targeted lectures. This is in addition to material specific to Attacks and Defences

- 1 hour lecture on forensics and data gathering including challenges and processes to be followed, defining the specific and measurable differences between the two disciplines, safety and cybersecurity
- 1 hour lecture on key data for maritime operations and how it can be modified (covering the categories of incidents e.g. navigation and positioning, maintenance and operations, emergency response, non-safety-critical systems, office-based systems and emerging technology e.g. IoT)

Part 4: Teachable scenarios (scenario themes)

Identification of six “reasonably foreseeable scenarios”*

Selected to mesh with safety-led mindset and teachability within an accident investigation context rather than reflect solely cybersecurity priorities i.e. what a CISO or another cyber professional would focus on

Technology-based scenarios developed following review

By necessity, some reasonably foreseeable scenarios with a high technical content (NB: majority of the CyBOK syllabus) cannot be included in the baseline approach (part 3).

*****’*Reasonably foreseeable scenarios’ is a term with a legal context related to application of health and safety legislation. Broader legal analysis and assessment not provided as part of this study.*

Context for development of teachable scenarios (1/2)

There is a need for digitally-based scenarios that encompass elements of cybersecurity, aligning to a (safety) accident investigation course

- Accident investigation incorporates a range of uncertainties and is process-driven (gathering of evidence) and requires a high level of applied skills, and knowledge
- An accident investigator needs to be able to appreciate digital factors such as
  - Complexity of the architecture: systems of systems, emergent properties and absence of clearly defined system boundaries
  - Role of the non-human in incident precursors and actions e.g. automated embedded routines
  - Difficulty in gathering and understanding digitally-based information as well as actions taken on that information, and by whom or what those actions were made

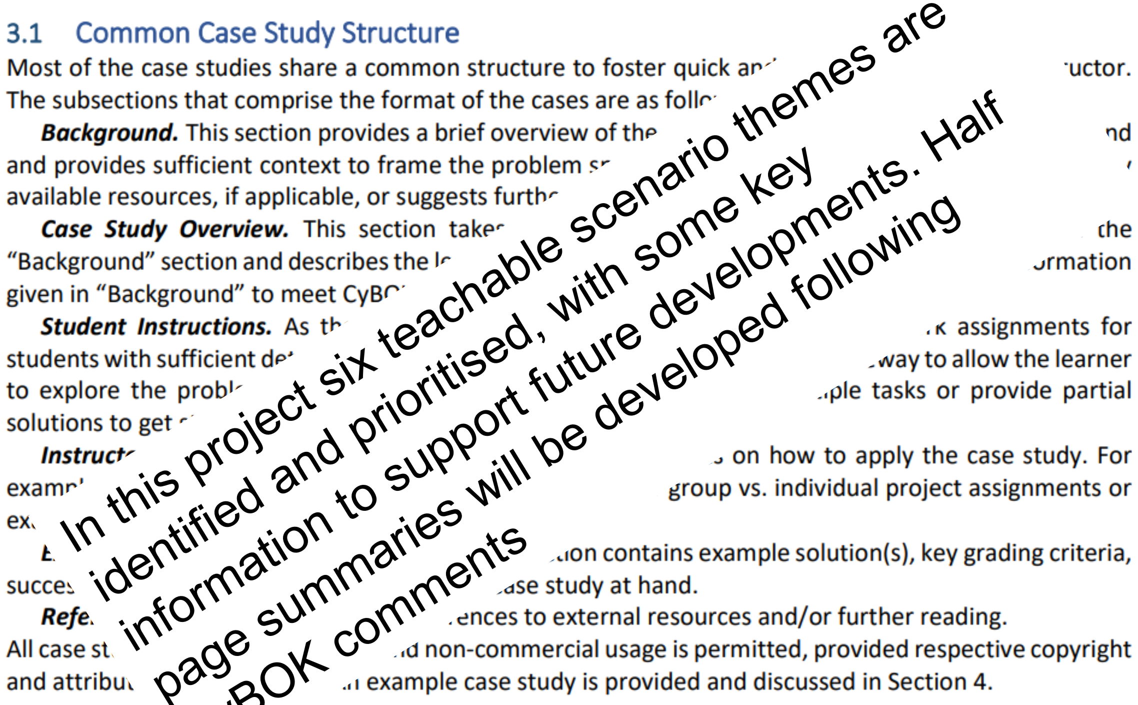
Context for development of teachable scenarios (2/2)

There is a need for digitally-based scenarios that encompass elements of cybersecurity, aligning to a (safety) accident investigation course

- Reading of reference information alone will not help develop these applied skills
- Selected industry trade association material (e.g. ENISA) is used to introduce the topic within a sector context, and themes underpinning scenarios identified
- Literature review used to identify source material from which scenarios can be developed
- AI, blockchain and other related activities are not covered in the scope of this project

CyBOK teaching scenarios

Issues with teaching safety alongside cybersecurity already noted by CyBOK. For this early pedagogical TRL work, based on initial screening, fully developed scenarios are not provided as the safety/cybersecurity crossover is not yet mature



3.1 Common Case Study Structure

Most of the case studies share a common structure to foster quick an uctor. The subsections that comprise the format of the cases are as follo

Background. This section provides a brief overview of the nd and provides sufficient context to frame the problem s , available resources, if applicable, or suggests furth

Case Study Overview. This section take the "Background" section and describes the l ormation given in "Background" to meet CyBO

Student Instructions. As th k assignments for students with sufficient de way to allow the learner to explore the probl ple tasks or provide partial solutions to get

Instruct on how to apply the case study. For examp group vs. individual project assignments or ex

E ion contains example solution(s), key grading criteria, succes ase study at hand.

Refe ences to external resources and/or further reading.

All case st d non-commercial usage is permitted, provided respective copyright and attribu n example case study is provided and discussed in Section 4.

In this project six teachable scenario themes are identified and prioritised, with some key information to support future developments. Half page summaries will be developed following CyBOK comments

"Even though the core concepts of safety and cybersecurity are comparatively relatable, students seemingly struggled less in finding, e.g., threats as opposed to hazards. Cybersecurity concepts seemed to be almost intuitively understandable, while safety concepts were not"

ENISA baseline

The following reports are used to provide cross-sector guidance (NCSC resources may also be used)

enisa

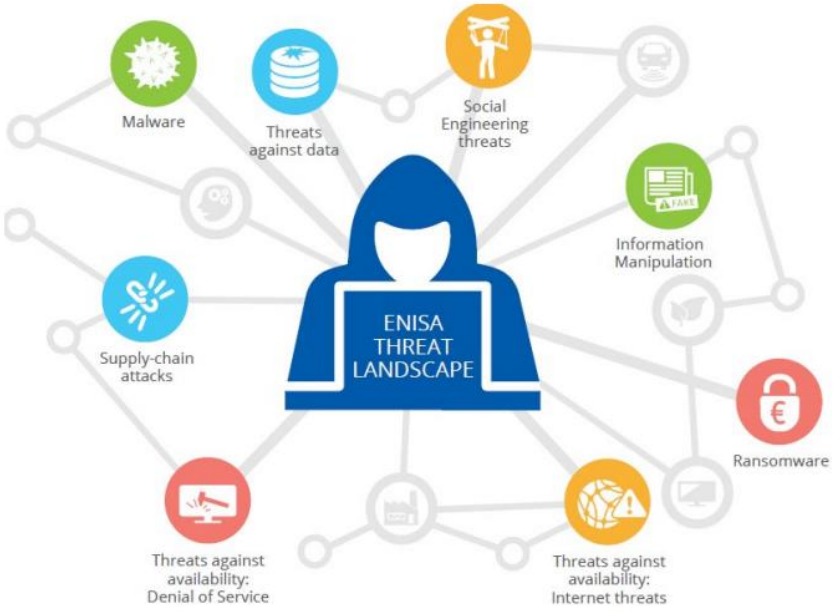
EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA THREAT LANDSCAPE 2023

July 2022 to June 2023

OCTOBER 2023

Figure 1: ENISA Threat Landscape 2022 - Prime threats


Malware
Threats against data
Social Engineering threats
Information Manipulation
Supply-chain attacks
ENISA THREAT LANDSCAPE
Ransomware
Threats against availability: Denial of Service
Threats against availability: Internet threats

enisa 20 years!

EUROPEAN UNION AGENCY FOR CYBERSECURITY

THREATS 2030

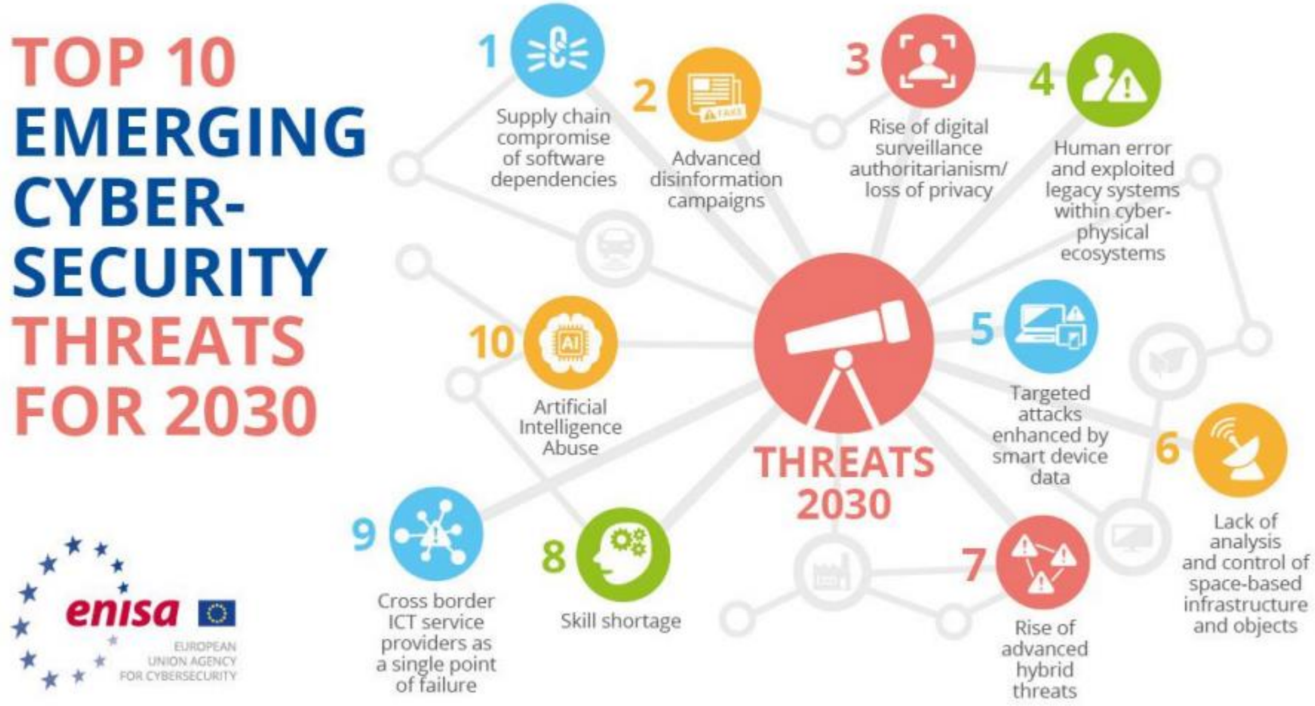
FORESIGHT CYBERSECURITY THREATS FOR 2030 – UPDATE

Executive Summary

MARCH 2024

A forward look profile

Figure 2: Top 10 threats



TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030
1 Supply chain compromise of software dependencies
2 Advanced disinformation campaigns
3 Rise of digital surveillance authoritarianism/ loss of privacy
4 Human error and exploited legacy systems within cyber-physical ecosystems
5 Targeted attacks enhanced by smart device data
6 Lack of analysis and control of space-based infrastructure and objects
7 Rise of advanced hybrid threats
8 Skill shortage
9 Cross border ICT service providers as a single point of failure
10 Artificial Intelligence Abuse
THREATS 2030
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

(Items 1, 4, 6, 8, 9 baselined in development of teachable scenarios in this project)

Increased attack surface in line with increased use of cloud, remote access, data management and supply chain (complexities) highlighted

Increasing number of incidents and near-misses of digital origin with potential safety impact, with ongoing trends in under reporting/under analysis.

This under reporting is key as safety (accident investigation) is strongly evidence and prior incident driven in terms of focus, techniques. Under reporting has a significant impact on teachability of cybersecurity

Methodology for identification of teachable scenario themes (1/2)

Initially (in proposal), it was suggested that safety and cybersecurity culture and management system differences might form basis of scenarios

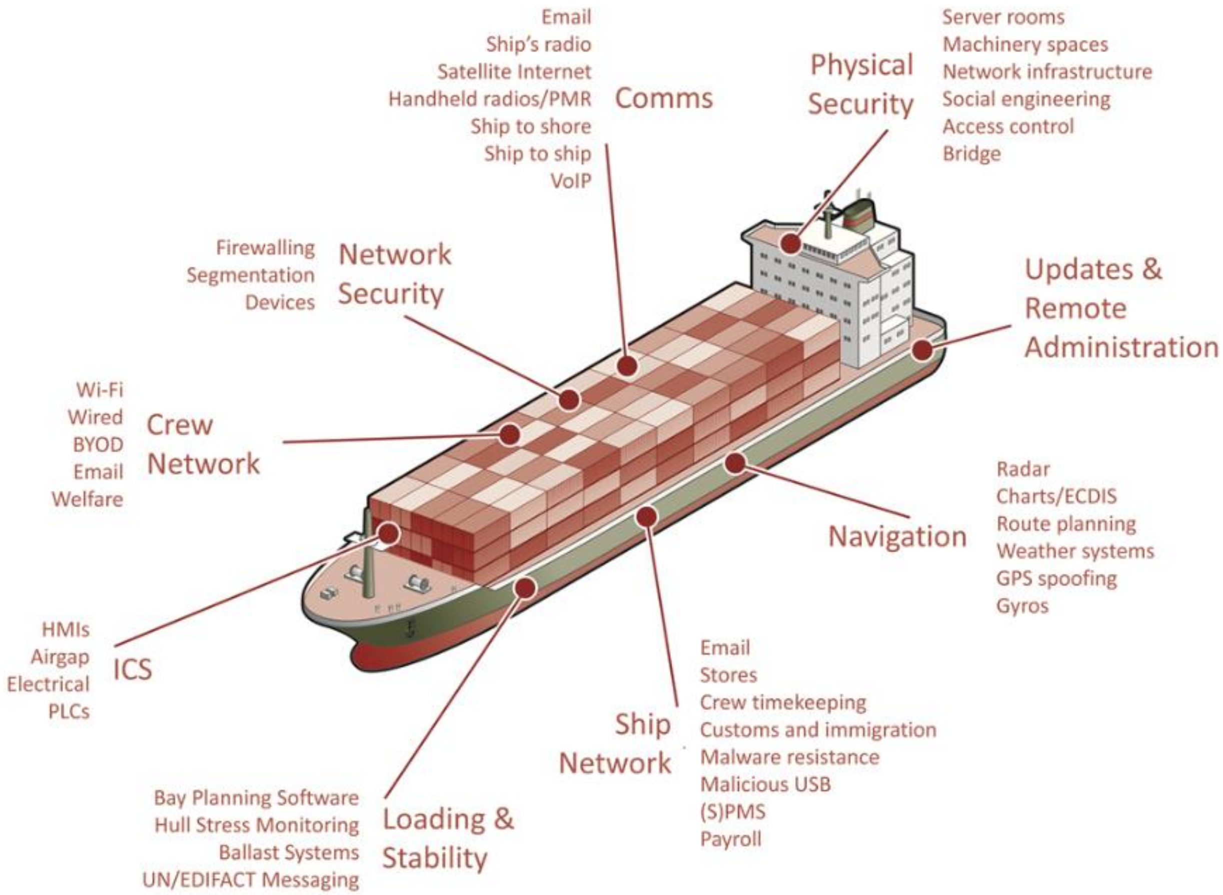
- Recommendations for development of scenarios were initially based on one or more of “people, plant, process” elements, evaluating how CyBOK can be embedded to safety (accident investigation) syllabus
- Literature review of cybersecurity culture versus safety culture carried out, limited evaluation of crossover topics
- In addition, there was limited scenario analysis of the crossover between two management systems
- A maritime-focussed review of recent cybersecurity incidents [Transnav paper] combined with review of recent DfT maritime research [MAR-RI programme] provided the guidance to the study leads that increasing digitalisation of the sector meant a more technologically focussed approach was appropriate

Methodology for identification of teachable scenario themes (2/2)

Initially (in proposal), it was suggested that safety and cybersecurity culture and management system differences might form basis of scenarios

- As teaching of accident investigation examples is sector-based, it was decided to focus on maritime as an example (covers international context, complex and moving systems, and legacy to emerging technologies)
- Six teachable scenarios A-F were defined as part of the project, designed to teach selected CyBOK core concepts, composite of references review (next slides)
- They are all linked, directly or through multiple steps, to collision (other vessels, shore, seabed or other), with follow on to fire, evacuation and/or oil spill (or other environmental impact) as a consequence of the collision. These consequences form the baseline of (safety) accident investigation training and implementation in the field

Cyber vulnerabilities outlined



PenTestPartners website and supporting resources

- Some general trends underpinning physical and virtual networks
- "While increased connectivity between ships, personal devices, and on-shore infrastructure has improved operational efficiency and physical safety, it also increases vulnerabilities across IT and OT systems"
- Use of cloud, remote access, data management and supply chain are underpinning themes across many reasonably foreseeable scenarios
- Maintenance is carried out over the air (OTA), local (USB etc.) for both safety and non-safety critical systems

A sample summary of incidents

Further scrutiny of the references has identified limited in-depth full academic publications, references below include general media articles

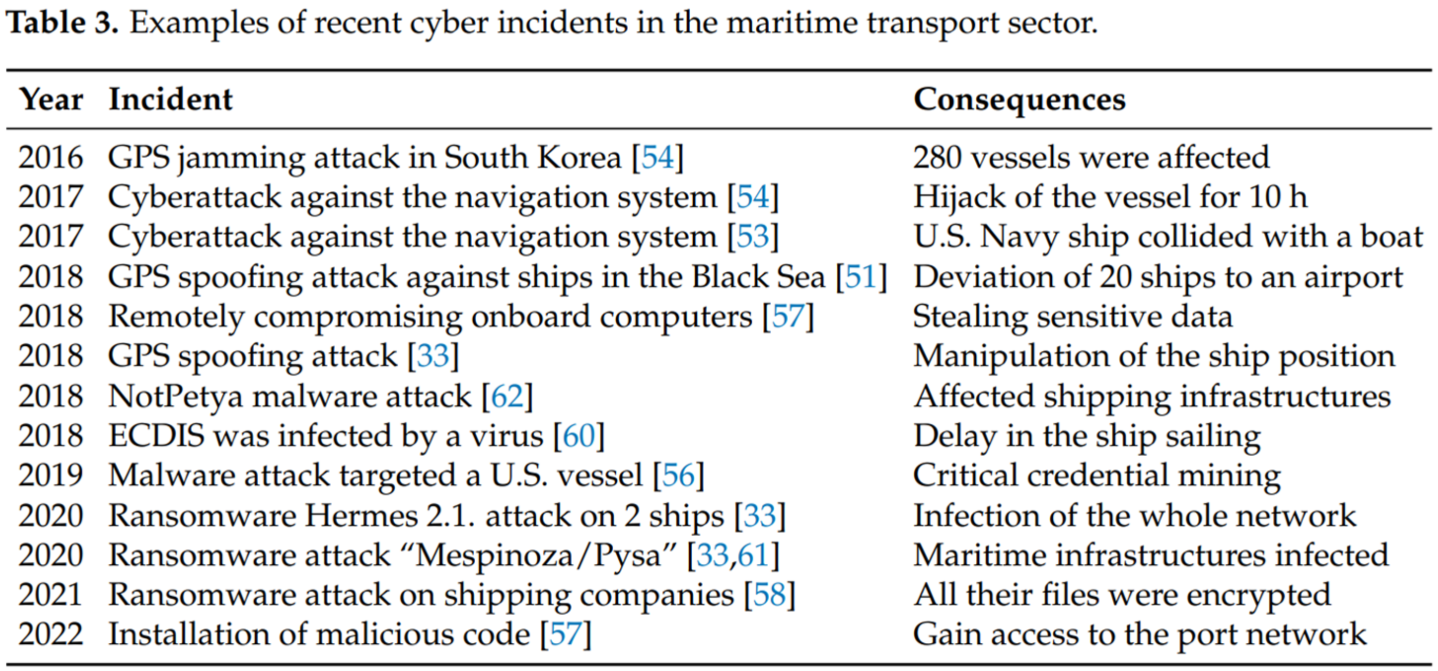


Table 3. Examples of recent cyber incidents in the maritime transport sector.

Year	Incident	Consequences
2016	GPS jamming attack in South Korea [54]	280 vessels were affected
2017	Cyberattack against the navigation system [54]	Hijack of the vessel for 10 h
2017	Cyberattack against the navigation system [53]	U.S. Navy ship collided with a boat
2018	GPS spoofing attack against ships in the Black Sea [51]	Deviation of 20 ships to an airport
2018	Remotely compromising onboard computers [57]	Stealing sensitive data
2018	GPS spoofing attack [33]	Manipulation of the ship position
2018	NotPetya malware attack [62]	Affected shipping infrastructures
2018	ECDIS was infected by a virus [60]	Delay in the ship sailing
2019	Malware attack targeted a U.S. vessel [56]	Critical credential mining
2020	Ransomware Hermes 2.1. attack on 2 ships [33]	Infection of the whole network
2020	Ransomware attack "Mespinoza/Pysa" [33,61]	Maritime infrastructures infected
2021	Ransomware attack on shipping companies [58]	All their files were encrypted
2022	Installation of malicious code [57]	Gain access to the port network

TRANSNAV
http://www.transnav.eu

the International Journal
on Marine Navigation
and Safety of Sea Transportation

Volume 15
Number 3
September 2021

DOI: 10.12716/1001.15.03.04

A Retrospective Analysis of Maritime Cyber Security Incidents

P.H. Meland[1], K. Bernsmed[1], E. Wille[1], Ø.J. Rødseth[2] & D.A. Nesheim[2]
[1] SINTEF Digital, Trondheim, Norway
[2] SINTEF Ocean, Trondheim, Norway

Range of automation systems

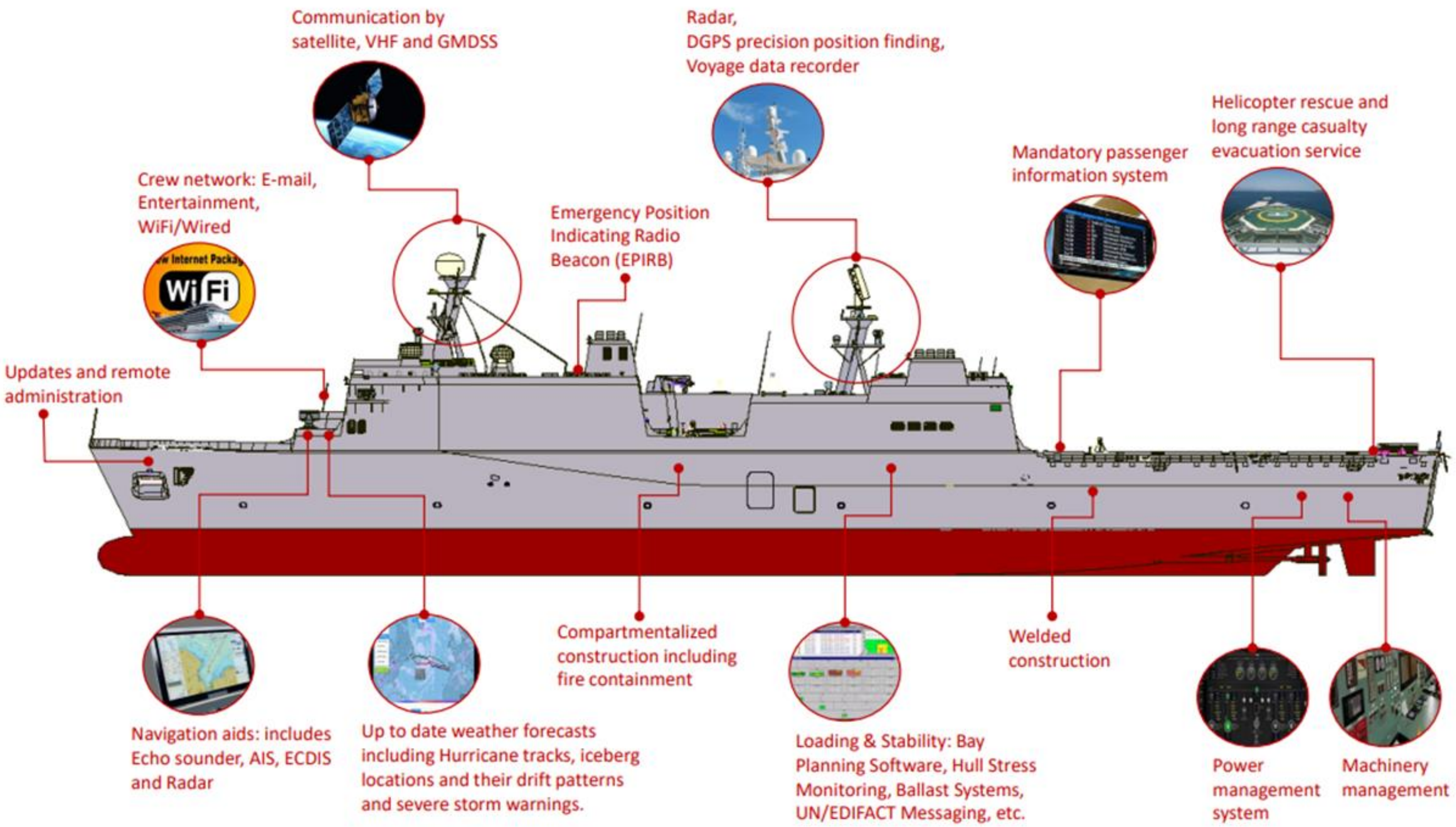

Communication by satellite, VHF and GMDSS
Radar, DGPS precision position finding, Voyage data recorder
Helicopter rescue and long range casualty evacuation service
Mandatory passenger information system
Crew network: E-mail, Entertainment, WiFi/Wired
Emergency Position Indicating Radio Beacon (EPIRB)
Updates and remote administration
Compartmentalized construction including fire containment
Welded construction
Navigation aids: includes Echo sounder, AIS, ECDIS and Radar
Up to date weather forecasts including Hurricane tracks, iceberg locations and their drift patterns and severe storm warnings.
Loading & Stability: Bay Planning Software, Hull Stress Monitoring, Ballast Systems, UN/EDIFACT Messaging, etc.
Power management system
Machinery management

Figure 1. Automation systems for modern and autonomous ships [13].

Teaching network concepts is key

Exposed systems represent a relatively high proportion of incidents/potential incident types

🟦 Carrier IT-system	🟦 Shipping company IT-system	🟦 Port IT-system	🟦 IT- systems onboard ships	🟦 IT- systems offshore installation	🟦 Communication systems
🟦 IT-systems subcontractors	🟦 IT-systems shipyards	🟦 IT-systems service providers	🟦 IT-systems onshore installations	🟦 IT-systems regulators	🟦 IT-systems research facilities
🟧 Espionage on maritime operation	🟧 Economic fraud	🟩 Misuse of AIS and positioning data	🟩 Manipulation of GNSS-signals used by ship	⬛ Other categories to be identified	🟦 *Exposed systems (blue boxes)*

Transnav

Orange: not in scope
Green: in scope but not an exposed system

Network and communication interfaces are highlighted, context for scenarios

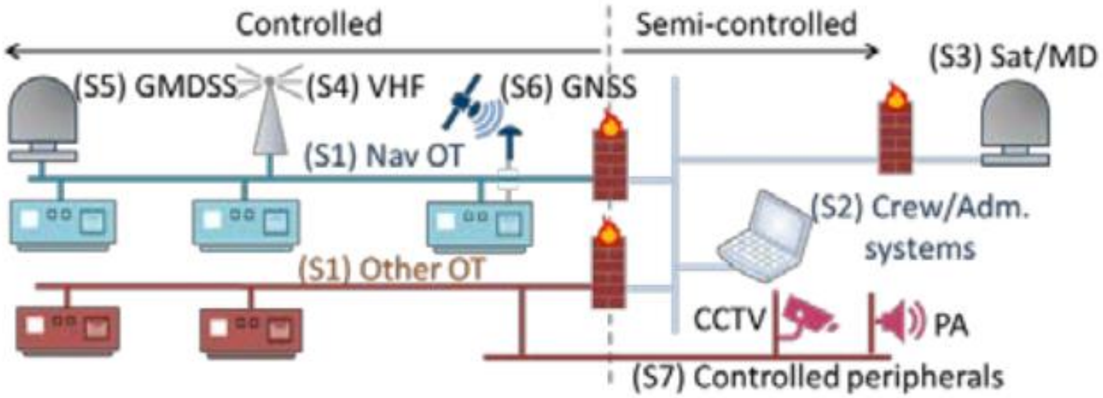
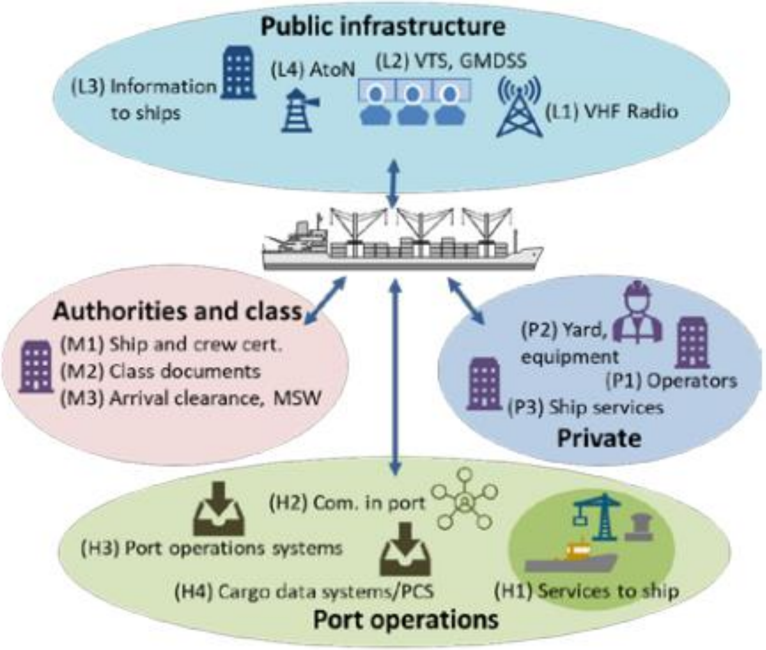


Figure 1. Attack points onboard the ship



Transnav

Figure 2. Attack points onshore and between ship-and-shore

Scenario A. Position and direction
“You are not where you think you are”

Navigation related incidents form a significant proportion of incidents considered in (safety) accident investigation analyses

- GNSS denial
- GPS Spoofing
- Interference with navaids
- ECDIS
- Slight course adjustment leading to collision or arrival elsewhere (piracy?)
- Ships “moored” at airports
- Modification of maps e.g. depth (bathyspheric) data
- Where short videos available, these can be added to the scenario illustration False AIS Data in Cyber-Attack Scenario (youtube.com)

Scenario B. Maintenance and operations “Systems are not as expected”

Significant proportion of digital technology updates are carried out as part of BAU (business as usual)

- IT and OT systems both involved in operations
- Onshore and offshore updates, part of regular maintenance, upgrades or reactive fixes (patches).
- Operational data, administrative information can be subject to attack
  - Ballast misloaded, leading to capsize or other operations
  - This scenario can also include port operations, interfering with vessel manifest etc.
  - Elements of automation – from automated cranes to trucks moving the containers.

Scenario C: Emergency procedures “Limited time, inaccurate information”

(Safety) accident investigators often conduct in depth reviews of operations under emergency procedures

- Full range of operational systems may be involved including HMI systems and data
- Scenario theme includes “big red button” emergency override, control of ship goes manual (opportunity to set independent control of two separate propellers)
- System design may mean that control passes or is perceived to pass to the wrong location (e.g. local not - as perceived - to the emergency control)
- Theme also includes manual override of emergency fire-fighting systems, communications and more
- For computer-controlled ship, malware on the network could also create loss of control
- Whilst the scenario theme is technologically-based, human factors and design of emergency procedures will be key

Scenario D: Not important for safety? “Safety-critical or non-safety critical?”

Perception within safety discipline that safety-critical systems are more important for safe operation, this discounts impact of disruption and/or network and data interactions across networks (“air gaps” can be ineffective)

- Factors to consider in in this scenario include:
  - Use of Windows-based systems (safety-critical or non-safety critical)
  - Flat network, shared resources, rather than segregated networks
  - Shodan (or other) ship-based system identification, network visibility
  - OT/IT separation not maintained in practice
- Updates of entertainment systems, passenger wifi, some operational information displays are not treated as safety-critical and so subject to less stringent controls, nor in depth evaluation of cybersecurity vulnerabilities.
- Increasing number and openness of digital connections (whether maintenance data to cloud, use of BYOD, or greater internet connections for staff (welfare connections) further ‘blurs the line’ between safety-critical and non-safety critical

Scenario E: Good office hygiene, afloat, onshore “Email, USB, YouTube links”

Generic IT cyber may provide a context for teaching (safety) accident investigation, although the lack of immediate link to safety means that other scenarios will need to be used alongside

CyBOK material can be used across a range of topics (samples include)

  - Shared passwords, hardcoded etc.
  - Phishing, Vishing and other social engineering including targeting senior decision makers
  - (Full list of topics not included here)

- The role of administration servers is key e.g. this example (TransNav analysis)
  - *“A tanker near the port of Naantali in Finland gets its administration server infected by ransomware. The backup disk is also wiped. Remote Desktop Protocol (RDP), a USB device or an email attachment are identified as probable attack vectors. The same vessel is infected again 4 months later near the same port”*
- Port ransomware attack, interaction between IT and OT for operations can also be highlighted

Scenario F: Emerging technology

A wide range of technological developments across multiple sectors represent future areas for (safety) accident investigation

- Examples of emerging technology in the maritime sector include
  - OT networks managing ship-based batteries as part of reducing emissions
  - ML on depth data, dynamically changing depth charts, rate of change (extending to attacks on AI data sets)
  - Parent vessel and autonomous network of mini-UAVs (surface or submarines)
  - Alternative to GNSS using radar and maps
  - MASS (maritime autonomous surface ships)
  - Autonomous mooring and bunkering for hydrogen
  - Port authority movement control of autonomous vessels

Next steps in scenario development (1/2)

Further development is needed but need to avoid modifying the scenarios for “acceptability” (believability) or perceived likelihood of occurrence and continue to focus on teachability

A number of factors will influence how scenarios play out in an international student cohort e.g.

- Multiple cultures, regulatory regimes for global operators and different country investigation methods will impact the investigation process, these will influence student use of scenarios
- How different regulators interact e.g. ICO fines/GDPR may end up driving IS/OT/IT modifications to improve cyber
- Cultural factors in communication, addressing rumours (and press) is an integral part of accident investigation
- Wide range of technical maturity of systems, across e.g. seafaring nations, so highlighting the existing use of legacy technologies (e.g. floppy disks, removable media) and their vulnerabilities without national/commercial characterisation

Next steps in scenario development (2/2)

Further development is needed but need to avoid modifying the scenarios for "acceptability" (believability) or perceived likelihood of occurrence and continue to focus on teachability

- Further skills development needs will shape more in-depth scenario development
  - Being able to rule out cyber is also an integral part of investigation, next stage in skills development will include being able to "rule in, rule out" possible causes
  - Increased awareness of the relative vulnerability of shoreside IT systems to cyberattack (including shared IT services across multiple operators or locations and complex supply chains) will enable better investigative approaches used by students
  - Accident investigators consider safety-related incidents but also the broader area of environmental impact (spills etc.) therefore cyber-attacks on control systems involved in environmental response will also need to be considered

Part 5: Priority ranking

Ranking of scenarios from part 4 on

Priority for teaching to accident investigators (perspectives from safety academics, cyber academics)

Ranking is not designed to confirm priority for action and/or likelihood of occurrence/severity of impact but the “fit” with (safety) accident investigation mindset, and opportunity for insertion into the syllabus.

Teachability (reasonably foreseeable scenarios, gamification) and pedagogical approaches covered in Part 6

Consultation on priority scenarios

Exercise: Rank the scenarios to the teaching of cybersecurity within a (safety) accident investigation MSc. (#1: Most important). Carried out in 1-2-1 conversations.

Biggest differences between safety and cybersecurity are for scenarios E and F, opposite ends of priority scale

Scenario	Teaching academic #1 (Safety, accident investigation)	Teaching academic #2 (Cybersecurity)	Teaching academic #3 (Cybersecurity)	Teaching academic #4 (Cybersecurity)
A (Position and direction)	=1	4	2	1
B (Maintenance and operations)	3	2	4	5
C (Emergency procedures)	4	3	=1	4
D (Safety-critical versus non-safety critical)	=1	1	3	3
E (Good office hygiene, afloat, onshore)	5	=1 **	=1	2
F (Emerging technology)	2	5	5	6

**: Should be taught to all

Teaching academic #1 additional comments (including aviation context)

- A (Position and direction)
  - In aviation there are some emerging situations where, due to GPS issues, ground proximity information is producing unusual data (“ground not where it’s expected to be”) in flight leading to a driver for inflight decision making (outside of normal protocols), whether it’s disabling a system, turning a system on and off or putting in place other operational procedures as a work around. This increases potential for accidents and near misses
- B (Maintenance and operations)
  - Falsifying records may be created by economic (e.g. sanctions) or other non-technical situations, in addition to drivers for modifying or deleting data (lack of availability impacting operations)
- C (Emergency procedures)
  - There is the potential for overwhelm, including both cybersecurity and safety-related malfunctions across multiple systems, people then don’t know which data to trust. Similarly, overreaction (course correction) at speed can lead to loss of control event
- D (Safety-critical versus non-safety critical)
  - Legacy systems get updated and upgraded over time, and both safety-critical and non-critical and network segmentation, whilst assumed, may still not be in place. Equally legacy system design has inherent safety challenges e.g. where two networks are interconnected, fire suppression and engine bus control, meaning that an inflight incident resulted in fatalities (Swissair Flight 111 – Wikipedia)
- E (Good office hygiene, afloat)
  - This is recognised as important in the professional (and personal) spheres but the contribution to (safety) accident investigation is underappreciated
- F (Emerging technology)
  - Whilst incidents with emerging tech haven’t yet been investigated in significant numbers, there is a need for the investigator community to accelerate their learning, but there is some reluctance to do so
- Cross-cutting theme of the potential for “claim” of access being sufficient to create an adverse response. For example, it’s only sufficient to suggest that (aviation) IFE (in-flight entertainment) has been accessed and used to modify the pilot flight deck control and for passengers to believe it. Technical access doesn’t need to be achieved.

Teaching academic #2 additional comments

- A (Position and direction)
  - In practice position modification is more difficult to achieve in the real world than theory, via GPS transmitters (specifications, power etc. above a threshold)
- B (Maintenance and operations)
  - Likely biggest clash between safety and cybersecurity. Perception that safety-critical systems are safety “certify then freeze”, whilst cyber “fix it now”.
- C (Safety-critical versus non-safety critical)
  - Safety/safe operations impacts broad range of systems, but safety specialists may not be interested in non-safety critical
- D (Emergency procedures)
  - Likely to be a significant overlap but a disparity in approaches, unclear what a combined response might look like. May be benefit in showing safety (accident investigators) scenarios such as water plant cyber-attack (e.g. pollution of supply)
- E (Good office hygiene, afloat)
  - Should be taught to all. Consider teaching this first.
- F (Emerging technology)
  - Deep fakes and misinformation are the areas of concern, the broader political domain. Unclear how this impacts on safety.
- Cross-cutting theme of communications e.g. all phone calls are digital (VoiP)

Part 6: Teachability and Pedagogical approaches

- Incorporating cybersecurity into (safety) accident investigation teaching is an emerging field
- Early-stage prototyping (early TRL pedagogical equivalent) is needed
- A high-level assessment of the teachability of the scenarios to (safety) accident investigators is presented
- Gamification approaches to the teachable scenarios (reasonably foreseeable scenarios) considered
- Pros and cons of
  - Assessment methods (self and peer assessment)
  - Reflective judgement (CPD reflective practice)
  - Synchronous and asynchronous learning

Context for results

Process followed to evaluate and rank the scenarios

- Results here and in the previous section are based on professional judgement and then evaluated “by difference” with both safety and cybersecurity academics on an individual basis
- Self-assessment will be influenced by individual perceptions of the field
- “Immaturity” of the safety-security crossover discipline limits how far we can go
- Section 7 presents the results of a broader consultation with the safety community via a Safety and Reliability Society webinar

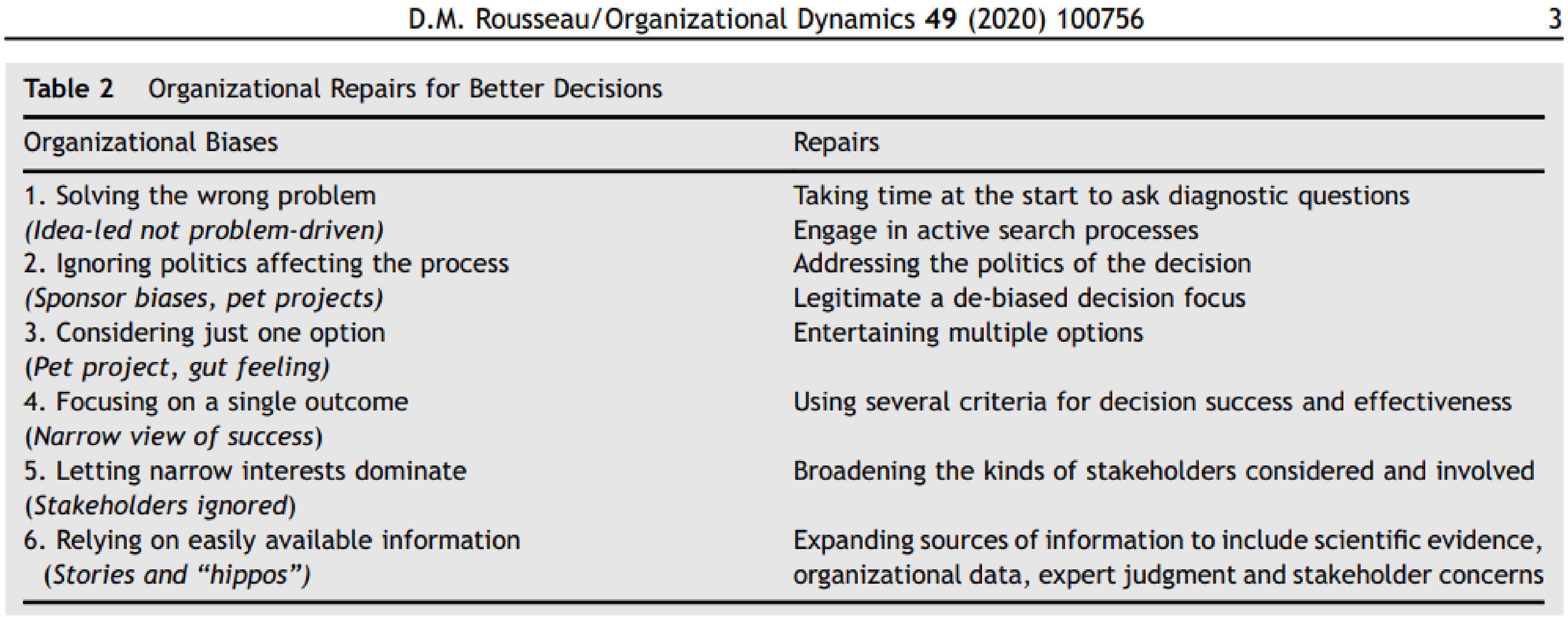
Review of teachability and pedagogical approaches across all scenarios

Scenario	Teachability through gamification (incl. ease of development and effectiveness of application)	Pedagogical approaches
A (Position and direction)	All scenario themes contain elements that can be readily developed and used in the education setting Detailed scenarios will need to be established in order for a teachability ranking to be implemented Ease of development (Low) Lots of existing material: A, E (Medium) Some resources: C, D (High) Low knowledge available: B, F	On review, lectures and small group discussions were identified as a preferred approach for delivery of the scenarios. Self and peer assessment (defined as students develop scenarios individually then discuss and rate as a group) is not preferred for (safety) accident investigators as at this time the gap between safety and cybersecurity is too great, and the students will want to be taught Asynchronous (incl. implementing deaf awareness principles for group discussion) to be looked at in further work. Reflective judgement (CPD reflective practice) may be beneficial once the inherent curiosity of accident investigators is combined with some cyber knowledge
B (Maintenance and operations)		
C (Emergency procedures)		
D (Safety-critical versus non-safety critical)		
E (Good office hygiene, afloat)		
F (Emerging technology)		

Gamification is defined as broadly following the ‘Decisions and Disruptions’ model

At early pedagogical TRL stages, organisational biases can’t yet be used

Initial proposal to use organisational biases as part of the consultation process not implemented due to the limited field experience of teaching cybersecurity scenarios to (safety) accident investigators. To be reconsidered in future phases of work, once student learners can be observed in the field using the scenarios developed in this phase of work



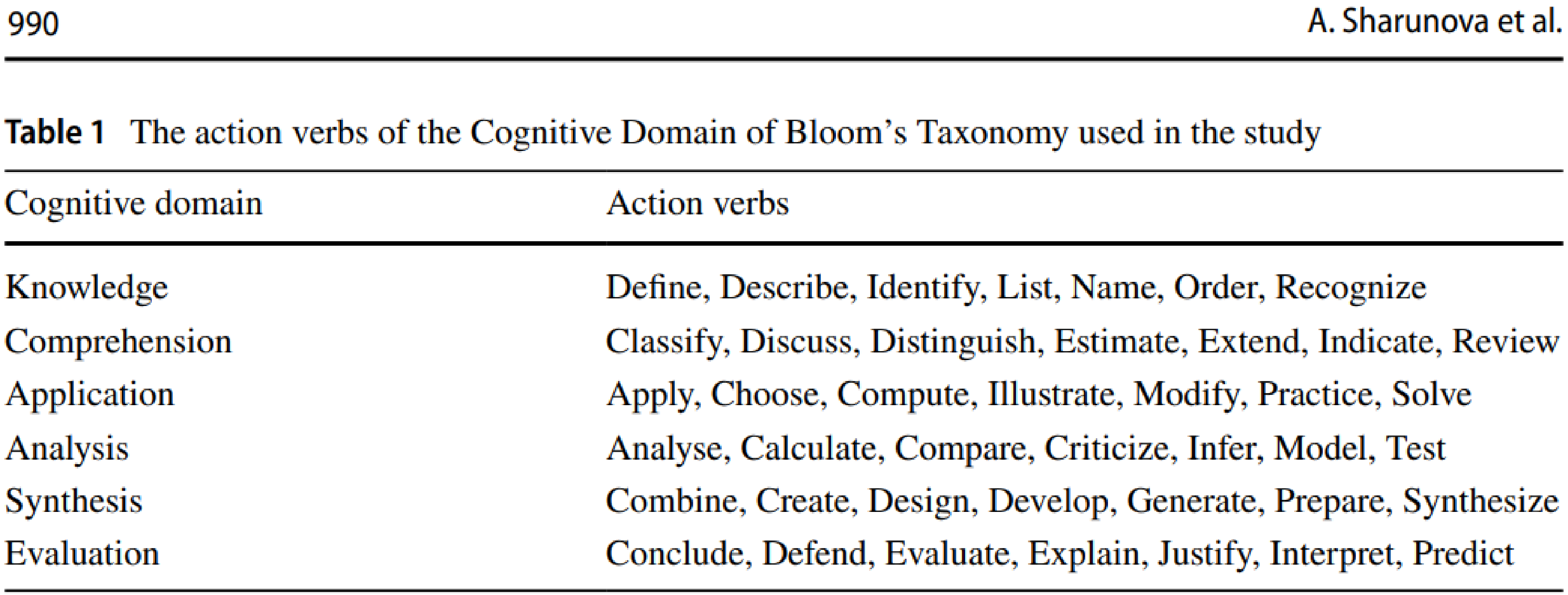
D.M. Rousseau/Organizational Dynamics **49** (2020) 100756 3

Table 2 Organizational Repairs for Better Decisions

Organizational Biases	Repairs
1. Solving the wrong problem	Taking time at the start to ask diagnostic questions
(Idea-led not problem-driven)	Engage in active search processes
2. Ignoring politics affecting the process	Addressing the politics of the decision
(Sponsor biases, pet projects)	Legitimate a de-biased decision focus
3. Considering just one option	Entertaining multiple options
(Pet project, gut feeling)	
4. Focusing on a single outcome	Using several criteria for decision success and effectiveness
(*Narrow view of success*)	
5. Letting narrow interests dominate	Broadening the kinds of stakeholders considered and involved
(*Stakeholders ignored*)	
6. Relying on easily available information *(Stories and “hippos”)*	Expanding sources of information to include scientific evidence, organizational data, expert judgment and stakeholder concerns

Bloom’s taxonomy

These thinking stages can be applied in future classroom-based tests of the scenarios, observation of student cognitive processes



990 A. Sharunova et al.

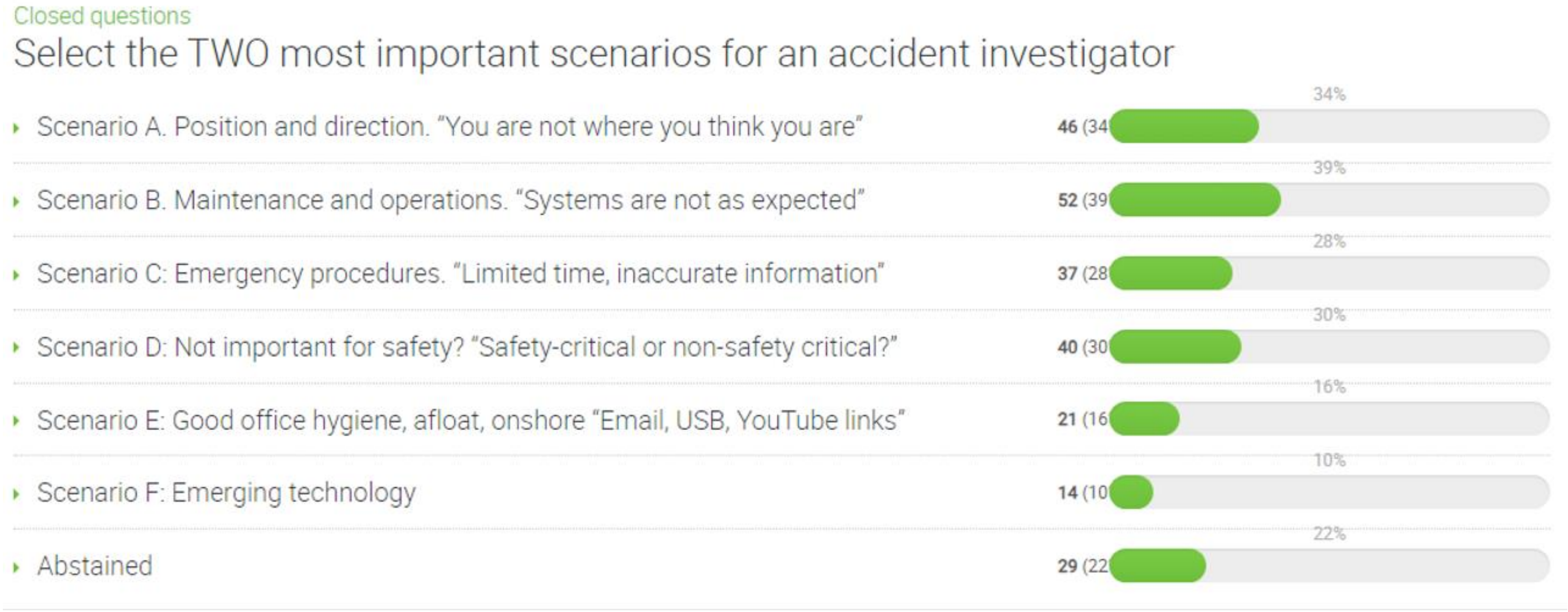
Table 1 The action verbs of the Cognitive Domain of Bloom’s Taxonomy used in the study

Cognitive domain	Action verbs
Knowledge	Define, Describe, Identify, List, Name, Order, Recognize
Comprehension	Classify, Discuss, Distinguish, Estimate, Extend, Indicate, Review
Application	Apply, Choose, Compute, Illustrate, Modify, Practice, Solve
Analysis	Analyse, Calculate, Compare, Criticize, Infer, Model, Test
Synthesis	Combine, Create, Design, Develop, Generate, Prepare, Synthesize
Evaluation	Conclude, Defend, Evaluate, Explain, Justify, Interpret, Predict

Part 7: Results and analysis of consultation with the safety community

- A webinar was held via the Safety and Reliability Society (SaRS) to present and seek feedback on the six scenarios developed
- SaRS is a Professional Engineering Institution that is focussed on safety and risk across multiple sectors
- Attendees at the free-to-attend webinars are global and come from a wide range of backgrounds
- 280 registered, 157 attended and 106 took part in the survey (29 abstained)

Scenario prioritisation by audience



Closed questions

Select the TWO most important scenarios for an accident investigator

Scenario A. Position and direction. “You are not where you think you are”	46 (34	34%
Scenario B. Maintenance and operations. “Systems are not as expected”	52 (39	39%
Scenario C: Emergency procedures. “Limited time, inaccurate information”	37 (28	28%
Scenario D: Not important for safety? “Safety-critical or non-safety critical?”	40 (30	30%
Scenario E: Good office hygiene, afloat, onshore “Email, USB, YouTube links”	21 (16	16%
Scenario F: Emerging technology	14 (10	10%
Abstained	29 (22	22%

Analysis of results

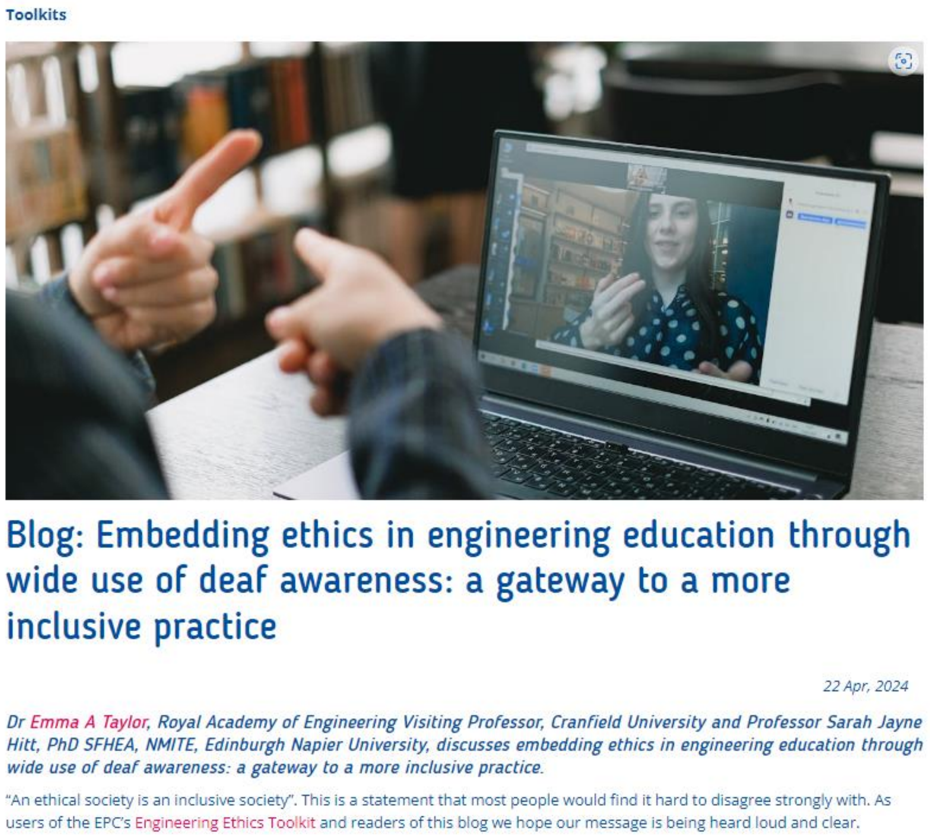
The survey results highlight a clear difference between safety and cybersecurity teaching academics and the generalist safety community

- The webinar respondents selected two scenarios (highest ranked selected by the most respondents, lowest ranked by the fewest)
  - B (Maintenance and operations)
  - A (Position and direction)
  - D (Safety-critical versus non-safety critical)
  - C (Emergency procedures)
  - F (Emerging technology)
  - E (Good office hygiene, afloat)
- In contrast, Scenario E was selected by the three cybersecurity academics as either the most important or second important, reflecting the current cybersecurity landscape
- Furthermore, the safety and accident investigation academic identified emerging technology as a high priority, again contrasting with the generalist safety community

Section 8: Deaf awareness

- Approaches to implementing deaf awareness in the teaching of safety and cybersecurity including scenarios are being considered as part of wider programme of work under the
- *Royal Academy of Engineering Visiting Professorship scheme, Digital Safety and Security*

Deaf awareness is linked to ethics, inclusive engineering and engineering education



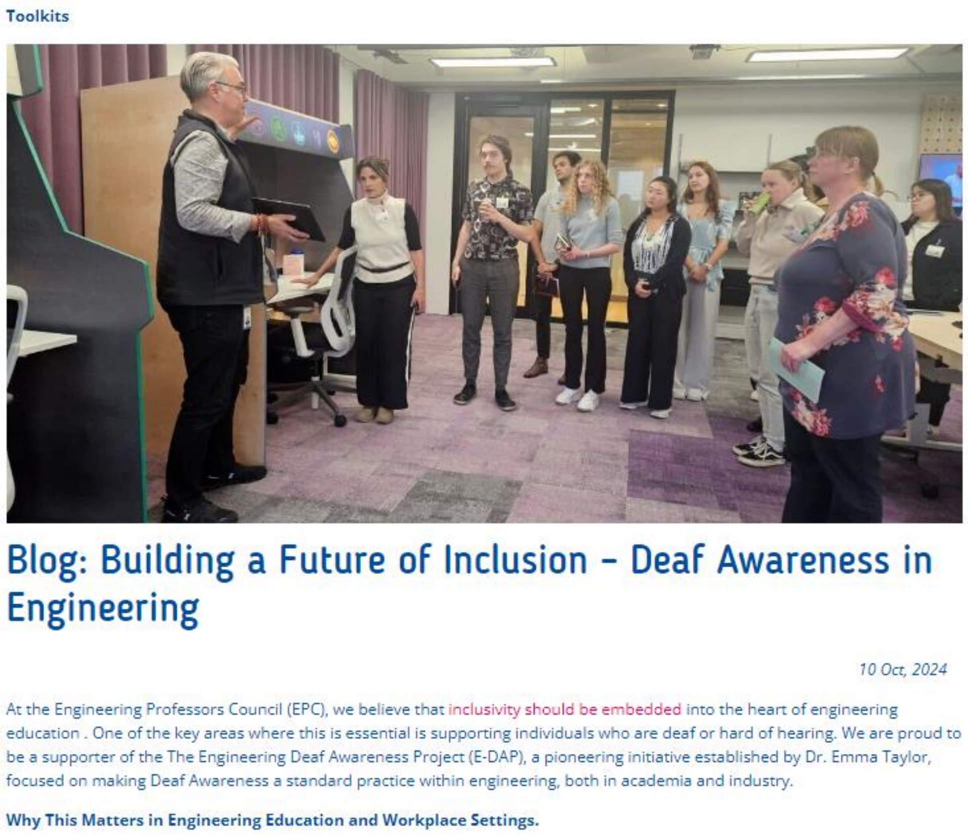
Toolkits

Blog: Embedding ethics in engineering education through wide use of deaf awareness: a gateway to a more inclusive practice

22 Apr, 2024

Dr Emma A Taylor, Royal Academy of Engineering Visiting Professor, Cranfield University and Professor Sarah Jayne Hitt, PhD SFHEA, NMITE, Edinburgh Napier University, discusses embedding ethics in engineering education through wide use of deaf awareness: a gateway to a more inclusive practice.

"An ethical society is an inclusive society". This is a statement that most people would find it hard to disagree strongly with. As users of the EPC's Engineering Ethics Toolkit and readers of this blog we hope our message is being heard loud and clear.



Toolkits

Blog: Building a Future of Inclusion – Deaf Awareness in Engineering

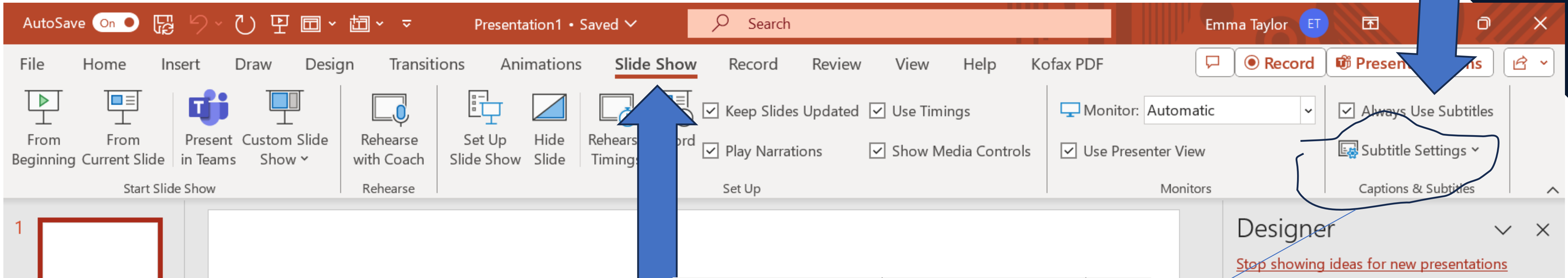
10 Oct, 2024

At the Engineering Professors Council (EPC), we believe that inclusivity should be embedded into the heart of engineering education . One of the key areas where this is essential is supporting individuals who are deaf or hard of hearing. We are proud to be a supporter of the The Engineering Deaf Awareness Project (E-DAP), a pioneering initiative established by Dr. Emma Taylor, focused on making Deaf Awareness a standard practice within engineering, both in academia and industry.

Why This Matters in Engineering Education and Workplace Settings.

[Blog: Embedding ethics in engineering education through wide use of deaf awareness: a gateway to a more inclusive practice - Engineering Professors Council (epc.ac.uk)]()
[Blog: Building a Future of Inclusion - Deaf Awareness in Engineering - Engineering Professors Council]()

Deaf awareness strengthens clear communication, understandable by all, key in accident investigation, education settings etc.



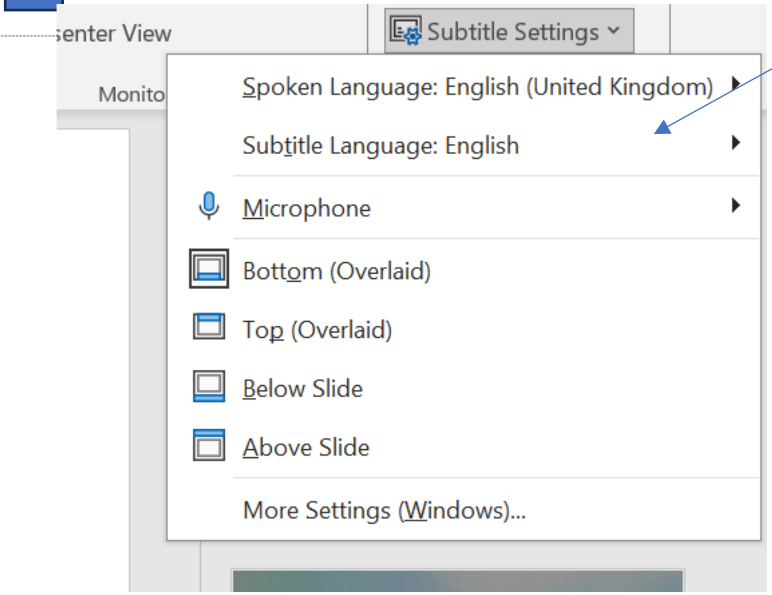
☑ Keep Slides Updated ☑ Use Timings

☑ Play Narrations ☑ Show Media Controls

Monitor: Automatic

☑ Use Presenter View

☑ Always Use Subtitles



Spoken Language: English (United Kingdom)

Subtitle Language: English

Part 9: Recommendations for further work

- This programme of work is an initial step towards identifying opportunities for integrating cybersecurity (based on CyBOK material) into the discipline of (safety) accident investigation
- This is an emerging field without established best practice, some topic areas require further work
- This includes how the three CyBOK security themes can be considered through using autonomous vehicles and cyber sensor attacks
- An evaluation is made of which elements of the HORA theme (human organisational regulatory aspects) should be prioritised in the next stages of this work
- A priority area is to address the perception of the safety community that general cybersecurity (Scenario E “Good office hygiene”) is a lower priority scenario than the others

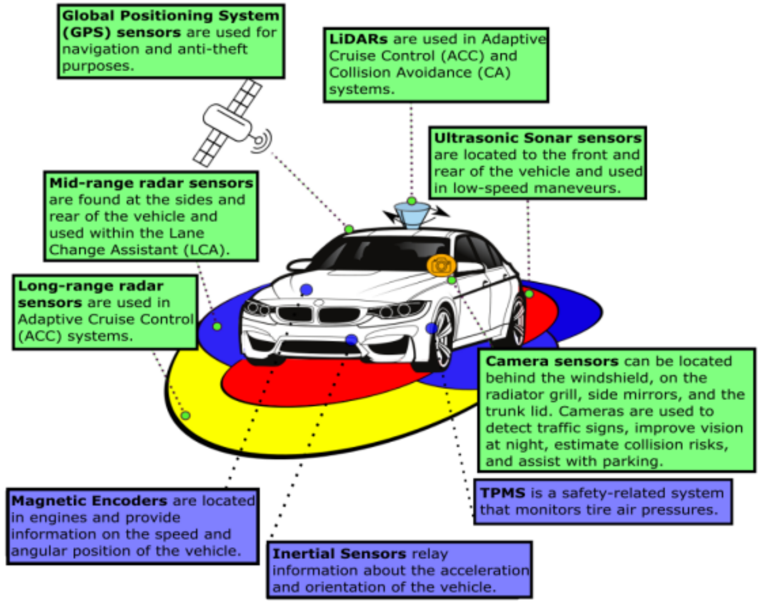
Part 9: Further work

A number of proposals for further work are made, additional information on points 1 and 2 in this section

1. Evaluate whether teaching of the 3 CyBOK themes (infrastructure security, systems security, software and platform security) to a non-technical audience can be enabled through “car sensor hack” scenarios. This builds on student familiarity with car-based sensors as part of their everyday activities
2. Consider development of teachable scenarios which are solely HORA (Human Organisational and Regulatory Aspects) and/or assess the feasibility of developing a HORA-only bolt-on to existing CyBOK scenarios using HFACS as a framework
3. Develop further the 5 x 1 hour lecture module topics (identified in Part 3)
4. Trial the output of this study and further work in a 2-day asynchronous Digital Safety Games across accident investigators (primarily non-technical, not engineers, postgraduate), with potential parallel exercise with multi-discipline engineering students who have received 2-day cybersecurity training undergraduate (new RAEng Visiting Professor funded 2024-2027). Embed elements of Scenario E (good office hygiene) and Scenario F (emerging technology).

1. Evaluate approaches to teaching 3 “security” elements of CyBOK syllabus

Use car-based scenarios as a framework to illustrate attacks and defences, and then introduce “security” (infrastructure, systems, software and platform)



Global Positioning System (GPS) sensors are used for navigation and anti-theft purposes.

LiDARs are used in Adaptive Cruise Control (ACC) and Collision Avoidance (CA) systems.

Ultrasonic Sonar sensors are located to the front and rear of the vehicle and used in low-speed maneuvers.

Mid-range radar sensors are found at the sides and rear of the vehicle and used within the Lane Change Assistant (LCA).

Long-range radar sensors are used in Adaptive Cruise Control (ACC) systems.

Camera sensors can be located behind the windshield, on the radiator grill, side mirrors, and the trunk lid. Cameras are used to detect traffic signs, improve vision at night, estimate collision risks, and assist with parking.

TPMS is a safety-related system that monitors tire air pressures.

Magnetic Encoders are located in engines and provide information on the speed and angular position of the vehicle.

Inertial Sensors relay information about the acceleration and orientation of the vehicle.

Fig. 2. Vehicle Dynamics Sensors (Blue) and Environment Sensors (Green) in Autonomous and Connected Vehicles

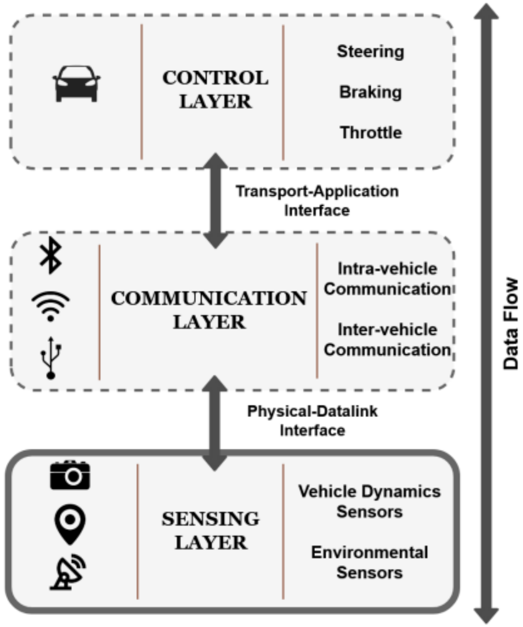


Fig. 1. Three-tier Connected and Automated Vehicle Architecture (AutoVSCC Framework)

El-Rewini et al, Cybersecurity Attacks in Vehicular Sensors, IEEE SENSORS JOURNAL, APRIL 2020

1. Trial teaching approach for CyBOK Security themes

Provisional half day course, 3x 1-hour lectures and group work exercise, building on the scenarios-based approach

- Outline three approaches to disrupting car operations
  - Dynamics: Magnetic encoders, inertial sensors
  - Tyre pressure monitoring systems
  - Sensors: LIDAR, ultrasonic, camera, radar, GPS etc.
- Summarise attacks and defences for each of the three approaches
- Highlight the role of one or more of infrastructure, systems and/or software and platforms security in allowing for attacks/implementing defences
- Compare sensors with human (OODA decision loop)
- Consider developing a further extension activity around ML based decision

1. Use human in the loop model OODA as a mental model to teach data

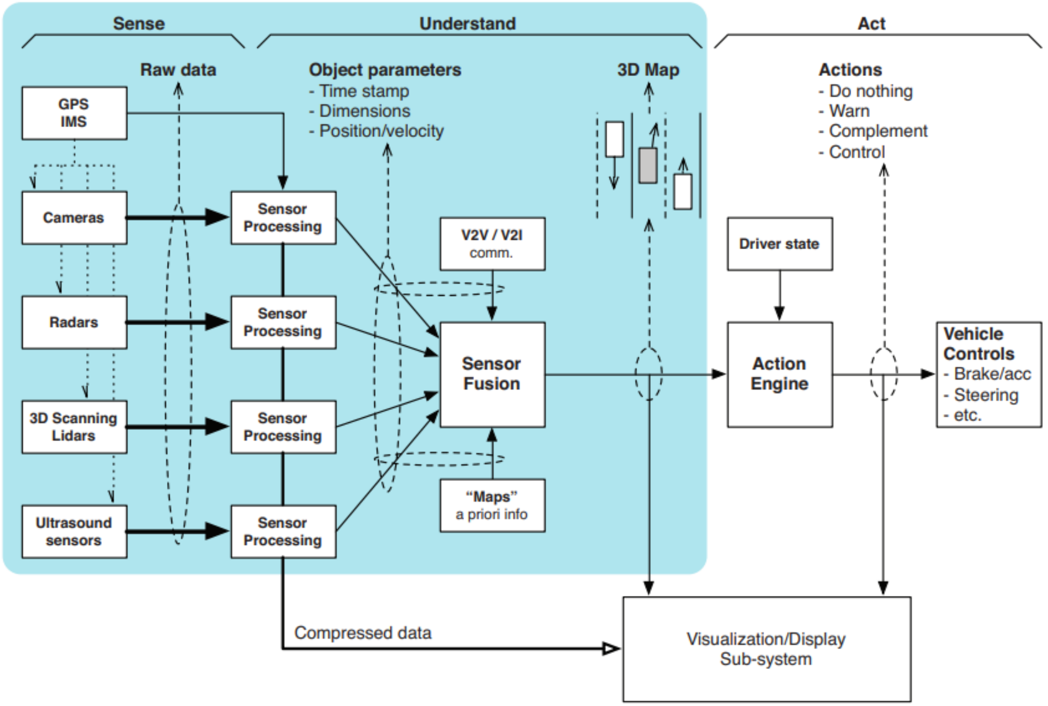
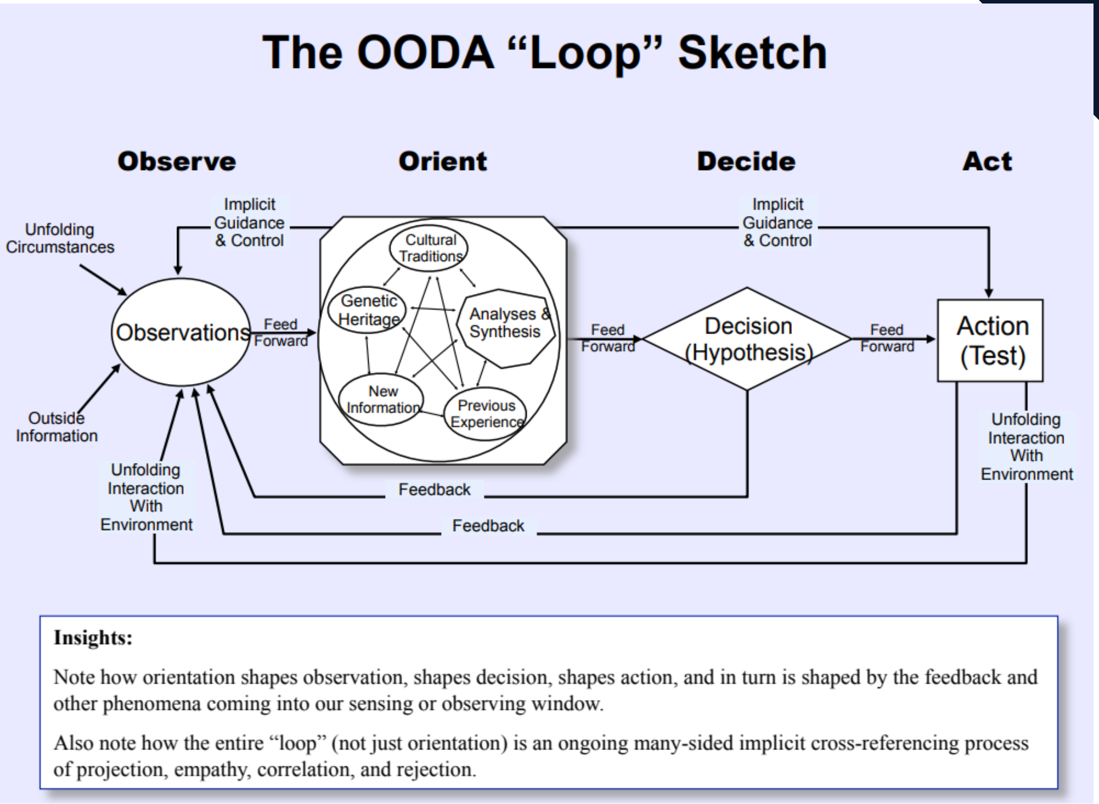


Figure 1: A functional view of the data flow in an autonomous car's sensing and control system [25].

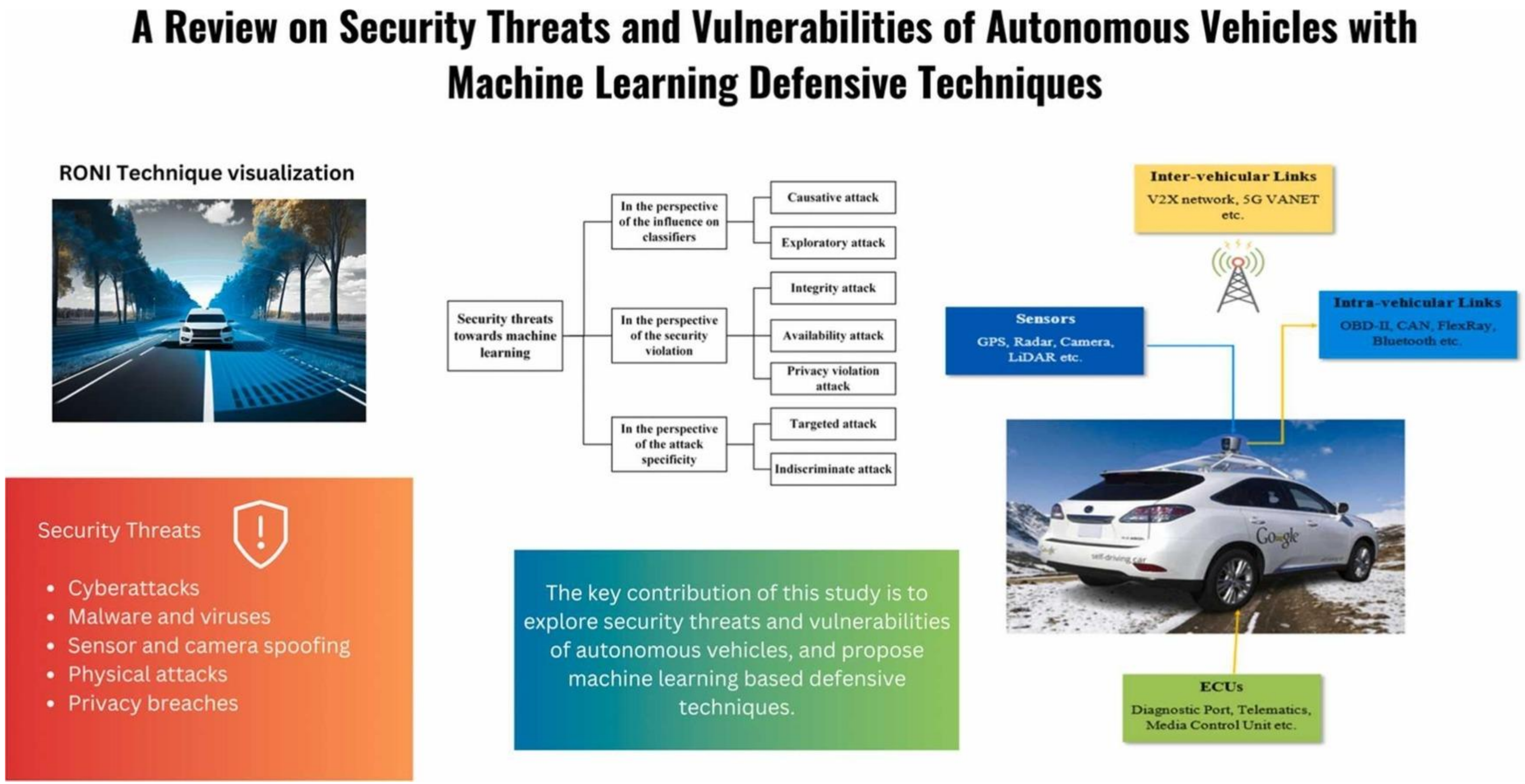


Insights:

Note how orientation shapes observation, shapes decision, shapes action, and in turn is shaped by the feedback and other phenomena coming into our sensing or observing window.

Also note how the entire "loop" (not just orientation) is an ongoing many-sided implicit cross-referencing process of projection, empathy, correlation, and rejection.

1. Develop student understanding of impact of ML on AVs



A Review on Security Threats and Vulnerabilities of Autonomous Vehicles with Machine Learning Defensive Techniques

RONI Technique visualization

Security Threats

- Cyberattacks
- Malware and viruses
- Sensor and camera spoofing
- Physical attacks
- Privacy breaches

The key contribution of this study is to explore security threats and vulnerabilities of autonomous vehicles, and propose machine learning based defensive techniques.

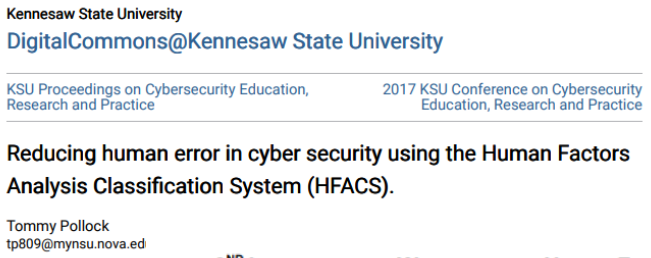
Security threats towards machine learning
In the perspective of the influence on classifiers
Causative attack
Exploratory attack
In the perspective of the security violation
Integrity attack
Availability attack
Privacy violation attack
In the perspective of the attack specificity
Targeted attack
Indiscriminate attack
Inter-vehicular Links
V2X network, 5G VANET etc.
Sensors
GPS, Radar, Camera, LiDAR etc.
Intra-vehicular Links
OBD-II, CAN, FlexRay, Bluetooth etc.
ECUs
Diagnostic Port, Telematics, Media Control Unit etc.
Google
self-driving car

Islam et al., Journal of Economy and Technology, Nov 2023

2. Develop bolt-on HORA case studies incorporating safety human factors

The role of human factors is well established in safety and accident investigation, including classification through HFACS and use of OODA

- CyBOK HORA (human organisational and regulatory aspects) material to be used as a baseline, with a focus on human factors as a “bridge” topic between safety and cybersecurity
- This will require bridging across to the people-led safety human factors perspective



Kennesaw State University

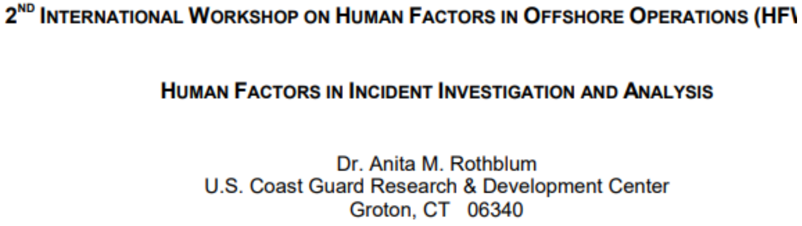
DigitalCommons@Kennesaw State University

KSU Proceedings on Cybersecurity Education, Research and Practice

2017 KSU Conference on Cybersecurity Education, Research and Practice

Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS).

Tommy Pollock
tp809@mynsu.nova.ed



2ND INTERNATIONAL WORKSHOP ON HUMAN FACTORS IN OFFSHORE OPERATIONS (HF

HUMAN FACTORS IN INCIDENT INVESTIGATION AND ANALYSIS

Dr. Anita M. Rothblum
U.S. Coast Guard Research & Development Center
Groton, CT 06340

Human Factors in Incident Investigation and Analysis

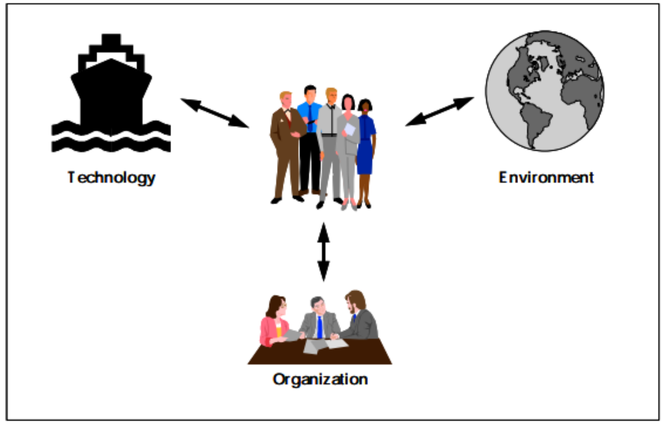
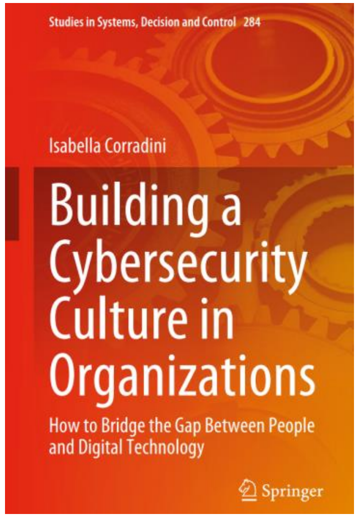


Figure 2. The Maritime System Is A *People* System



Studies in Systems, Decision and Control 284

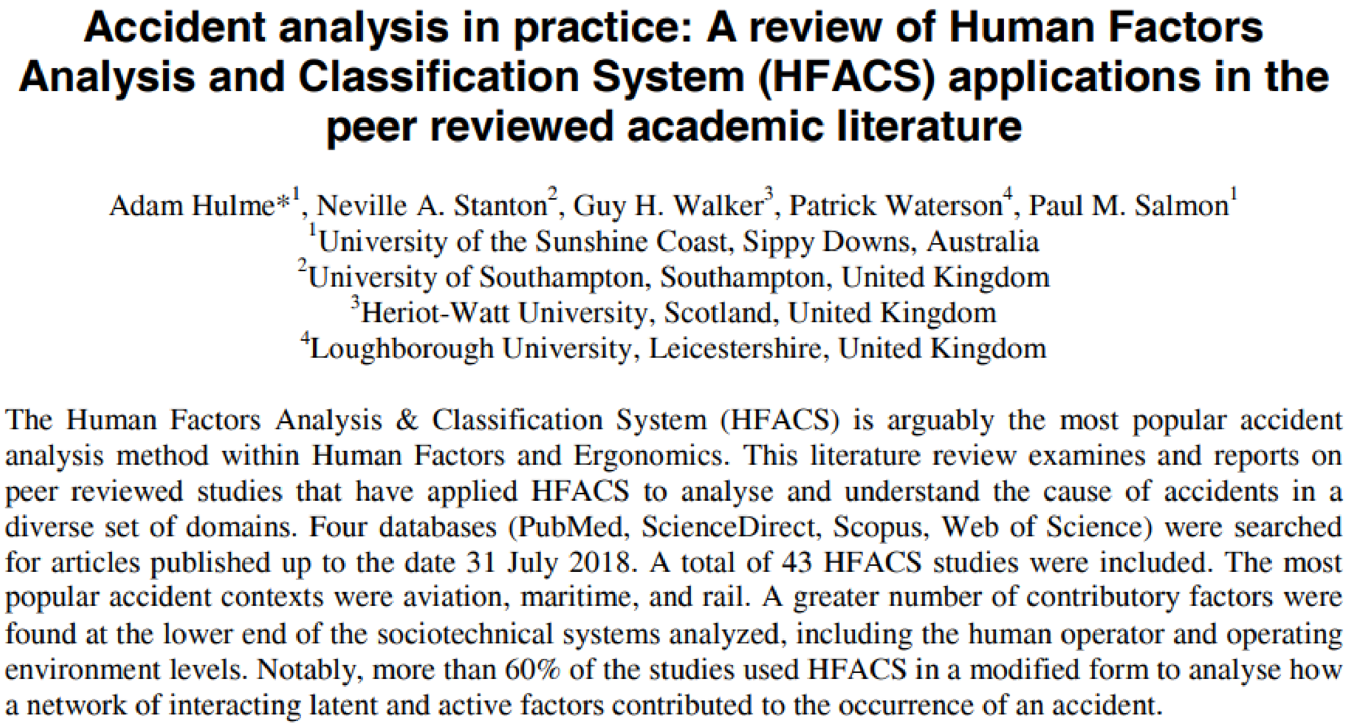
Isabella Corradini

Building a Cybersecurity Culture in Organizations

How to Bridge the Gap Between People and Digital Technology

Springer

2. Scenarios developed should incorporate elements of analysis using HFACS



Accident analysis in practice: A review of Human Factors Analysis and Classification System (HFACS) applications in the peer reviewed academic literature

Adam Hulme*[1], Neville A. Stanton[2], Guy H. Walker[3], Patrick Waterson[4], Paul M. Salmon[1]
[1]University of the Sunshine Coast, Sippy Downs, Australia
[2]University of Southampton, Southampton, United Kingdom
[3]Heriot-Watt University, Scotland, United Kingdom
[4]Loughborough University, Leicestershire, United Kingdom

The Human Factors Analysis & Classification System (HFACS) is arguably the most popular accident analysis method within Human Factors and Ergonomics. This literature review examines and reports on peer reviewed studies that have applied HFACS to analyse and understand the cause of accidents in a diverse set of domains. Four databases (PubMed, ScienceDirect, Scopus, Web of Science) were searched for articles published up to the date 31 July 2018. A total of 43 HFACS studies were included. The most popular accident contexts were aviation, maritime, and rail. A greater number of contributory factors were found at the lower end of the sociotechnical systems analyzed, including the human operator and operating environment levels. Notably, more than 60% of the studies used HFACS in a modified form to analyse how a network of interacting latent and active factors contributed to the occurrence of an accident.

"HFACS …to analyse how a network of interacting latent and active factors contributed to the occurrence of an accident"

HFACS has been considered in cybersecurity, but primarily from IT/IS and organisational perspective, it is an emerging area

2.HFACS could be extended to consider cybersecurity, need for human centred approach recognised in CIS

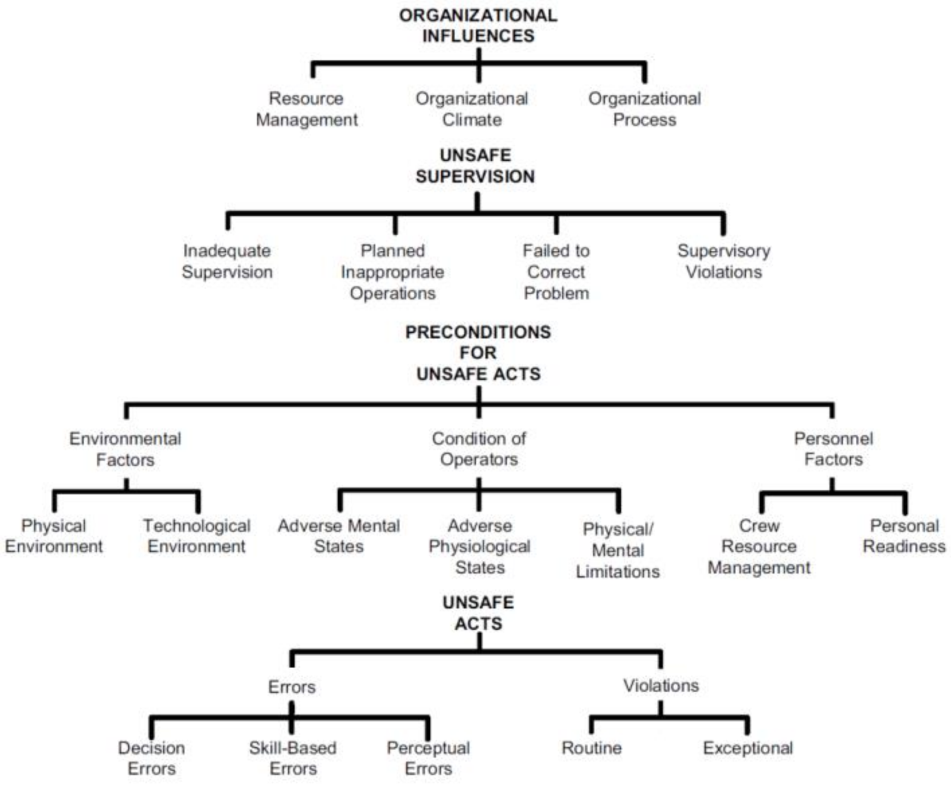


Figure 1. The HFACS framework.

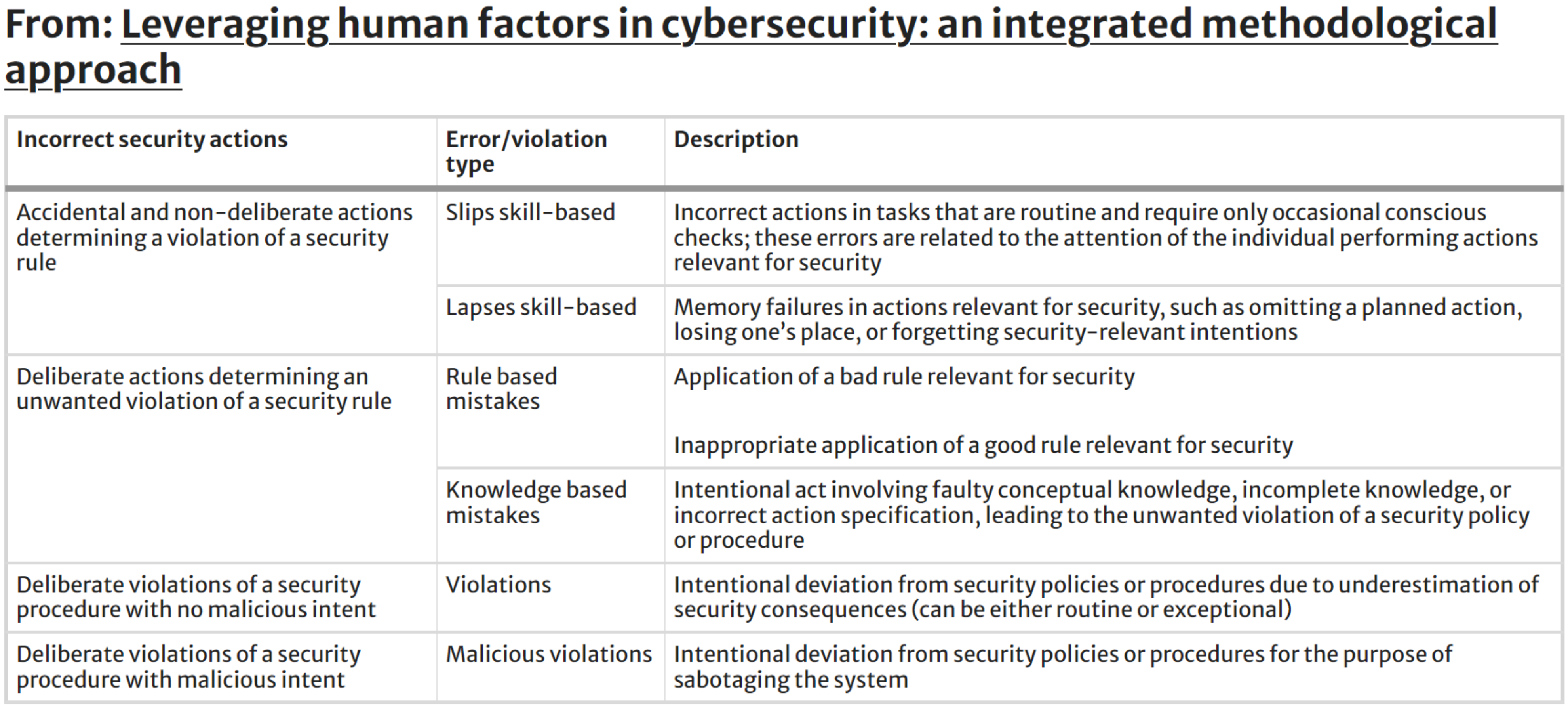
Figure 1 (Shappell et al (2007)

“Historically, CIS [Computer Information Security] has usually been approached adopting a technology-centric viewpoint, with little – if no – consideration and understanding of the end users’ cognitive processes, needs and motivations”

“The recent research in cybersecurity widely agrees that a holistic approach as opposed to technical solutions alone is required to contrast cyber-attacks”

“This has been especially recognised in well-addressed sectors, such as education and healthcare, but also in novel and emerging fields, such as autonomous vehicles, where users’ behaviours and attitudes are able to undermine technological advancements “

2. Some mapping has been carried out between security and safety human factors

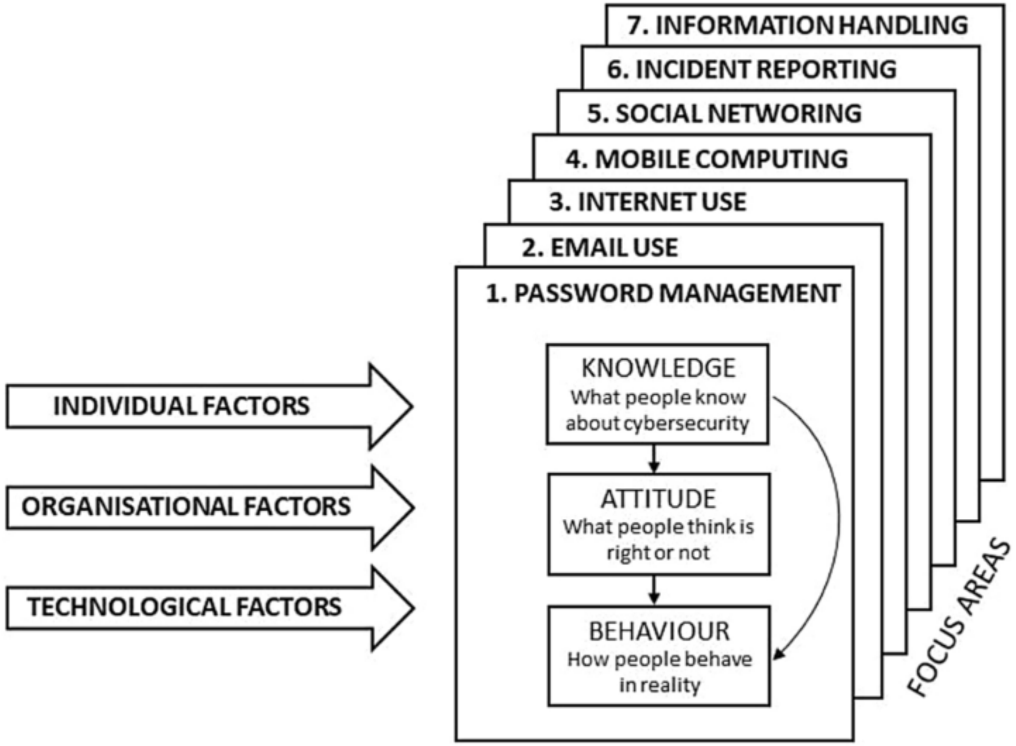


From: Leveraging human factors in cybersecurity: an integrated methodological approach

Incorrect security actions	Error/violation type	Description
Accidental and non-deliberate actions determining a violation of a security rule	Slips skill-based	Incorrect actions in tasks that are routine and require only occasional conscious checks; these errors are related to the attention of the individual performing actions relevant for security
	Lapses skill-based	Memory failures in actions relevant for security, such as omitting a planned action, losing one's place, or forgetting security-relevant intentions
Deliberate actions determining an unwanted violation of a security rule	Rule based mistakes	Application of a bad rule relevant for security Inappropriate application of a good rule relevant for security
	Knowledge based mistakes	Intentional act involving faulty conceptual knowledge, incomplete knowledge, or incorrect action specification, leading to the unwanted violation of a security policy or procedure
Deliberate violations of a security procedure with no malicious intent	Violations	Intentional deviation from security policies or procedures due to underestimation of security consequences (can be either routine or exceptional)
Deliberate violations of a security procedure with malicious intent	Malicious violations	Intentional deviation from security policies or procedures for the purpose of sabotaging the system

2. Challenges are anticipated in taking cyber security HF and comparing it to safety HF

From: Leveraging human factors in cybersecurity: an integrated methodological approach



Focus areas of the HAIS-Q questionnaire

Human factors (HF) are seen through different perspectives when considering safety and cybersecurity

It’s not clear whether the (safety) accident investigators have got any established practice using cybersecurity human factors in a safety context

This can be established through 1-2-1 consultation as part of further work

2. Some elements of CyBOK HORA not prioritised for further work

Scenario-based teaching needs to minimise background reading and research to focus on student thinking skills (accident investigation)

- HORA = Human Organisational and Regulatory, recommend focussing on human and organisation in the next stage of scenario development
- A legislation and regulatory-led approach to developing scenarios is been discounted as a priority for further work due to the significant volume of both safety and cybersecurity governance, regulatory and legislative material, at national and international level and the lack of established practice integrating both sectors
- Cybersecurity and safety standards and frameworks also provide valuable guidance but also represent a significant body of work which, as for legislation and regulation, has not yet been analysed and synthesised aggregated over both discipline areas