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

Abstract

There is a growing need to incorporate cybersecurity risks into safety management systems, particularly in Critical National Infrastructure (CNI). Despite this increasing complexity, cybersecurity integration into safety-related curricula remains limited, largely due to the lack of real-world case studies or mature hybrid investigation methodologies, and the existing high teaching loads involved in safety-focused syllabuses. This report explores approaches to expanding the reach and impact of the Cybersecurity Body of Knowledge (CyBOK) through its integration into safety accident investigation education.

To bridge these gaps, this study evaluated the teachability of cybersecurity within safety accident investigation courses at Cranfield University, using scenario-based teaching methods. CyBOK themes were mapped to key MSc modules (including ‘Fundamentals of Accident Investigation’ and ‘Applied Marine Accident Investigation’) to identify potential integration points. The preferred scenario-based approach aligns with existing accident investigation frameworks, which already employ case studies of past incidents as learning tools.

Key findings identified the "Attacks and Defences" theme from CyBOK as having the most potential for integration into safety investigation education, particularly in linking technical controls with human and management systems. Insights from past rail and marine cybersecurity incidents, such as the UK Cambrian rail line ERTMS case, informed the scenario development, illustrating the complexity of managing digital safety risks and the importance of considering both safety-critical and non-safety-critical systems.

Six cybersecurity scenarios were developed to reflect real-world challenges in safety accident investigations, based on the maritime sector. These scenarios addressed key issues such as navigation errors, system updates, human-machine interface failures, and noted the emerging role of autonomous vessels and machine learning. The scenarios were evaluated for relevance and teachability, with input from both safety and cybersecurity professionals. Feedback revealed different perspectives between the two fields, particularly on emerging technologies and office hygiene, helping to shape selection of scenarios for teaching.

The report also highlighted the need for further development in areas such as Systems, Infrastructure, Platform, and Software security, which are underrepresented in current safety accident investigation syllabuses. Additionally, future work should consider international regulatory and cultural differences, particularly in maritime cybersecurity, and develop skills for accident investigators to "rule in or rule out" cyber-related causes during investigations.

In conclusion, while this study represents an early step in integrating CyBOK into safety accident investigation education, it also underscores the potential for cybersecurity to enhance the scope and depth of safety investigations. Further work is required to broaden scenario development, refine pedagogical approaches, and address the emerging regulatory landscape that increasingly emphasises the crossover between safety management systems and the cybersecurity domain.

Introduction

The vision for CyBOK as an established, internationally recognised resource for all the security community sectors (academia, industry, and government) is increasingly championed across cybersecurity. But, in the closely related safety domain, there is low CyBOK awareness. This low awareness exists alongside limits on a drive for integration of cybersecurity into already packed teaching schedules. In addition, the interface between the two disciplines has been recognised as incorporating some challenges (e.g. the recent IET Code of Practice on Cyber Security and Safety) [1].

Increasing regulatory scrutiny and lower levels of maturity for combined safety and cybersecurity management systems is changing the regulatory environment. For example, the current priorities and trends noted in regulatory reports indicate the importance of considering software and cybersecurity of digital systems e.g. ORR section 1.92 Annual Report of Health and Safety on Britain's Railways (orr.gov.uk) [2]. The ongoing journey to an integrated approach across safety and cyber security is noted across industry, including by UK regulators (e.g. HSE, OFGEM, ORR, ONR, example given in [3]) and across wider industry-academia partnerships such as PETRAS [4].

Regulators such as the ORR further clarify [5]

"With new software-based systems introduced to help with the operation of the network, new risks have emerged. Duty holders should manage their systems so that software design, operation, maintenance, and cyber security risk is overseen in the same way as any other safety risk. It should form part of their wider Safety Management System."

In addition to safety regulatory scrutiny, there is now also a timeliness driver to bridge the safety-security gap once both IT (information technology) and OT (operational technology) elements of digital systems.

This is because the increasing digitalisation and connectivity of Critical National Infrastructure (CNI) is blurring the lines between IT cybersecurity and OT (operational technology) cybersecurity. The former is relatively well understood, broadly across the cyber security community, whilst the latter is a more specialist domain, with much legacy equipment. Operational technology cybersecurity is particularly relevant for safety in CNI, particularly given the rapid growth in remote access, provision of cloud-based services, complex supply chain and transfer of data and services from 'on prem' (on premises) to the cloud [6].

Broadening accident investigation to incorporate cybersecurity is therefore 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.

However, accident investigation skills are typically taught through analysis of previous incidents, along with field work. Because of the changing landscape of CNI and other factors, it can be assumed that there are ongoing trends in under reporting/under analysis, along with an assumed increasing number of incidents and near-misses of digital origin with potential safety impact. These two assumptions are key as safety (accident investigation) is strongly evidence-based and prior incident driven in terms of focus, and development of investigation techniques. The absence of an evidence base of existing incidents therefore has a significant impact on teachability of cybersecurity within the context of safety accident investigation, further compounded by the challenges associated in working across the safety and security disciplines [1].

There is also a problem associated with the maturity of the discipline and experience in teaching across. If the hybrid safety-security courses do not exist in academia, then the skills cannot be developed to serve industry and government needs. But if the hybrid security-safety methodologies are not yet mature, it may be assumed that they cannot yet be taught (further compounded by the limited public domain data). It is worthwhile noting that perception of one discipline by another varies e.g. cybersecurity specialists may say that "cybersecurity is a process not an event," and "safety is static not dynamic," but safety specialists will say "safety is a process not an event." The two sectors do not naturally align.

The current maturity of both the field of (safety) accident investigation incorporating cyber and the teaching of accident investigation is still developing, but given the increasing focus on cybersecurity as a driver for safety-related incidents,

and that that “safety” is a much broader scope than safety-critical systems, it is reasonable to assume that the accident investigation sector may not wish to wait for the methodologies to mature in order to develop capabilities to analyse the incidents.

To plug the gaps, credible and usable teaching scenarios are needed to train accident investigators, even if real world case studies based on real incidents are not available right now, nor a mature and established methodology for working across the safety-security discipline intersection. CyBOK material and cyber pedagogical experience may provide opportunities to fast-track the development of both competencies and teaching delivery.

The CyBOK material is broken down into five themes (Figure 1):

- Human Organisational and Regulatory Aspects
- Attacks and Defences
- Infrastructure Security
- Systems Security
- Software and Platform Security

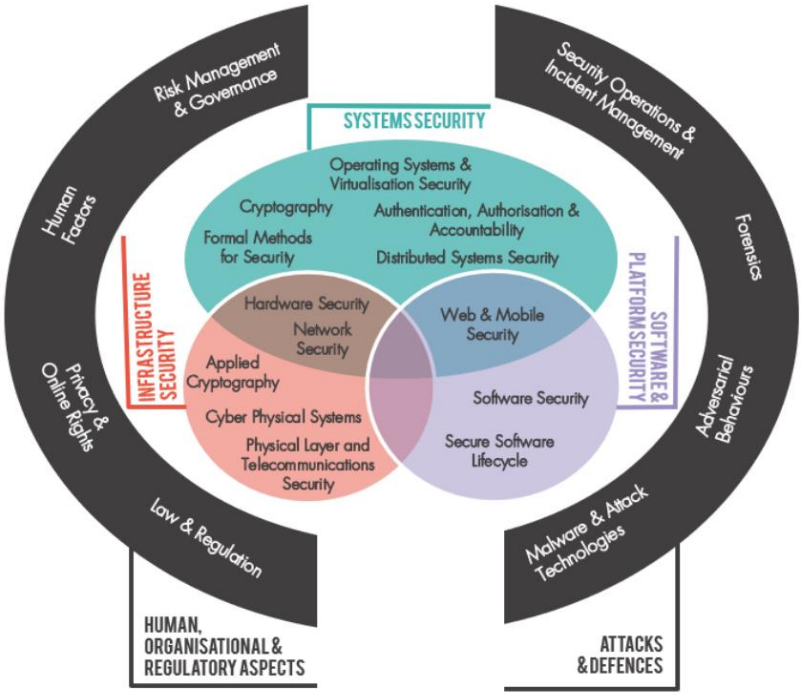

Figure 1: Cybersecurity Body of Knowledge (CyBOK) framework [7]

In 2022 the Royal Academy of Engineering funded a Visiting Professorship at Cranfield University (held by the lead author of this report) to sound out teachability of cybersecurity. The goal was to explore, test and identify opportunities to integrate cybersecurity material into teaching trials. Engaging with students and academics, the goal was to calibrate appetite and potential for success across five MSc courses at Cranfield University. The syllabuses span transport CNI regulation, technology, people, and processes. The learners are a global cohort, spanning from recent graduates to career mature professionals including pilots and accident investigators.

Cranfield University Safety MSc courses within scope are:

- Airworthiness
- Safety and Human Factors Analysis
- Advanced Safety and Management of Risk
- Aviation Digital Technology Management
- Accident Investigation

Initial screening over the first couple of years of the Visiting Professorship (2022-2024) identified that gamification and role play was effective in breaking down learner socio-technical barriers as well as providing a sandbox to test

teaching and develop new views on safety-security implementation [8]. A combined scenario and gamification teaching across a combined career mature and recent graduate cohort can be a test bed for accelerating findings on what approaches will work and land for implementation in the real world (and what will not).

This work for CyBOK builds on that programme with the objective of identifying which parts of CyBOK are best suited for initial trials of scenario-based teaching within the selected Cranfield University MSc programme. Given the lack of existing capabilities and/or time resources in the student (and academic) cohort, a targeted and tailored approach is needed when evaluating opportunities for use of CyBOK material. As a baseline assumption during the trial, across a three-week MSc accident investigation programme, teaching time available for cybersecurity typically ranges from 1-4 hours.

It is important to highlight that this short study is not focussed on describing the current situation “as is” with respect to aligning and implementing the cybersecurity and safety disciplines. This “as is” problem is already well captured in a range of documents e.g. the IET Code of Practice [1], captured in Figure 2.

A recent CyBOK study (CyBOK usage in the classroom, Aug 2023) [9] also identified the following challenges when developing and trialling case study scenarios with software and cybersecurity students:

““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.”

It can be assumed that such translation and interpretation challenges are equally present when going from cybersecurity to safety and vice versa.

These factors have shaped the definition of methodology used for this short study.

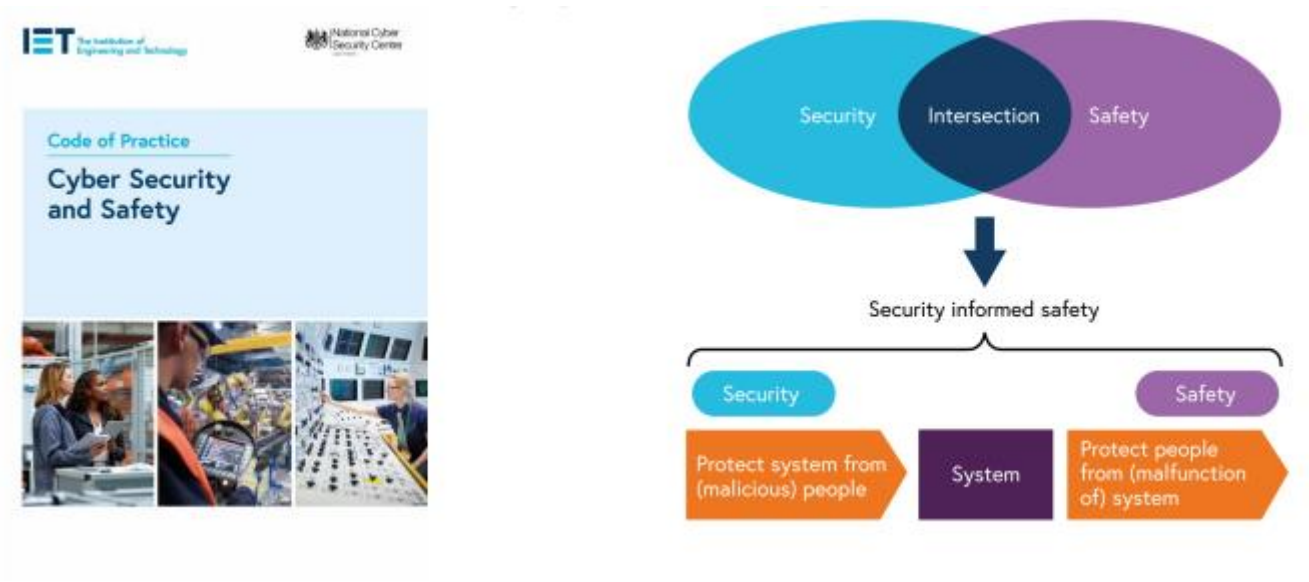

Figure 2: IET Code of Practice Cyber Security and Safety

Methodology

A short programme of work was defined to establish opportunities for teaching cybersecurity into the safety-led MSc courses at Cranfield University. This was implemented through a high-level course syllabus mapping from the 5 MSc courses to the CyBOK topic areas, focussing on two modules, Fundamentals of Accident Investigation and Applied Marine Accident Investigation.

A scenario-based approach forms the backbone of the teaching of safety accident investigation. Much of the teaching is delivered through analysis of previous incidents. The end state following those scenarios typically meets one or both of the following consequences, with the potential for impact on safety (loss of life, during the incident and after, during evacuation and recovery) and environmental impact, including loss of the asset. Both are core to marine accident investigation:

- collision (with other vessels, shore, “floor” of ocean (seabed) etc.)
- fire, evacuation, oil spill (including as a consequence of collision)

A scenario-based approach therefore was selected to evaluate the opportunity for teaching cybersecurity into the safety-led accident investigation courses.

The following tasks were carried out:

- High level analysis and initial 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
- Development and use of a ranking structure for teachability of the 5 CyBOK themes
- Development of six scenarios using the results of the high-level screening and research through published literature
- Engagement with senior teaching academics in cyber security safety accident investigation to rank the scenarios in order of importance for use in the classroom
- Presentation of the six scenarios to the wider safety community and solicit their feedback on the priority ranking
- Draw high level conclusions and evaluate areas for further work
- Some additional opportunities for short lectures to fill certain topic area gaps were also identified

During the study, a number of expert inputs were sought through anonymised interviews, inviting teaching Professors in both safety and cybersecurity domains. They were asked to rank the scenarios developed, focussing on priority (importance of the topic) and teachability, considered through gamification and a concise list of pedagogical approaches. To ensure a broad range of engagement opportunities the results were delivered to the wider safety community in the format of a final webinar presentation with an interactive online questionnaire to establish scenario ranking. Both approaches were designed for an initial first pass and the findings should be further tested in a more structured and larger cohort consultation.

The build of scenario themes was based on teaching in an accident investigation context. This is due to the expectation that teaching safety accident investigation is most likely to need development soon as safety-related incidents (or near misses) with a suspected cyber element are anticipated to occur in greater numbers. This is because 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 with the potential to impact on safe operation. As the emergent properties have not yet been codified into the safety incident and near miss reporting systems, it is likely that there may be a lag between incidents and near misses occurring and then being recorded and analysed as part of the historical trend approach to safety accident investigation. Incorporating the CyBOK resources into the safety accident investigation ecosystem provides an opportunity to bridge the gap.

To help the build of scenario themes, a review of previously reported marine incidents was carried out (Table 1). It was initially assumed that enough detail was available in academic journals. However, despite the wide range of references available, the review of the references themselves provided limited substantiation of details (to the level needed to provide scenario theme development).

Scenarios based on one or more controls for management of risk (people, "plant" (technology) and processes elements) were considered. It was initially assumed that the following themes might be appropriate starting points:

- Safety culture and cybersecurity culture, overlaps and differences
- Management system differences, and difficulties with integrated implementation of the different management system approaches to safety and cybersecurity

A high-level literature review of cybersecurity culture versus safety culture was carried out. There appeared to be limited evaluation of crossover topics between the two discipline areas. In addition, there was limited scenario analysis of the crossover between two management systems, likely due to the challenges of building a combined management system, in line with the findings of the IET Code of Practice on Cyber Security and Safety.

Table 1: Example of recent marine cybersecurity incidents [from Meland et al., 2021, TransNav] [7]

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

It was decided instead to look for theme overlaps between CyBOK (Figure 1) and the syllabus components of the selected accident investigation modules. The approach taken was to identify reasonably foreseeable scenarios. It is important to note that understanding and implementation of the CyBOK content in the safety domain may vary, and successful incorporation of the content into the safety accident investigation teaching may be dependent on the level of underlying knowledge required to understand it. Consideration was therefore taken of where the CyBOK material could be most easily absorbed into existing safety syllabuses, leading to a potentially lower initial hurdle to adoption.

A maritime-focussed review of recent cybersecurity incidents combined with review of recent UK Department for Transport (DfT) maritime research (MAR-RI programme) [10] was carried out. It provided the indication that, due to increasing digitisation of the sector, including attack points on the ship, on shore and also ship to shore communications, a more technologically focussed context for development of scenarios was appropriate. Considering the range of automation systems onboard and exposed systems representing a relatively high proportion of incidents/potential incident types (Figure 3), this was used to frame the selection of the reasonably foreseeable scenarios[1].

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

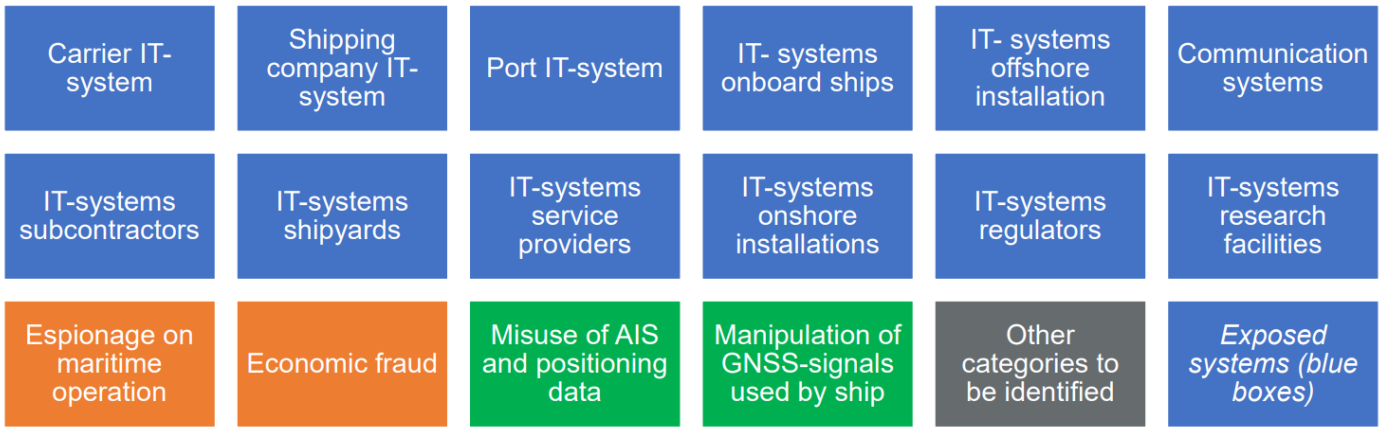

Figure 3: Representation of the different categories of incident (blue: exposed system) (adapted from Meland et al. 2021) [11]

It is important to stress that the six reasonably foreseeable scenarios presented in this report do not represent a hierarchy of importance (defined as one or more of vulnerabilities for exploitation, interest to third parties etc.) but a subset of scenarios where it is considered that the cybersecurity context can be imported into the safety accident investigation teaching. By necessity, some reasonably foreseeable scenarios with a high technical content (i.e. the majority of the CyBOK syllabus) cannot be included in the baseline approach for this study.

To characterise the feasibility of generating hybrid scenarios incorporating CyBOK material and the scope of the accident investigation courses, an alignment scale was developed (Table 2). his alignment scale is qualitative and relative and characterises - within the current syllabus framework provided by the MSc in Fundamentals in Accident Investigation (with the specialist modules in Applied Maritime Accident Investigation) - the degree of alignment of each the five CyBOK themes to the relevant accident investigation modules.

Table 2. High-level categories used to map CyBOK material to the Safety Accident Investigation MSc (categories defined as part of the methodology for this study)

Alignment scale definition	**Colour code in table**	**Notes**
Directly associated and CyBOK material accessible to accident investigators		Topics of mutual understanding across safety (accident investigation) and cybersecurity e.g. risk management, governance and regulation. Although the content is materially different across 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

The scale does not define 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 skill set (as

developed through the MSc module study) and the nature of opportunities for use of the CyBOK material in the field by those trained accident investigators.

Colloquially, it is a ranking of whether an accident investigator will pick up a CyBOK document index and be able to use it in one of four contexts (green, yellow, orange, red) where the two end points of the scale are defined as follows:

- The safety academic can understand the content, read, and absorb and then assess how it might be integrated into their professional practice (scale: green - directly associated), and
- The potential for situation where the CyBOK index page of topics 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 etc.) (scale: red - no available point of reference)

The methodology developed for this short study was further bounded by a few key challenges involved in mapping safety accident investigation syllabuses to the CyBOK areas. These factors then then shaped the conclusions, including:

- The large volume of material, and the underpinning technical knowledge needed to carry out the mapping, noting that few people (any?) are fully fluent in both safety and cybersecurity disciplines
- The need to create a tailored process on how to develop the scenarios, then decide, define, and apply the ranking criteria (part of the pedagogical assessment)
- The process for how feedback could be sought, and the analysis structured, recognising the diverse backgrounds and limited time and the subjective nature of expert judgement
- The need to produce something practical that other people can then trial in a teaching context, using small teams, either cybersecurity, safety, or combination safety-cybersecurity

Given that the teaching context for safety-security topic overlap has not yet been explored in depth, this first pass study is based on individual questionnaires and ranking of scenarios, from both the cyber discipline and selected academic leads at Cranfield University. Even if an individual has got perfect and complete knowledge of all topics and discipline areas (all CyBOK, all topics within the scope of the 5 MSc courses), the implementation "immaturity" of the safety-security crossover engineering discipline means expert judgement will be used and unconscious biases therefore come into play.

This early-stage prototyping is in effect an early TRL pedagogical equivalent and is not based on in-depth application of structured research methods. It was initially planned to make use of the six decision 'de-biasing approaches' used to counter unconscious bias in collective decision making [12], but due to the study schedule and scoping limitations this was not possible to implement as initially planned.

Recommendations for further work were instead developed through consideration of whether the three CyBOK themes (infrastructure security, systems security, software and platform security) initially assessed as not embeddable within existing safety accident investigation teaching syllabus and timetable ("red" category in Table 2) could instead be enabled through "car sensor hack" scenarios. This builds on student familiarity with car-based sensors as part of their everyday activities.

Another approach to development of teachable scenarios which are solely HORA (Human Organisational and Regulatory Aspects) based was identified, potentially using the accident investigator's HFACS (Human Factors Analysis and Classification Systems) framework. These two approaches, reported in the further work section, are exploratory only. A parallel activity carried out outside the scope of this study to assess the teachability through gamification incorporating pedagogical assessment was not completed at the time of this activity. Further work in this area will be able to take advantage of future published results.

AI, blockchain and other related emerging technologies are not covered in the scope of this project.

Results

Evaluation of the structure of safety risk management and the types of controls

Safety risk management is structured around controls divided into the following categories [2] [2]:

- People
- Process
- “Plant” (technology) *[see footnote)*

These controls are identified through the implementation of a risk management process as shown in the figure below, which is from ISO31000, as referenced in the IET Code of Practice [1]).

The hierarchy of controls (i.e. which type should be used first) is set by legislation/regulation known as MHSWR in the UK. Technical controls may be selected over administrative controls in this hierarchy. This approach is reviewed on a case-by-case basis and is dependent on the approach taken to manage the hazard. A hazard is defined as a situation with the potential to cause harm).

Industry regulators scrutinise safety management systems (process, organisation, management) alongside people (skills and competences, roles, responsibilities). Technical controls are the third type of controls identified through the risk assessment process (risk identification, analysis, and evaluation) to treat risk.

Safety accident investigators focus on all three categories of controls with the goal of identifying where they have failed to manage the risk effectively.

This controls framework therefore provides a potential lens through which safety professionals can view cyber security, and thus a framework for incorporating cybersecurity into scenario-based teaching. The discipline of cybersecurity (as mapped by CyBOK) is broadly technology based i.e. aligned with the “plant” (technology) category of control. Understanding the role of people in the management of risk (e.g. attack/defend) and data (e.g. incident management, forensics) requires an understanding of the technology.

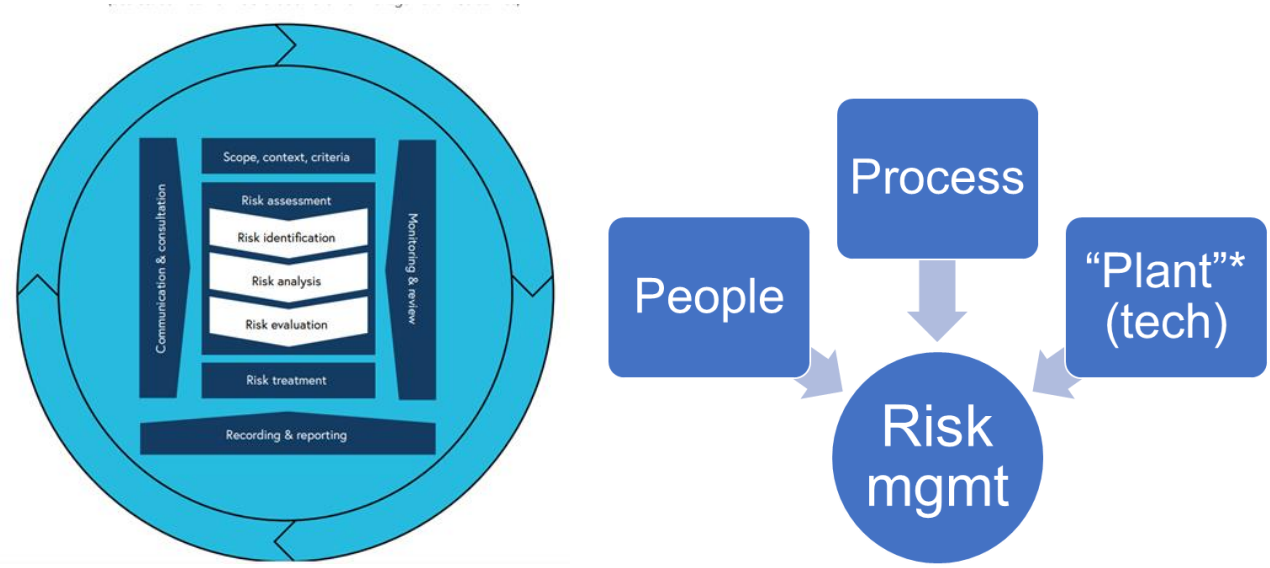

Figure 4: Implementation of a risk management process to identify three categories of control.

Longer term, beyond the scope of this contract, if common points of understanding can be established between the CyBOK framework and the safety hierarchy of controls, including the relative level of technical knowledge required to

[2] Categories of controls originally from energy where “plant” refers to process control equipment (valves, pipework, vessels, control systems). Plant = technology (hardware, software…)

understand the role of people in both safety and cybersecurity risk management of frameworks, the insights generated may also be of benefit in teaching and in the field. However, it can be assumed that this will require a broader range of scenarios to be developed and used as well as addressing some of the challenges identified in the IET Code of Practice in Cyber Security and Safety.

Insights gained via consideration of a rail accident investigation.

Rail accident investigators have gained experience in the challenges associated with investigating a recent digital safety incident. The Rail Accident Investigation Branch (RAIB) report [13] on the UK Cambrian rail line ERTMS signalling incident highlighted the difficulty of gathering and understanding the data and the software operation that led to that point. Identifying and evaluating where integrity and availability of data was not maintained shaped the multi-year investigation process.

The report content and presentations and discussions with the wider safety community (e.g. Safety and Reliability Society webinar [14]) shone a spotlight on both the challenges capturing the ‘as is’ and the root causes of the incident. A full capture of all the software development stages was one goal of the investigators. This was only partially achieved due to the divergence between the software version as implemented on the UK Cambrian line and that assessed through the safety case process, something that was uncovered during the investigation.

Another insight was gained through looking at the links between software of different safety integrity levels (SIL), where the level that needs to be achieved is linked to the criticality of the software. The development and deployment of safety-critical software is strongly version controlled and defined within set system boundaries. However, issues can occur when data flows between different Safety Integrity Levels (SIL) combined with reliance on previous safety cases based on earlier software versions, with a change management process used to manage the updates. The operators of the system considered that because the various processes around the SIL-rated elements of the signalling system had been implemented and signed off, that the system was safe to operate. This then meant that certain operational quirks, leading to the need for regular system restart etc., were not considered in more detail. If the assumption that if the assessment process is ‘signed off’ and therefore the system is safe and/or that only malfunction of safety-critical software has the potential to cause a safety incident is held, it limits how safety accident investigators may approach their initial investigation. This assumption may also unnecessarily limit the scope boundary initially set by the safety managers or the accident investigators. Incorporation of CyBOK material into the safety accident investigation scenarios as part of the development of teaching scenarios may help counter these assumptions.

One way to achieve this is to highlight that safety is also “a process not an event,” and that, outside the assumed close supervision and management of SIL-rated safety critical systems, operational safety is a lot more flexible than may be perceived. For example, OTA (over the air) updates (cars) or in situ updates (USB) (trains) are routinely carried out as part of regular maintenance, upgrades or reactive fixes (patches). It can be assumed that updates of passenger entertainment systems, passenger Wi-Fi, passenger displays are not treated as safety-critical and so subject to less stringent controls, nor in depth evaluation of cybersecurity vulnerabilities. However, in a transport setting these interfaces with the passengers can be disrupted leading to incorrect information which can then be used to create e.g. panic, crush, and injury situations.

For scenarios where freight is involved instead of passengers, whether rail or maritime, a wide range of issues can occur, particularly around incorrect loading and balancing of cargo or tracking of potentially hazardous goods. A complete system perspective is necessary, considering ports and terminals and multi-modal transfers, as well as the transport systems (trains, ships) themselves. Scenario-based approaches will be valuable here in developing further the safety accident investigator skill set for digital safety investigations.

Implementation of software updates as part of the patching process is integral to day-to-day cybersecurity operations, but the need to fix software versions through the safety case process is often raised as a problem. In the Cambrian incident, this was further compounded by the divergence between the version of software that was formally assessed and deployed, and the version that was implemented on the Cambrian rail line. A series of locally implemented changes cumulatively led to potentially unsafe system operation which was only identified when a train driver queried a change in the information locally available to them. This was some time after the system update that led to the hazard had occurred.

A complete system view of operations needs to consider all digital systems where malfunction may lead to system or human actions and provide a clear view on the links between updates to safety-critical systems and the much broader business as usual maintenance and operations activities. This bridges the gap between safety-critical and non-safety critical systems and provides a framework for the development of the scenarios.

There are therefore two approaches to crafting scenarios that emerge from consideration of a rail accident investigation. A scenario is based on either:

- Technical ("plant") controls i.e. what elements failed to manage the hazard, and how this manifested itself
- People and (management) processes i.e. how this situation came to occur, including the role of people

Given that rail accident investigators, and regulators, focus on safety management systems, it was initially assumed that a management process-based approach to scenario development for the teaching of cybersecurity within a safety accident investigation programme would be a preferred approach.

Analysis and screening of CyBOK themes against (safety) accident investigation modules

To establish a baseline of safety accident investigation knowledge and skills against which CyBOK material could be mapped, a high-level syllabus mapping for the Cranfield University MSc courses (Fundamentals of Accident Investigation, Applied Marine Accident Investigation) was carried out. Reflecting industry needs, it indicated that a clear proportion of teaching time (including field and classroom exercises) focussed on two out of three of the risk management category controls (people, processes), with less focus on the third ("plant" i.e. technology). Where technology topics were raised, it was generally in the context of analysis of previous incidents that had occurred.

Key general accident investigation modules included:

- 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 accident investigation modules included:

- Marine accident investigation process
- International perspective (coordination, and cultures)
- National and international regulations and code

To develop selected scenarios for use within the safety accident investigation, the CyBOK material screened to identify "implementability" within a (safety) accident investigation teaching context. Assessment was 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) as shown in Tables 3 and 4. Note that the alignment scale used (Table 1, defined as part of the methodology) is qualitative and relative and characterises the degree of alignment of each of the five CyBOK themes to the relevant accident investigation modules. Colloquially, it's a ranking of whether an accident investigator will pick up a CyBOK document index and be able to use the material (green) through to not being able to understand the index page of CyBOK resources nor see the context for how it might be used (red), as defined in Table 1.

As noted in the methodology, this assessment 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 skills developed through the MSc module study, and thus the opportunity for integrating the CyBOK material into scenario-based teaching.

When the safety accident investigation syllabus for Fundamentals of Accident Investigation (Table 3) and Applied Marine Accident Investigation (Table 4) was broken down into themes and a high-level screening applied (using Table 2) a number of initial conclusions could be made. As expected, there were limited to no opportunities for the more technically focused CyBOK themes (Infrastructure Security, Systems Security, and Software and Platform Security) to be linked into the existing syllabus structure.

More surprisingly, there was less overlap than initially anticipated between the CyBOK HORA (Human Organisational and Regulatory Aspects) theme and the accident investigation syllabus. This is potentially linked to the fact that the regulatory framework in cybersecurity is anchored around information security (confidentiality, integrity, and availability of data) whilst regulation in safety is around preservation of life, with environmental impact and asset protection as associated themes.

Whilst the legal and regulatory context and the national and international regulations and codes were documented for both safety accident investigation and cybersecurity, there was a significant volume of material for both discipline areas. When considering both the scope of this study scope and the limited time available for cybersecurity teaching in the safety accident investigation classroom, there did not appear to be an easy route to identifying and developing scenarios which would not also involve the students in significant background reading.

Based on the screening, compared with the other topics, the Attacks and Defences element of CyBOK had the most potential for closer integration into the safety accident investigation syllabus. It represented technologically based controls (essential to the implementation of cybersecurity) but also linked to management systems and the role of people in managing the risk (e.g. ransomware). This topic was therefore a starting point for the development of reasonably foreseeable scenarios in this study.

The Attacks and Defences category also aligned to the incident summary used as part of the definition of methodology for this work [11]. This is due to the high number of network-based incidents (as a proportion of the total maritime incidents) as reported in Figure 3. Exposed systems represent a relatively high proportion of incidents/potential incident types.

Lastly, use of Attacks and Defences also allowed for the consideration of both IT and OT elements of a maritime system as well as highlighting core elements of cybersecurity in malware and attack technologies, including penetration test, ransomware and use of Wireshark and malware analysis to improve security requirements[3].

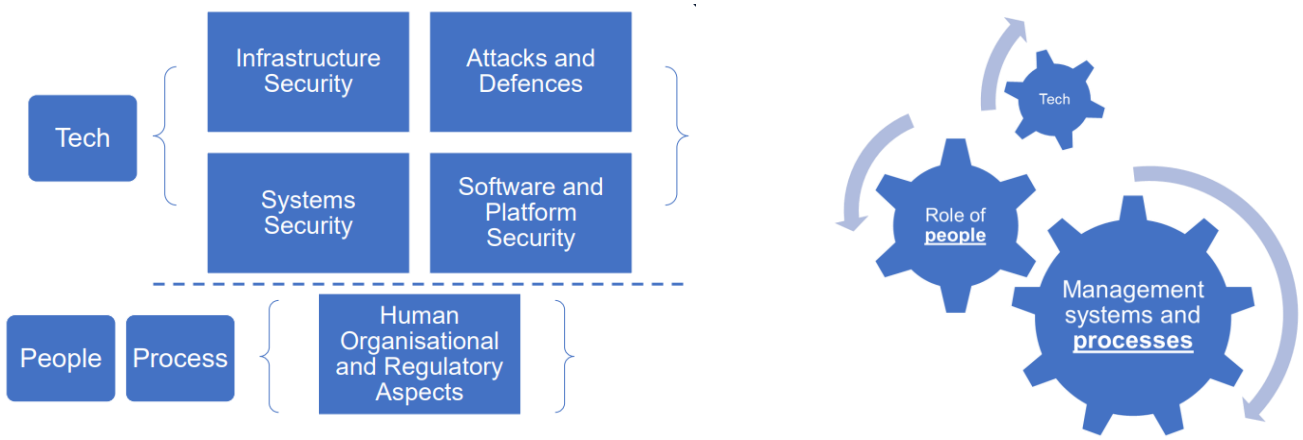

Figure 5: Mapping of CyBOK themes against the three categories of controls.

[3] Taken from Malware_Attack_Technologies_v1.0.1.pdf (cybok.org)

Table 3: Mapping of CyBOK themes (Figure 1) to the Fundamentals of Accident Investigation MSc syllabus elements using the mapping categories from Table 2

	CyBOK Themes *(Figure 1, 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				

Table 4: Mapping of CyBOK themes (Figure 1) to the Applied Marine Accident Investigation MSc syllabus elements using the mapping categories from Table 2

	CyBOK Themes *(Figure 1, 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					

Development of scenarios for safety accident investigation teaching

To teach cybersecurity to safety accident investigators, there is a need for reasonably foreseeable scenarios that encompass elements of cybersecurity, and that align to a (safety) accident investigation course syllabus.

Accident investigation incorporates a range of uncertainties and is process-driven (gathering of evidence) and requires an elevated level of applied skills, and knowledge. An accident investigator needs to be able to appreciate 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

CyBOK-informed reasonably foreseeable scenarios that are developed for use in the safety accident investigation context need to develop skills to address these factors.

The application of the methodology in this study identified that the Attacks and Defences theme of CyBOK provided a better opportunity for alignment into the safety accident investigation syllabus than the other CyBOK themes. Attacks and Defences links the technological elements of cybersecurity to the broader operation of a maritime system (shore and at sea) and bridges across IT and OT.

It is important to recap that the scenarios developed in this study are not aligned with the ‘as is’ list of highest priorities for action by those individuals and organisations that are involved in implementing real-world cybersecurity for maritime operations. They have been developed for teachability within a safety accident investigation syllabus including “fit” with (safety) accident investigation mindset, and opportunity for insertion into the syllabus.

The scenarios were developed based on the maritime sector as this allows for consideration of the international context (e.g. different regulatory regimes and cultures). Maritime systems are complex, with some elements in motion (ships are moving systems) and include legacy to emerging technologies. They were informed by an in-depth literature review taken from [11].

The scenarios listed below 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) that occur because of the collision. This means that they align closely with the types of scenarios already covered in safety accident investigation courses:

- Scenario A. Position and direction - “You are not where you think you are.”
- Scenario B. Maintenance and operations - “Systems are not as expected.”
- Scenario C: Emergency procedures - “Limited time, inaccurate information”
- Scenario D: Not important for safety - “Safety-critical or non-safety critical?”
- Scenario E: Good office hygiene, afloat, onshore
- Scenario F: Emerging technology

The scenarios are outlined in more detail in Table 5.

Once the scenarios had been prepared they were then discussed with both safety and cybersecurity teaching professionals in order to identify the higher priority scenarios for use in a teaching context (Figure 6) as well as the wider safety professional community (Figure 7), who were asked to identify their top two priority scenarios.

An ENISA publication on cybersecurity trends to 2030 was used to provide a broader context for the development of the scenarios (Figure 8). The increased use of cloud services, along with remote access and data management of onboard and shore systems, combined with supply chain (complexities) highlights the importance of considering these topics:

- Supply chain compromise of software dependencies
- Human error and exploited legacy systems within cyber-physical ecosystems
- Lack of analysis and control of space-based infrastructure and objects
- Skill shortage
- Cross border ICT providers as a single point of failure

It was notable that the biggest differences between the safety accident investigation academics and the cybersecurity academics were for scenarios E (good office hygiene, which covers elements such as ransomware and phishing) and F (emerging technologies). They were ranked at opposite ends of priority scale, reflecting the relevant exposure of the two sectors to these types of incidents. The emerging technology category was ranked as the second most important for teaching, reflecting the absence of existing safety accident investigation studies. This rapid cross-check showed the importance of taking a combined approach across both discipline areas when developing the scenarios.

Further discussions were held with two academics, one from each discipline, to explore the context for each of the scenarios (Table 6). The different perspectives highlighted the importance of developing credible cybersecurity scenarios for non-cybersecurity specialists, whether safety accident investigators or otherwise.

The scenarios were then reviewed by the authors to make an initial valuation of their teachability (availability of material, reasonably foreseeable scenarios, gamification) and pedagogical approaches that could be used (Figure 9). The scenarios A (position and direction) and E (good office hygiene) were identified as the ones which had the most potential for use with a maritime safety accident investigation cohort. Loss of position and direction information is integral to many existing maritime accidents and therefore would be more easily teachable within the context of other accident scenarios.

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

Figure 6: Results of a scenario ranking exercise to assess the priority for the teaching of cybersecurity within a (safety) accident investigation MSc. (#1: Most important). Carried out in 1-2-1 conversations.

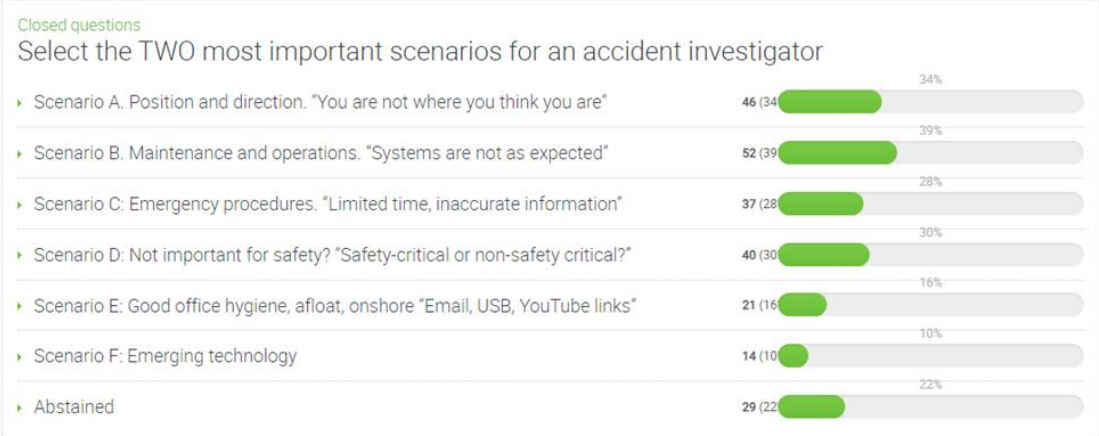

Figure 7: Results of an online consultation with more than one hundred respondents [4]

[4] Incorporating cybersecurity knowledge into safety accident investigation: An educational perspective. – The Safety and Reliability Society (sars.org.uk)

Figure 2: Top 10 threats

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

Figure 8: ENISA report outlining emerging cybersecurity threats for 2030.

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

Figure 9: Preliminary evaluation of teachability and pedagogical approaches for the six scenarios

Table 5: Six reasonably foreseeable scenarios developed to support teaching of cybersecurity within a safety accident investigation course.

Scenario defined in this study	**Summary rationale for scenario**	**Additional notes**
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 analysis	There are a range of ways in which position and direction can be modified. ● GNSS denial ● GPS Spoofing ● Interference with navaids (navigation aids) ● ECDIS (electronic chart and depth information system) ● Slight course adjustment leading to collision or arrival elsewhere (rationale may include a range of reasons e.g. 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 maintenance and operations e.g. ● 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. Other elements of automation – from automated cranes to trucks moving the containers – can be considered.
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 (human machine interface) 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) This theme also includes manual override of emergency fire-fighting systems, communications and more. For a 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 Wi-Fi, 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	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 (machine learning) 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

Table 6: Additional observations on the scenarios from safety accident investigation and cybersecurity academics

Scenario defined in this study	**Additional comments (safety accident investigation teaching academic)**	**Additional comments (cybersecurity teaching academic)**
Scenario A. Position and direction *"You are not where you think you are"*	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.	In practice position modification is more difficult to achieve in the real world than theory, via GPS transmitters (specifications, power etc. above a threshold).
Scenario B. Maintenance and operations *"Systems are not as expected"*	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).	Likely biggest clash between safety and cybersecurity. Perception that safety-critical systems are safe "certify then freeze," whilst cyber "fix it now."
Scenario C: Emergency procedures *"Limited time, inaccurate information"*	There is the potential for overwhelm, including both cybersecurity and safety-related malfunctions across multiple systems, people then do not know which data to trust. Similarly, overreaction (course correction) at speed can lead to loss of control event.	Safety/safe operations impact broad range of systems, but safety specialists may not be interested in non-safety critical.
Scenario D: Not important for safety? *"Safety-critical or 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).	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).
Scenario E: Good office hygiene, afloat, onshore	This is recognised as important in the professional (and personal) spheres but the contribution to (safety) accident investigation is underappreciated.	Should be taught to all. Consider teaching this first.
Scenario F: Emerging technology	Whilst incidents with emerging tech have not 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.	Deep fakes and misinformation are the areas of concern, the broader political domain but it is unclear how these impact on safety.
General to all scenarios	Cross-cutting theme of the potential for "claim" of access being sufficient to create an adverse response. For example, it is 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 does not need to be achieved.	Cross-cutting theme of communications e.g. all phone calls are digital (VoiP).

Opportunities for short lectures to fill certain topic area gaps.

In addition to the incorporation of six cybersecurity-based reasonably foreseeable scenarios, as outlined in this report four additional lectures can be added to the existing safety accident investigation syllabus.

New taught module recommendations for generic content to be added:

- 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 (linking to CyBOK)
    - 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 considered 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.
- 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)

Further Work

This short study is an initial step towards identifying opportunities for integrating cybersecurity into the discipline of (safety) accident investigation using the Cybersecurity Body of Knowledge (CyBOK). This is an emerging field without established best practice. Further development is needed but there is a need to avoid modifying the scenarios for “acceptability” (believability) or perceived likelihood of occurrence and to continue to focus on teachability.

Some topic areas require further work, including how the three CyBOK security-related themes (Systems, Infrastructure, Platform and Software) can be considered, given the lack of cybersecurity content and skills in the safety accident investigation cohort discipline. These three areas may be better explored through scenarios based on autonomous vehicles and cyber sensor attacks.

An evaluation is made of which elements of the HORA theme (human organisational regulatory aspects) could be incorporated should be prioritised in follow on work.

The results presented here are preliminary and due to the emergent nature of the pedagogical research involved with incorporating cybersecurity into safety accident investigation scenarios, there has been limited reference to more established research methods. For example, it was initially proposed to use organisational biases as part of the consultation process. However, this was not implemented due to the limited field experience to date in teaching cybersecurity scenarios to (safety) accident investigators (“early pedagogical TRL stages"). The application of organisational biases as part of the development of hybrid safety-cybersecurity scenarios should 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. In addition, the ‘thinking stages’ from Bloom's taxonomy can potentially also be applied in future classroom-based tests of the scenarios, incorporating observation of student cognitive processes.

International factors are often important in safety accident investigation. Several 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, and this 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

Further skills development needs will shape more in-depth scenario development.

Being able to rule out cyber is also an integral part of investigation. The next stage in skills development will include being able to “rule in, rule out” possible causes, requiring a more in-depth cybersecurity skill set. 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.

Overall, there is a wide range of further work that needs to be initiated to mature the development of cybersecurity-related scenarios linked to CyBOK resources that can be integrated into existing safety accident investigation courses.

Conclusion

There is growing recognition that cybersecurity risks need to be incorporated into safety management systems. However, there is a gap in hybrid safety-security academic courses, hindering the development of much-needed skills across different sectors. In addition, the lack of open-source real-world case studies and mature hybrid investigation methodologies makes teaching cybersecurity within the context of safety accident investigation particularly challenging. As a result, cybersecurity integration into the safety domain has been limited.

The increasing complexity of systems, and the rise of remote access and cloud services integral to system operation, make addressing the skills and teaching gap around safety-security intersection an increasingly important priority. There is low awareness, and challenges present when academics aim to add cybersecurity into already packed safety-related curricula. This study evaluated approaches to broadening the reach and impact of the Cybersecurity Body of Knowledge (CyBOK) through a feasibility study on teachability to bridge this gap.

Alongside the increasing academic focus on hybrid safety-security, the regulatory landscape is evolving, with increased scrutiny on combining safety and cybersecurity management. Across a range of sectors, incident and near-miss investigations are an integral part of the regulatory activity. To address these gaps, credible teaching scenarios are needed to train accident investigators, even without established case studies of safety-informed investigation methodologies being available. Clearly, challenges arise due to a lack of real-world case studies and hybrid safety-security academic courses, hindering skill development in this area. This is particularly relevant for Critical National Infrastructure (CNI), where digitalisation is blurring the lines between IT and operational technology (OT) security.

To address this need, Cranfield University has evaluated the teachability of cybersecurity within safety accident investigation through a Royal Academy of Engineering Visiting Professorship held by the lead author. The study methodology involved mapping CyBOK themes to safety accident investigation syllabuses as taught at Cranfield, with a focus on two key modules: ‘Fundamentals of Accident Investigation’ and ‘Applied Marine Accident Investigation’ Some CyBOK materials are more accessible than others for development and use of scenario-based teaching within Cranfield’s MSc programs, given the constraints caused by the complex interface between safety and cybersecurity. A scenario-based teaching method is the preferred approach, as it aligns with the existing safety accident investigation framework, where case studies of past incidents are commonly used for learning.

Insights from rail accident investigations, particularly the UK Cambrian rail line ERTMS (digital signalling) incident, were used to highlight the complexity of managing digital safety, which combines safety and cybersecurity for digital systems. Investigators encountered challenges in capturing accurate information on software versions and understanding discrepancies between assessed and implemented versions. This example of complex and challenging investigation revealed the risks of assuming that system safety is guaranteed once safety-critical elements are signed off, overlooking the potential hazards from non-critical systems or software updates. All systems, safety-critical and non-safety-critical are vulnerable to cybersecurity modifications. Whilst cybersecurity was not identified as a root cause, the investigation process and development of scenarios informed this project’s approach.

This report also considers the framework for integrating cybersecurity principles into safety accident investigations as input to developing the scenario-based teaching resources. Safety risk management is structured into three categories of controls: People, Processes, and Plant (technology), aligned with ISO31000. Technical controls, which can be prioritised over administrative ones due to the hierarchy of controls guidance embedded in the MHSW Regulations, are crucial in managing risks, and regulators closely monitor these frameworks. Safety management systems form the cornerstone of many regulatory evaluations, across multiple CNI sectors.

Given this context, two approaches for building teaching scenarios emerged: focusing on technical control failures and examining the roles of people and processes in accidents. Integrating both these approaches into accident investigation teaching can expand the scope of investigations to include both safety-critical and non-safety-critical systems, thereby enhancing investigators’ ability to manage digital safety risks effectively.

Key tasks included analysing the CyBOK themes against safety investigation modules to identify potential integration points and challenges, evaluating safety risk management structures, and ranking CyBOK topics based on their

suitability for teaching. A ranking system was developed to assess how well CyBOK content could be integrated into safety investigation courses. The scale ranged from "directly associated" to "no available point of reference." Mapping CyBOK themes to accident investigation syllabuses revealed at times limited overlap between highly technical cybersecurity themes and existing accident investigation curricula. The CyBOK Attacks and Defences theme showed the most potential for integration into safety accident investigation teaching, especially in linking technology-based controls to human and management systems, offering a pathway to teach safety investigators about managing both safety-critical and non-safety-critical systems.

The study also reviewed recent open-source marine cybersecurity incident information to explore overlaps between safety and cybersecurity, particularly in managing risk across people, technology, and processes. Six scenarios were developed for a scenario-based teaching method, leveraging the existing use of case studies in safety investigation. Recognizing the complexity of maritime systems, the scenarios were designed to reflect real-world challenges in maritime operations, such as system complexity, the role of non-human factors, and the difficulty of managing digital data.

The scenarios developed addressed incidents like navigational errors, maintenance failures, emergency procedure malfunctions, and distinctions between safety-critical and non-safety-critical systems. They focussed on situations such as navigation disruption, system updates, human-machine interface failures, and acknowledged emerging technologies such as autonomous vessels and machine learning. The scenarios were evaluated for their relevance to real-world maritime safety incidents, ensuring they could be effectively taught within a safety-focused context. Insights from both past rail and marine cybersecurity incidents informed the scenario development, illustrating the complexity of digital safety management and the risks posed by software updates, system discrepancies, and human factors.

Feedback was gathered from senior academics in safety and cybersecurity through interviews, and an interactive webinar, to rank the scenarios by importance and teachability. Input from both safety and cybersecurity professionals was used to prioritise these scenarios, revealing different perspectives between the fields, particularly on topics like emerging technologies and office hygiene. Additional cybersecurity lectures to support a safety accident investigation course were proposed, covering organisational factors, human elements in cybersecurity, and forensic data gathering. These would help bridge the gap between traditional safety investigation and the emerging cybersecurity risks present in modern maritime systems.

Despite limitations, such as the complexity of combining the two disciplines, and the subjective nature of expert judgement, the study identified several promising areas for further work. These include developing scenarios around car sensor hacks and using human factors frameworks for cybersecurity education. The CyBOK theme Human Organisational Regulatory Aspects (HORA) may also usefully support future work. The methodology and findings serve as an early-stage exploration of how cybersecurity can be taught within the context of safety accident investigation. Broadening of scenario development is required, particularly in exploring CyBOK topics such as Systems, Infrastructure, Platform, and Software security which do not map well to existing safety accident investigation syllabuses. For all topic areas it is important to avoid adjustments to scenarios for perceived acceptability or likelihood, and to focus on the teachability of underlying concepts.

Cultural and regulatory differences in the international maritime space will also play a role in how cybersecurity is integrated into safety accident investigations. Expanding cybersecurity skill sets is crucial, particularly in enabling investigators to "rule in or rule out" cyber-related causes during safety investigations. The investigation process must account for technical disparities between nations and regulatory impacts on cybersecurity. Furthermore, the next phase of scenario development must consider environmental incidents and cyber-attacks on control systems used in environmental response. All these factors will play into priorities for further work.

This evolving field also needs further pedagogical work to integrate cybersecurity into safety investigation education effectively. Future phases should incorporate organisational biases and apply frameworks like Bloom’s taxonomy to assess student cognitive engagement. International factors, such as cultural and regulatory differences, will impact how scenarios are taught in diverse student cohorts.

The CyBOK (Cybersecurity Body of Knowledge) framework offers a lens for incorporating cybersecurity into safety accident investigation teaching, particularly through the development and use of scenario-based teaching. Continued development of teaching scenarios and further exploration of underrepresented topics will be necessary to fully realise

the potential of CyBOK in this context. In conclusion, while this study is an early step in integrating CyBOK into safety accident investigation education, the findings underscore the need for more work, noting the potential of cybersecurity to enhance the scope and depth of safety investigations. Other factors shaping the direction of work include emerging regulatory frameworks and guidance that address hybrid safety-cybersecurity, with a range of challenges noted in the IET Code of Practice in Cyber Security and Safety.

References

[1] The Institution of Engineering and Technology (IET), Code of Practice on Cyber Security and Safety, Code of Practice: Cyber Security and Safety (theiet.org), report, accessed 2/8/24.
[2] The Office of Rail and Road (ORR) Annual Report of Health and Safety on Britain's Railways 2023 to 2024, Section 1.92, Annual report of health and safety on Britain's railways 2023 to 2024 | Office of Rail and Road (orr.gov.uk), report, accessed 2/8/24.
[3] The Health and Safety Executive (HSE), Cyber security - Electrical, Control and Instrumentation (E, C&I) - HSE, website, accessed 2/8/24.
[4] The PETRAS National Centre of Excellence for IoT Systems Cybersecurity (2016-2024), Petras - Home (ucl.ac.uk), website, accessed 2/8/24.
[5] Appleton, P., Working with the rail industry to respond to cyber security threats | Office of Rail and Road (orr.gov.uk), blog, accessed 2/8/24.
[6] The UK National Cyber Security Centre (NCSC), Operational Technology (OT) - NCSC.GOV.UK, website, accessed 2/8/24.
[7] The Cybersecurity Body of Knowledge (CyBOK), CyBOK – The Cyber Security Body of Knowledge, website, accessed 2/8/24.
[8] Taylor, E. A., Safety-Cybersecurity Education: Enabled by Deaf Awareness, Delivered Through Gamification, presented at the AdvanceHE Teaching and Learning Conference 2024, https://www.linkedin.com/pulse/test-title-dr-emma-taylor-cissp-ceng-qnq5e/, results reported by blog, accessed 2/8/24.
[9] Mead, N. R, and Tenbergen, B., CyBOK Usage in the Classroom, August 2023, Report_CyBOK_Usage_Classroom.pdf, report, accessed 2/8/24.
[10] The UK Department for Transport (DfT) funded MarRI-UK activities, Maritime Research and Innovation UK (marri-uk.org), website, accessed 2/8/24.
[11] Meland, P.H. et al., A Retrospective Analysis of Maritime Cyber Security Incidents, TransNav the International Journal on Marine Navigation and Safety of Sea Transportation, 15(3), 519-530, Sept 2021.
[12] Sharunova, A. et al., Applying Bloom's Taxonomy in Transdisciplinary Engineering Design Education, International Journal of Technology and Design Education, 32, 987–999, 2022.
[13] The Rail Accident Investigation Branch (RAIB), Loss of Safety Critical Signalling Data on the Cambrian Coast Line, 17/2019, Loss of safety critical signalling data on the Cambrian Coast line, 20 October 2017 (publishing.service.gov.uk), report, accessed 2/8/24.
[14] Taylor, E. A., Incorporating Cybersecurity Knowledge Into Safety Accident Investigation: An Educational Perspective, Incorporating cybersecurity knowledge into safety accident investigation: An educational perspective. – The Safety and Reliability Society (sars.org.uk), webinar and panel discussion, accessed (SaRS members only) 2/8/24