Received 10 May 2023
Revised 18 July 2023
21 August 2023
1 September 2023
Accepted 1 September 2023

# Human factors and cyber-security risks on the railway – the critical role played by signalling operations

Eylem Thron
*MIMA, London, UK*

Shamal Faily and Huseyin Dogan
*Computing and Informatics Research Centre, Bournemouth University, Bournemouth, UK, and*

Martin Freer
*MIMA, London, UK*

## Abstract

**Purpose** – Railways are a well-known example of complex critical infrastructure, incorporating socio-technical systems with humans such as drivers, signallers, maintainers and passengers at the core. The technological evolution including interconnectedness and new ways of interaction lead to new security and safety risks that can be realised, both in terms of human error, and malicious and non-malicious behaviour. This study aims to identify the human factors (HF) and cyber-security risks relating to the role of signallers on the railways and explores strategies for the improvement of "Digital Resilience" – for the concept of a resilient railway.

**Design/methodology/approach** – Overall, 26 interviews were conducted with 21 participants from industry and academia.

**Findings** – The results showed that due to increased automation, both cyber-related threats and human error can impact signallers' day-to-day operations – directly or indirectly (e.g. workload and safety-critical communications) – which could disrupt the railway services and potentially lead to safety-related catastrophic consequences. This study identifies cyber-related problems, including external threats; engineers not considering the human element in designs when specifying security controls; lack of security awareness among the rail industry; training gaps; organisational issues; and many unknown "unknowns".

**Originality/value** – The authors discuss socio-technical principles through a hexagonal socio-technical framework and training needs analysis to mitigate against cyber-security issues and identify the predictive training needs of the signallers. This is supported by a systematic approach which considers both, safety and security factors, rather than waiting to learn from a cyber-attack retrospectively.

**Keywords** Human factors, Cyber-security, Railway, Safety, Resilience, Training needs

**Paper type** Research paper

## 1. Introduction

Railways are complex, safety-critical infrastructure systems (Wilson, 2007) which have traditionally been largely mechanical in nature. Train drivers and signallers predominantly



The authors would like to express gratitude to Chris Avis at MIMA, who provided valuable comments and feedback on this manuscript.

Information & Computer Security
Vol. 32 No. 2, 2024
pp. 236-263
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-05-2023-0078

operated mechanical or electro-mechanical equipment and interfaces and communicated with each other, and railway controllers, by fixed telephone lines or closed radio systems. However, over the past 20 years or so, particularly in the UK, there has been a huge increase in passenger demand that could not be satisfied by simply increasing the available infrastructure in a country with such limited space. Instead, technological solutions are increasingly being used to expand the capacity and efficiency of the legacy infrastructure. This has led to the on-going evolution of a Digital Railway, gradually transforming it into a cyber-physical system (CPS) similar in nature to others which have already made the leap, such as banking, defence or health industries.

In this relatively short time, the UK railway has gone from localised mechanical signalling with semaphore signals to computer-based signalling with colour light signals, automatic train protection (ATP), and more recently it has begun to operate in-cab signalling. These advances have led to improved operational efficiency through centralisation of control, increasing automation and remote condition monitoring, which, in turn, has led to increased capacity, reliability, energy efficiency and cost effectiveness.

However, this digitisation of the railway naturally involves distributed computer-based systems networked over the internet, cloud-based data storage, internet protocol addressable components (such as closed-circuit television cameras) and so on, all of which present potential cyber-security vulnerabilities that are well-known in other industries but are new to the railway.

As this rapid digital transformation is becoming exponentially widespread across the railway; it has come to include booking and ticketing, customer information systems, security monitoring, communications, remote condition monitoring of system components, and via traffic management, train control and train automation systems. Importantly, there is also growing interest in layering artificial intelligence (AI) across these various railway systems to further increase operational capacity and efficiency. The exposure to potential cyber-security vulnerabilities is thus spreading across the width and breadth of the railway system as more and more of it is digitised, and as result it is increasingly changing the role of the human actors the system, such as signallers, controllers, train drivers and maintainers.

### *1.1 Cyber-security*

Cyber-security is the activity, process, ability, capability or state whereby systems and component information are protected from unauthorised use, modification or exploitation (Evans *et al.*, 2016). Cyber-security risks within critical infrastructure such as railways can result in catastrophic damage, ranging from financial and reputational loss to safety and potential loss of life or deny the use of infrastructure to its operator or other users.

### *1.2 Cyber-security incidents*

Cyber-attacks are now threatening critical infrastructure such as hospitals, financial institutions, security services and railways, as evidenced by several cyber-attacks in the past decade on various CPS (Caire, 2017; Fachot, 2018; Tyagi and Sreenath, 2021). For example, the "WannaCry" outbreak impacted hospitals and general practitioner surgeries across the UK in 2017, resulting in the cancellation of thousands of appointments and operations (Wikipedia, 2017). In 2021, a cyber-attack on the UK's Defence Academy caused significant damage. In 2022 alone, there were 1,829 reported cyber incidents in the financial industry worldwide (Statista, 2023). In a very recent data breach case, the names and ranks of every serving officer in Ireland were exposed by the Police Service of Northern Ireland and caused significant risk (BBC, 2023).

Like most other critical infrastructure, railways are increasingly comprised of complex CPS, where safety and security are of paramount importance. There have already been

numerous attacks on the railways around the world, ranging from passenger information systems to rolling stock, and even including the unintended movement of points under a tram (Baker, 2008; Antoni, 2018). The UK railways experienced four attacks in 2016 (Sky, 2016), and there have been various attacks in North America (Caire, 2017; Fachot, 2018). In December 2020, a ransomware attack damaged the operations of TransLink, the public transportation agency for the city of Vancouver, Canada, which left residents unable to use their Compass metro cards or pay for new tickets via the agency's Compass ticketing kiosks (CBC News, 2020). In another example, in 2003, a malware infection of a company's system in Florida disrupted signalling, dispatching and other operational systems, resulting in widespread delays (Bastow, 2014).

Similar incidents took place in Europe. The "WannaCry" attack also precipitated system failures in Deutsche Bahn AG rail infrastructure, with ransomware messages appearing on station information screens and subsequent widespread disruption of operations. This was widely regarded as a "wake-up call" for the railway industry, as described by cyber-security experts (RailTech, 2017). Denmark also suffered from a cyber-attack to its train network in 2022, which caused a major breakdown (Euronews, 2022), as well as did Italy (IRJ, 2022).

There are also operational risks, such as when in October 2017, a Distributed Denial-of-Service (DDoS) attack was blamed for the partial shutdown of Sweden's Transport Agency (Transportstyrelsen) website, causing subsequent train delays across large parts of Sweden (The Local, 2017). From the perspective of train operating companies, cyber-attacks could impair drivers' usage of the system, they can also cause reputational damage, result in the loss of customers' personal data and have serious financial costs in terms of both system repair and compensation for passengers affected by the resulting disruption, as well as serious regulatory repercussions and other legal liabilities as other CPS environments have experienced. Thus, in addition to societal, safety and operational risks of cyber-attacks on the railways, there are also business risks ranging from loss of revenue to reputational loss. In April 2018, Great Western Railway found that around 1,000 of its passengers' details had been compromised. This revealed ticketing systems to be a highly exposed rail information system with similar vulnerabilities to those faced by other similar websites (e.g. payment security that requires sophisticated mitigation strategies) (BBC, 2018).

Cyber-attacks or malicious targeting by terrorists, foreign state actors or hacktivists can also not be excluded. Recent cyber-attacks on Ukraine, Belarus and Russia showed that railways are now potential targets in warfare through state hackers who are seeking to disrupt transportation systems even at the risk of causing loss of life (Reuters, 2022; Guardian, 2022).

Cyber-attacks on the railways are likely to increase, given the growing extent and complexity of rail networks and constant innovation by organised crime groups, hacktivists and nation states. Rail infrastructure being relatively unprotected and attacks not being easily attributable also makes rail transport a "high-value and soft target" for cyber-attacks (Caire, 2017; Gabriel *et al.*, 2018; Ghafir *et al.*, 2018; Thaduri *et al.*, 2019).

In terms of potential risks and consequences, a cyber-security attack or accidental breach in a railway system is similar to other critical infrastructure comprised of complex CPS. Increased connectivity and automation makes attacks easier, more convenient and potentially possible from other countries on a networked system (Gabriel *et al.*, 2018; Thaduri *et al.*, 2019).

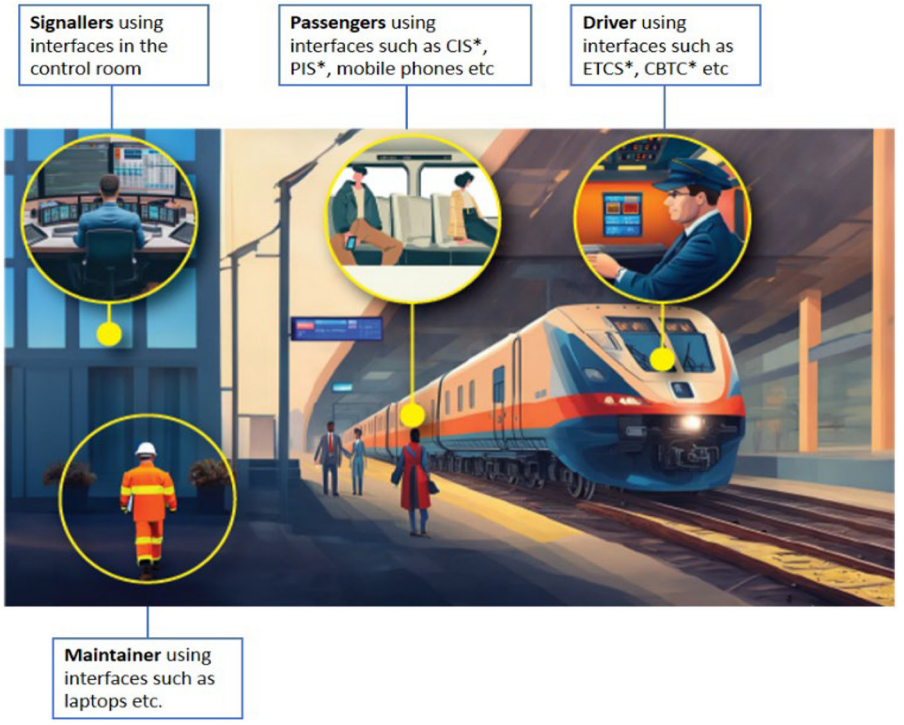
The developing deployment of digital communication and signalling systems, such as the European Rail Traffic Management System (ERTMS), while beneficial in terms of improved safety, increased efficiency and capacity, also introduces new risks on the railways. Any cyber breach on these modern systems can have more widespread

consequences, potentially leading to accidents, injury or even loss of life, making it a higher-stakes environment.

*1.3 Railways as socio-technical systems*

While considering cyber-security concerns, one important point to note is that railways are socio-technical systems with humans, such as drivers, signallers, maintainers and passengers using them on a daily basis. Each group independently interacts with various systems in different and occasionally unexpected ways, and they will continue to do so with increased digitisation on the railways (see Figure 1). This emphasises the importance of human factors (HF), which includes the study of human behaviour; in particular, how they interact with rail systems, how they manage tasks and how they perform in given situations and environments. Understanding and integration of rail HF is acknowledged to be a crucial part of railway operations and safety (Wilson, 2007; Wilson *et al.*, 2007). Additionally, because HF methods provide data and evidence based on real people, it promotes a better understanding of safety and security risks and provides engineering support to mitigate accidental incidents or malicious threats.

In terms of HF-related risks, as railways are used by a large number of passengers, power breakdowns due to a cyber incident could lead to secondary hazards as railway staff attempt to manage the situation and safely return passengers to stations without full system functionality or passengers lose patience and attempt to find their own way out of trains.




**Notes:** CIS = customer information system; PIS = passenger information system; ETCS = European train control system; CBTC = communication-based train control

**Figure 1.** High-level socio-technical representation of the railway users (designed in leonardo.ai and augmented by Adobe Photoshop, copyright Mima 2023)

Thus, HF, with its focus on human behaviour, provides a mechanism for security concerns to be recognised as safety risks worth investigating further.

The next section will describe the characteristics of signallers, potential risks around their role and everyday use of railway CPSs.

### *1.4 Signaller's role*

The signaller's role is critical in ensuring the safety of train operations. Their main purpose is to regulate the movements of trains via signals (lineside or in-cab indications) within an area of control that they are trained to operate. The signaller will set routes for trains and manage controlled level crossings, making sure they are clear of vehicles and pedestrians before allowing trains to cross. This is vital to ensuring trains get to and from their destinations according to the timetable. They also manage maintenance access to the track (line blocks and possessions) to ensure that people working on the infrastructure are safely segregated from running train traffic. They consequently work on multiple tasks, process large and complex amounts of information quickly, make critical decisions in real-time, work in shifts and control rooms often operating 24/7 and communicate with multiple people in a busy railway environment (see Plate 1). The pressure of making the right choices under time-sensitive conditions can be significant, especially in degraded modes where equipment faults, failures or incidents that delay train movement occur, increasing the risk

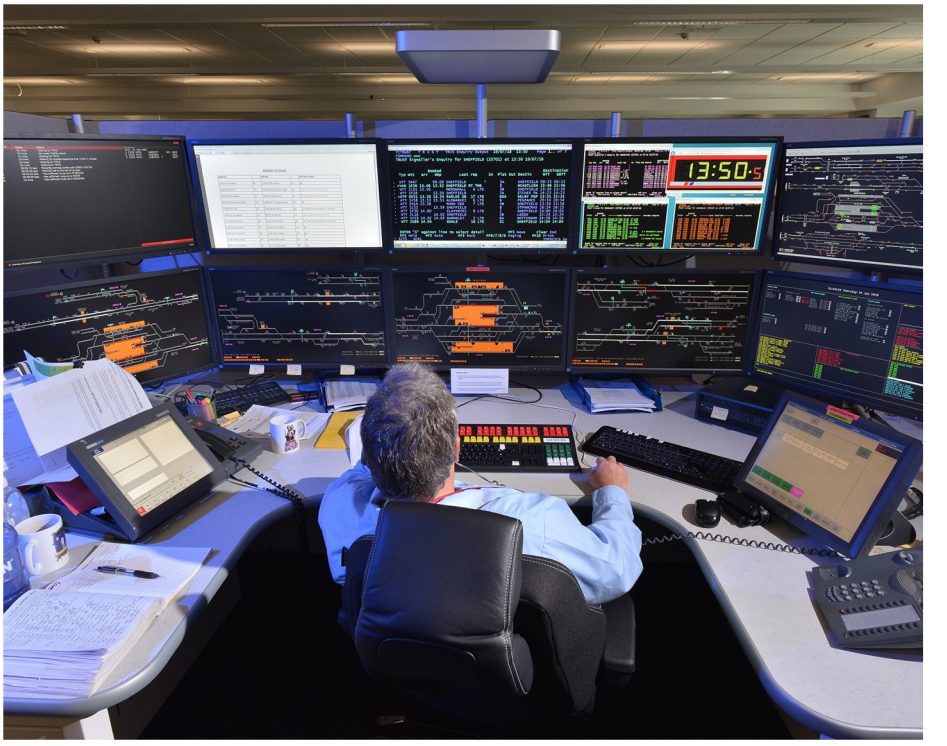



**Plate 1.**
Modern control rooms

**Source:** RailEngineer (2021)

of human error (Sharples *et al.*, 2011). Any mistakes or errors can have serious consequences, which may lead to incidents and accidents.

Cyber-security risks related to signaller tasks require investigation due to the potential risks around their safety-critical role, ever-increasing automation and existing system integration and HF challenges they encounter during their day-to-day operations. Overall, not only are signallers the most safety critical operators and recently exposed to new threats, but they are also among the least trained or aware of the emerging risk.

### *1.5 The gap in research*

To date, there is very little research on cyber-security issues around human error and non-malicious threat of operators on critical infrastructure, such as railways. Broad risk mitigation strategies for mitigating well-known cyber-security threats on the railways typically focus on the technology, while the HF-related research has been limited, with the consideration of password generation being the only notable exception (Metalidou *et al.*, 2014). Interestingly, often poor technological design "solutions" are eventually found to be the real cause of human errors or mistakes, where rules relating to cyber-security are intentionally disobeyed due to "cumbersome design" of systems (Altaf *et al.*, 2019).

The signaller's role is safety-critical, similar to most of other operators using CPSs. However, as railways are adopting more automation, the role of signallers increasingly evolves to include managing complex automation in their day-to-day systems. Studies to date provide very little insight into the HF or "readiness" aspect of signallers to the fast-changing "Digital Railway", despite increasing levels of risk and the growing list of consequences that could result from a cyber-attack on control systems. Given these factors, it is essential to investigate risks and challenges related to signallers in control rooms to ensure effective human-machine interaction, improve safety, enhance human performance, ensure efficient operation of railway networks, all the while identifying and managing the growing range of potential cyber-security threats and risks they are starting to face.

Thus, this study aims to help to close this gap by considering the role of the signaller, the HF cyber-security issues they face within the context of their activities, and understanding how those issues can lead to current and future security and safety risks and present strategies for resolving them. These are motivated by the following two main research questions:

*RQ1.* What are the current and future HF issues around cyber-security for railway CPSs, and how are HF-related issues impacting the role of signallers in particular?

*RQ2.* How could these cyber-security risks be mitigated and, as a result, the overall "Digital Resilience" be improved, i.e. novel cyber-resilience strategies to improve security and make railways flexible/resilient to cyber-attacks, with regard to making the "whole" of the railway resilient, including the human elements?

The research questions would be similar for other CPSs in other industries (e.g. nuclear, air traffic control, process control, etc.) and their operators' roles.

In Section 2, we first provide a summary of some of the main research outcomes within wider cyber-security and related HF issues, followed by the risks specific to the railway industry. We will then discuss potential mitigating strategies. Section 3 details the methodology, and Section 4 discusses the findings of interviews ($n = 26$) conducted with various experts from the railway industry, and Section 5 presents the discussion.

The key themes from the literature review are presented in Section 2.

## 2. Related work

### *2.1 Literature review*

A systematic literature review was conducted for this study. The articles selected have the aims and objectives related to HF and cyber-security issues and/or mitigations on critical infrastructure, railways, workplaces and their CPSs. Specifically, systematic searches of six electronic databases were conducted, including the Web of Science, Scopus, Science Direct, PubMed, ScienceOpen and SpringerLink. A bibliography tool, Google Scholar, was also used to identify relevant articles, and high-quality, peer-reviewed journal papers were prioritised.

As this study is multidisciplinary, covering several scientific disciplines, the publications were selected from a wide range of disciplines; such as psychology; social sciences; HF; information security; computer science; transportation; railways and engineering management. A Boolean keyword search was used with key terms, "AND" and "OR", including cyber security, cyber resilience, information security, human factors, railway, critical infrastructure and cyber physical systems with variations of those keywords. A total of 52 papers and articles were initially selected for review after the search criteria were applied. Following the completion of the final screening, further journal and conference papers, as well as industry-led publications and reports, were also reviewed, as detailed in the references list.

A summary of the main research outcomes is as follows.

### *2.2 Human error/non-malicious behaviour risk*

Most issues with cyber-security tend to be approached from either human error or awareness perspectives (Metalidou *et al.*, 2014; Evans *et al.*, 2016; Widdowson, 2016; Gratian *et al.*, 2018; Jeong *et al.*, 2019) or technology perspectives (Wright and Jun, 2019; Leveson, 2020).

Human error/non-malicious behaviour literature showed that the majority (over 80%) of cyber-security breaches are ascribed to human error or non-malicious behaviour (Metalidou *et al.*, 2014; Evans *et al.*, 2016; Hadlington, 2018) for a range of systems and industries.

Non-malicious behaviour can include unintentional/accidental information sharing, additional workload related to new technology fatigue, memory lapse, misjudgement, lack of understanding, lack of knowledge, lack of motivation, risky beliefs, risky behaviour, lack of training, lack of awareness, poor planning, lack of attention to detail, ignorance and accidental insider (Metalidou *et al.*, 2014; Evans *et al.*, 2016; Hadlington, 2017, 2018; Ghafir *et al.*, 2018). This behaviour can be exhibited both by the general public and operators working on critical infrastructure (Kour *et al.*, 2019).

Research on the impact of individual characteristics (e.g. personality, demographics and risk-taking preferences) on security behaviours showed that some personality traits (e.g. high extraversion, high neuroticism) were linked to unintentional or accidental information sharing; as well as demographics such as younger age and being female (Gratian *et al.*, 2018; Hadlington, 2018; Jeong *et al.*, 2019), specifically for users of business or public systems.

These studies suggest individual differences could be used to predict "good security behaviours" and made recommendations around "tailored security training and awareness" (Gratian *et al.*, 2018; Widdowson, 2016). However, they lack information about how such "customised training" would be implemented across industries and, for safety-critical roles, how individual differences might inform about cyber-resilience in certain risky situations (e.g. when the technology fails) or the cost-impact of "tailored" training across industries.

Various studies also suggest that poor (cumbersome) technological design may induce operators to make what are perceived as human errors or mistakes, but where, in fact, rules

are not followed due to "inadequate design" of systems (Altaf *et al.*, 2019). To tackle such issues, several human–computer interaction (HCI) techniques recommend supporting the security awareness approach (Altaf *et al.*, 2019) for safety-critical industries in particular.

*2.3 Organisational factors*

Organisational culture is described as a culture that is associated with a business and/or work organisation by Jeong *et al.* (2019). Research shows that organisational factors contributing to security risks are still poorly understood (Malatji *et al.*, 2019; Thaduri *et al.*, 2019; Wright and Jun, 2019). To fill this gap, there have been some HF studies focused on organisational issues, and new techniques and tools developed in recent years to assess how individual differences (e.g. personality traits and demographics) influence security behaviours around complex digital systems (Metalidou *et al.*, 2014; Ki-Aries and Faily, 2017; Friedberg *et al.*, 2017; Hadlington, 2018; Wright and Jun, 2019).

Some of this research considered humans as "the weakest link" in creating safe and secure digital environments and thus focused on human characteristics, behaviours, risk-taking preferences and mitigations around training and awareness (Metalidou *et al.*, 2014; Caire, 2017; Hadlington, 2017), as discussed earlier. Some other studies highlighted organisational issues around culture, regulatory or assurance (Evans *et al.*, 2016; Kour *et al.*, 2019). More recent research sought insight into a lack of safety-related requirements as the root cause of security-related incidents (Leveson, 2020). Here, the "human" may be central to safety in an otherwise unsafe environment, hence a potential solution to (instead of the cause of) the issue in the right context. Several other studies considered poor technological design as the real cause of human errors or mistakes where rules around cyber-security are intentionally disobeyed due to usability issues or otherwise prevent them from being an effective part of the solution (Altaf *et al.*, 2019). Suggestions are made to design systems around human tasks and goals (Ki-Aries and Faily, 2017; Altaf *et al.*, 2019). As well as traditional techniques and methods (Gratian *et al.*, 2018), numerous new automated risk assessment techniques are being developed to understand the "human" as part of a wider system of systems context – including the organisational aspect of cyber-security (Friedberg *et al.*, 2017; Ki-Aries and Faily, 2017; Altaf *et al.*, 2019; Wright and Jun, 2019).

*2.4 Malicious behaviour*

There is a fast-growing external threat to most computer systems (as, for example, in banking, hospitals) and also on critical infrastructure, including railways (Caire, 2017; Ghafir *et al.*, 2018; Thaduri *et al.*, 2019; Tyagi and Sreenath, 2021). The threat actors (attackers) associated with cyber-security for railways include state actors, hacktivists or hobby hackers, activists, non-politically motivated threats, cyberespionage agents, cyber-spies, cyberterrorists and unsatisfied employees (malicious insiders). Threat actors' motivations range from financial gain to testing their own skills or making the headlines (Chen *et al.*, 2014; Caire, 2017; Gabriel *et al.*, 2018; Hadlington, 2018; Kour *et al.*, 2019; Thaduri *et al.*, 2019; Tyagi and Sreenath, 2021).

As well as the active engagement of skilled and motivated threat actors into systems through their own or funded resources, another major security concern is the threat of social engineering attacks, as discussed in the next section.

*2.5 Social engineering*

Social engineering is a psychological manipulation, persuasion or influence technique used by attackers to get critical or sensitive information from unwilling targets or access to restricted areas (Hadlington, 2017; Ki-Aries and Faily, 2017; Ghafir *et al.*, 2018). Attackers

target human vulnerabilities and succeed due to the characteristics and behaviours of people (Metalidou *et al.*, 2014; Hadlington, 2017; Hadlington, 2018). In their study on security threats to critical infrastructure, Ghafir *et al.* (2018) found that social engineering is among the top information security threats faced by multiple industries and organisations. Ki-Aries and Faily (2017) summarised the issue as social engineering "can bypass or undermine other technological security controls".

### *2.6 Cyber-security risks on critical infrastructure*

Cyber-security studies on critical infrastructure and their CPSs show that cyber-attacks against critical systems are now common and recognised as one of the greatest risks facing today's world; and can include operational, safety, financial, national security and environmental risks (Maglaras *et al.*, 2018; Pollini *et al.*, 2022).

Studies mostly reported on risks related to threat actors (e.g. state hackers), organisational factors (e.g. lack of training/monitoring), as well as vulnerabilities around new and existing technologies and social engineering (Tyagi and Sreenath, 2021). Some of those studies focused on technological aspects of cyber-security vulnerabilities and solutions (Yaacoub *et al.*, 2020), while others looked at attacker motivations, attitudes or attack methods (Alqudhaibi *et al.*, 2023; Riggs *et al.*, 2023).

However, there are few HF studies that consider operators working on critical infrastructure, and there is little published significant HF analysis of cyber-security for control functions, and specifically the role of operators. This is despite increasing levels of risk and the growing list of consequences (both in terms of volume and severity) that could result from a cyber-attack on infrastructure or operators' equipment.

### *2.7 Human factors and cyber-security risks related to railways*

As well as technological and attacker-related risks described earlier, rail systems are increasingly at risk from human error, such as failures to update and configure software correctly. Many cyber-security breaches are due to non-malicious human behaviour or human error, and as such, can affect key railway stakeholders such as signallers, drivers and maintainers. This includes actions as seemingly innocent as attaching unauthorised devices to networks, which may expose or introduce vulnerabilities allowing malicious actors to obtain access to systems. The role of the maintainers and third-party suppliers is also crucial in these scenarios. In some cases, "accidental insiders" are responsible for the incidents without any intention to harm – e.g. "hobby hackers" simply testing their own skills (Altaf *et al.*, 2019). Social engineering or HF issues such as high workload, tiredness, distraction, and subsequently reduced situational awareness can also lead to such incidents. Such incidents could also be linked to the working culture of an organisation.

*2.7.1 Signalling-related risks on the railways.* The UK railway signallers are now being introduced to ERTMS: the European standard for the command, control and signalling (CCS) systems. CCS systems in recent years include safety critical interlocking systems, forms of ATP, automatic route setting (ARS) and related control systems and, on some lines, automatic train operation (ATO), which are introducing increasing levels of automation within rail signalling (Digital Railway, 2018). They typically incorporate some measure of resilience should the signalling system malfunction due to intentional or unintentional circumstances, e.g. a way of mechanically stopping trains.

Signallers control the movement and direction of trains by operating signalling controls or by monitoring, and when necessary intervening with ARS systems. These manage train movements through the network to provide an efficient train service and maintain safety (Sharples *et al.*, 2011).

As well as numerous operational benefits, increased automation and connectivity on the digitised railway also bring with them increased and more far-reaching cyber-security risks to signalling operations. These include:

- Mounting an attack is much easier (e.g. anywhere attackers have a data signal and Wi-Fi);
- Service disruption as the fail-safe nature of systems can be exploited to stop trains;
- Further safety impact due to interconnected and networked train, control and signalling systems; and
- Attacks might target train systems, control systems (e.g. ERTMS) via wireless connected implanted devices, driver machine interfaces (DMIs), line side systems, passenger information systems and signaller traffic management systems in control rooms.

Disruption of the services on the railways (e.g. through taking the signalling down) is a potentially big cyber-security threat. Signalling-related errors could disturb railway services significantly – directly or indirectly. DDoS by taking the Traffic Management System (TMS) down could lead signallers not being able to use safety-critical functionalities (e.g. ARS) or use incorrect settings. A potential cyber-attack could increase signallers' workload and challenge their situational awareness, which would, in turn, impact their safety-critical decision-making.

Studies show that existing signalling systems are often safe; however, the issue with the control systems and safety-critical systems (e.g. interlocking) is often human vulnerability, such as failures in decision-making (Sharples *et al.*, 2011). Furthermore, the issues are often not contained within one system or piece of equipment but rather can be spread across multiple systems that are increasingly networked together. These vulnerabilities can be exaggerated in the event of a cyber incident and are thus worthy of investigation.

*2.7.2 Risks related to organisational factors on the railways.* Organisational factors causing cyber-related risks to the railways are found to be a lack of security culture and awareness, "relaxed" or a very controlling or restrictive organisational culture, and a lack of training/monitoring (Ghafir *et al.*, 2018; Kour *et al.*, 2019).

Ghafir *et al.* (2018) suggest that organisational factors increase cyber-related risks to the railways due to several issues, including a lack of security culture and awareness. Kour *et al.* (2019) highlighted parts of organisational culture (i.e. lack of systematic review of maintenance activities) and lack of training/monitoring can cause the most harm. Several rail organisations, such as CYRail (2018), provided recommendations to overcome such organisational issues. The data and insights from these studies were found to be useful, but suggestions on "cyber awareness" lack detail on considering how they might potentially affect operator workload and how it can be integrated operationally.

Despite the impact of human error and organisational risk related to signallers' day-to-day activities, few studies have examined how cyber-attacks on the railways can be prevented at the human and organisational levels both in terms of "what they cause" and "what they can prevent".

### *2.8 Summary of findings*

In spite of numerous multidisciplinary and multi-faceted research in this area, with studies conducted including a wide range of disciplines; such as psychology; social sciences; HF; information security; computer science; transportation; and engineering management, there remains a lack of HF approaches to understand the interrelationship between the areas of

safety and security for the identification of user-centric and organisational cyber-security risks and potential mitigations.

In particular, there are very few HF-related studies, including detailed consideration of operators working on railways (particularly the key safety critical role of signallers), with mitigation strategies focused on technological means, while the HF-related research has been limited, with the only notable exception of password generation. Additionally, organisational factors are poorly understood; and there have been very few applications of cyber-security and railway operations' HF issues studied within socio-technical models which focus on specific operator tasks and goals (e.g. signallers).

A high-level summary of the outcomes is shown in Table 1 below.

| Risk | Vulnerabilities | Areas |
|---|---|---|
| Human error<br>Non-malicious insider<br>External attacker (malicious) | Human error related to HF<br>Accidental (non-malicious)<br>Personality<br>Negligence<br>Sabotage<br>Rogue attitude<br>Demographic attributes<br>Social engineering<br>Organisational factors (lack of security culture and awareness)<br>Poor technological design (system failure or usability)<br>Software vulnerabilities (new/ updated technology) | Computer and information systems<br>Internet<br>Business systems<br>Public (e.g. university) systems |
| Non-malicious insider<br>Malicious insider<br>External attacker (malicious) | Social engineering<br>External attacker pretending to be an employee (malicious)<br>External attacker intrudes into the system to cause harm or gain power (malicious, e.g. spear phishing, baiting and pretexting)<br>External attacker intrudes into the system out of curiosity or hobby (non-malicious/negligent/reckless)<br>External attacker intrudes into the system in relation to certain characteristics/attitudes<br>Organisational factors (i.e. lack of security culture and awareness)<br>Organisational factors (i.e. lack of systematic review of maintenance activities)<br>Organisational factors (i.e. lack of training/monitoring)<br>Unknown attack vectors<br>Software vulnerabilities (new technology)<br>Legacy systems or system integration challenges | Critical infrastructures within various sectors (nuclear, energy, railway, power grid, health, finance and aviation).<br>Retail systems<br>Public sector systems |

**Table 1.**
Summary of literature findings

**Source:** Created by authors

*2.9 Cyber-security issues within a socio-technical framework*

Nevertheless, HF has significant potential for a better understanding of safety and security risks by providing data and evidence based on real people and could provide engineering support to mitigate accidental incidents or malicious threats. A holistic and socio-technical issues review [Wilson (2007) theory] can help to investigate all aspects of HF, including personal, job/tasks, organisational and wider external (i.e. regulatory) factors in everyday activities of the operators and by investigating recent railway incidents.

Thus, to close this gap a high-level socio-technical view of HF attributes on the railways relevant to signallers were carried out through semi-structured interviews, as detailed further below. The interviews were designed to find out answers to the following questions:

*Q1*. Are there human-related (e.g. human error/accidental insider, behavioural cyber-related risks), organisational or job design factors that may cause railways to be more susceptible to a cyber-attack?

*Q2*. Are the railways, and specifically the operators (e.g. signallers), properly prepared to identify or recognise and deal with a cyber-attack?

*Q3*. Is there a gap in signallers' attitudes, attributes or knowledge of cyber-attack (e.g. would they know the difference between human error and cyber-attack)?

*Q4*. Are there specific functions that may be susceptible to cyber-related risk?

*Q5*. Does automation make systems more vulnerable to cyber-security risks?

## 3. Methodology

*3.1 Procedure*

Several techniques were considered for data collection, including focus groups and questionnaires, experiments or interactive management. Semi-structured interviews were chosen as the most suitable method due to the data size and remoteness of the interviewees, followed by thematic analysis. A snowballing sampling strategy was used to select the study participants as this is a niche area (Biernacki and Waldorf, 1981). The participants were selected from rail infrastructure organisations based on their insight into the day-to-day operations and risks on the railways. Organisations included rolling-stock manufacturers, who are leading the way for future railway technologies, and rail consultancies working closely with rail and cyber-security stakeholders. Participants from major cyber-security firms specialised in solving security-related issues on the railways were also selected for their insight into the type and level of risks. Various rail operators were considered for the study, including signallers and maintainers. Eventually, signallers were chosen as the exemplar case study as they are typically the "first line of defence" and key decision makers following a cyber-attack.

Following the snowball sampling strategy steps, 21 participants agreed to be interviewed. Participants were chosen to reflect a wide range of knowledge and experience in cyber-security, railway operations, design and academia. All participants were either working in the industry or were currently conducting cogent research in collaboration with industry.

A semi-structured interview schedule was drawn up and based upon the findings from previous research on HF-related cyber-security issues. They are a type of qualitative research method where an interviewer asks broad, open-ended questions (Kvale and Brinkmann, 2009). The interview schedule included the background of the interviewee;

experiences in the railway industry, cyber-security/automation or HF and experiences and opinions related to the interview questions. Interview questions considered the HF and cyber-security-related risks on the railways, the strategies for mitigation from the interviewee's perspective, and the role of the signallers and other railway workers during a cyber-attack. Issues with increasing automation, direct or indirect consequences of cyber-related threats, and human error on staff, and passengers and other adversities which could disrupt the railway services, were also discussed.

Each interview lasted between 1 and 2 h, and regular breaks were given during the interviews, as required. Some participants returned for a second interview. Following the interviews, thematic analysis was used to identify themes in the responses. Thematic analysis is a qualitative research method used to identify and group themes from data (Guest *et al.*, 2011; Brooks *et al.*, 2015). After the thematic analysis, theoretical saturation was achieved. Theoretical saturation in qualitative data often signals the end of data collection as additional data collection does not result in new information (Guest *et al.*, 2006). Following this step, around six themes were noted and analysed further.

### *3.2 Participants*

The participants consist of a railway safety executive, HF consultants at various levels, incident investigator/advisors, Internet of Things/cyber-security executive and engineers, railway systems, security and signalling engineers, the UK and European signallers and ex-signallers at various levels, senior academics at universities and lead assessors working on major UK railway projects.

The list of the participants is shown in Table 2.

### *3.3 Analysis*

Each interview was transcribed and thematically analysed using Nvivo, which is a software programme used for qualitative data analysis. It includes importing, categorising, prioritising, managing and analysing unstructured, large data such as interviews and surveys.

NVivo was used to support template analysis to further examine and develop codes using a set of initial (priori) codes based upon data within the headings and sub-headings in the interview schedule. Priori codes are used to study concepts and themes established during this study (Guest *et al.*, 2011) and helped to further organise, code and analyse interview data. Alternatives to thematic analysis, e.g. ontology, a formal system used to analyse data in a systematic way, were considered; however, due to the size of the interview outputs, thematic analysis was chosen as the most suitable method by the researchers.

As discussed in the earlier section, there is a need to investigate whether the rapid digitisation of railways around the world is exposing passengers and operators to new security risks from a "socio-technical" point of view (rather than focusing on human tasks and performance alone). For this purpose, the results of the interviews investigated and summarised under the socio-technical design framework are discussed in the following section.

## 4. Results

Six main cyber-security risks related to the role of the signallers arose from the interviews and subsequent thematic data analysis. These risks, the related HF issues, as well as potential mitigation strategies are considered in the sub-sections that follow.

| Participant no. | Organisation | Job title | Experience |
|---|---|---|---|
| P1 | Rail organisation (infrastructure) | Safety professional | Wide-ranged safety, engineering, security design programmes |
| P2 | Rail organisation | HF consultant | Various railway programmes |
| P3 | Rail organisation | Safety professional | Safety investigation |
| P4 | Rail organisation | Safety professional | Safety investigation |
| P5 | Rail organisation | HF expert | HF programmes |
| P6 | Manufacturer | Security engineer | Security design |
| P7 | Global consultancy | Cyber-security professional | Security engineer |
| P8 | Global rail consultancy | Signalling executive | Control and signalling projects |
| P9 | Global rail consultancy | Digital resilience expert | Cyber-security and systems designer |
| P10 | Global rail consultancy | Railway systems security engineer | Railway systems security engineer |
| P11 | UK railways | Signaller | Train signaller |
| P12 | European railways | Ex-signaller | Train ex-signaller |
| P13 | UK (mainland) railways | Ex-signaller | Train ex-signaller and engineer |
| P14 | European programme | HF lead (European signalling) | Train ex-signaller and trainer |
| P15 | University #1 | HF expert/senior academic | HF expert and senior researcher |
| P16 | University #2 | Doctorate student | Engineering project researcher |
| P17 | Train operating company | Senior manager | Engineer and manager |
| P18 | University #3 | Academic | Academic on HF and cyber-security |
| P19 | Global consultancy | Ex-signaller and consultant | Experience on signalling |
| P20 | Rail organisation | Principal engineer | Signalling expert |
| P21 | Automotive industry | Technology consultant | Experience in automation and cyber-security in automotive and rail industries |

**Source:** Created by authors

**Table 2.**
Participants list

*4.1 Types of cyber-security risk*

*4.1.1 Cyber-attack risks due to increasing automation and connectivity.* There is a wide belief that automation – such as ARS – significantly reduces the contribution of human error to train accidents. One interviewee suggested that signallers "cannot do" without the ARS due to the increased size of their geographical areas. At peak times, signallers are responsible for around 300 people for each "dot" on their screen; thus, they have to know "where the trains are".

Besides various benefits, more automation and connectivity through these systems indirectly introduce cyber-security risks as it is easier to attack the trains. As the safety-critical systems and equipment are increasingly distributed across large geographical areas, it is also now more difficult to ensure that they are secure as it can be difficult to locate them if they are subjected to such an attack. As one of the "worst case scenarios", an attack can take place within the control room where signallers operate on a day-to-day basis.

"Say if all screens go blank (following a cyber-attack), signallers won't know where the trains are (as they cannot know how the automation [ARS] works)" (P11).

More intelligent systems and automation also impact wider operations as the attack can take place anywhere within the infrastructure, e.g. robots used for maintenance, trackside

technology and connected passenger systems alongside automation in the control rooms. Thus, it is unclear what the target can be, and where on the railways it is.

"Often the attacks wouldn't be on the infrastructure, but rather on somewhere else. For instance, systems on the train could be the target (e.g. ERTMS) or anything else – and we wouldn't know" (P10).

Cyber-attack threats on the trains can also impact drivers' day-to-day operations. The resulting risks and consequences are not clearly understood. One concern is the failure brought by DMI and ERTMS or by ATO. An interviewee suggested that if the technology fails, "the signallers will have to call each driver's phone and the operators will have to do things manually" (P13).

This scenario carries various other risks, such as the driver's may not have a mobile phone signal and/or the signaller's may not have the phone number of the driver.

*4.1.2 European Rail Traffic Management System-related risks.* The interview data indicated that more network connectedness brings new opportunities for attackers and cyber-criminals as both driver assistance and control systems present new attack surfaces. Implementation of the ERTMS, for example, brought considerable benefits, as well as risks through installing "backdoors", according to a cyber-security engineer.

"Should such a backdoor be introduced to the system and if any vulnerabilities exist (in the system), an attacker could take control of the train" (P9).

For example, tampering with ERTMS is possible by implanting a small device with wireless connectivity, which also introduces further risks for both trains and stations.

"(Mounting) an attack is much easier than it was in the past (e.g. anywhere attackers have a data signal and Wi-Fi)" (P1).

*4.1.3 Human-centred cyber-security and organisational risk.* Interviewees suggest that when the railway organisations place new equipment on the railways, the human part of the integration is not always considered, which poses another cyber-security risk. One aspect of this risk is the lack of awareness and action from senior management, as well as organisational factors where managers assume the decisions made by operators are trivial. Humans are at the heart of the resilience in the system, and signallers, in particular, are the "decision makers". Their non-integration into the system or lack of preparedness can be an issue in itself.

"They (industry) often think of that piece of equipment – e.g. workstation. But don't always consider the integration of that equipment –the human part of integration" (P3).

Increased automation also means that signallers do more monitoring than setting routes, which changes the way they work. They also have increasingly complex and evolving responsibilities. This can lead to human-error-related cyber-security issues – such as missing signs of adversity. Signallers' "day-to-day attitude" should change to accommodate these changes.

"Is automation obscuring (the operations)? Signallers should be aware of the digital railways – electronics, network connectivity, Wi-Fi, all that. . . " "They need to be able to say that: 'I have a digital system in front of me now, it can have vulnerabilities'" (P4).

The importance of trust in the system automation and its potential impact on a cyber-attack was also emphasised during the interviews. Signallers may overly trust the system and not challenge the changes when something "odd happens" or "the system behaves in a way it shouldn't", according to another interviewee (P5). Conversely, there could also be operational consequences following a potential cyber-attack if drivers lose trust in the intelligent systems.

"If drivers won't trust the system anymore (following a cyber-attack), they will simply not drive, no trains will be in operation" (P15).

Misuse of information by drivers due to increased automation can potentially be another threat, according to a railway expert and investigator (P3), where the railway staff may cause the issue unintentionally, e.g. a driver inappropriately using an automated function on a train (e.g. automated brakes), potentially leading to cyber-security-related risks.

*4.1.4 Problems distinguishing between a system fault and a genuine cyber-attack.* Often, cyber-attacks mimic system faults, therefore, identification of the issues with automation has the potential not only to identify automation-related HF issues but also cyber threats and vulnerabilities. General IT vulnerability, such as software update failures, can also make the rail systems open to attack. The only way signallers can know that something is wrong is if the change is highlighted on the workstation.

"Regular day, regular workstation, then cyber-attack – would they (signallers) know whether the automation was tampered with? There isn't an indication that would show that" (P15).

Social engineering techniques, such as concealing a cyber-attack as a fault in the system, can be an issue combined with HF issues such as workload and distraction. A particularly busy day can lead to not noticing changes in the system, and these might be inappropriately be labelled as "human error".

"Humans can be the target as well. Not only the system but manipulating human actions until there is a serious error. Say signallers keep moving a dot (location point) due to some false information until (they make) an error" (P18).

*4.1.5 Signallers not prepared for a cyber-attack.* Signallers are not prepared for a cyber-attack because they do not expect one. Nevertheless, the role of the signaller following an infrastructure attack has direct or indirect consequences on their day-to-day activities.

"They (signallers) don't need – another thing (which) might go wrong. Not fixing (the issue) presents another issue" (P17).

Signallers are the last line of defence in the event of an attack. However, as they are unable to distinguish between an attack and a fault in the system, they are also not specifically trained for an attack's aftermath:

"Disruption management is not mature. Cyber-attack will be a form of "disruption". They (signallers) need to be educated so that they can react to it when there is a fault" (P7).

If digital systems fail, signallers need to take manual control, but the steps for mitigation are unclear. One reason is the difference between an attack and some other disruption on the railways:

"The threat is different than any other adversity. Say if there is a bomb, everyone will go to a secure location. With that (cyber-attack) they don't know how to deal with it" (P3).

Overall, ($n = 9$) interviewees suggest that signallers often do not directly cause cyber-related risks, and the risks can originate from adversity or other parties, e.g. maintainers or third-party suppliers during maintenance. Moreover, a signaller's day-to-day duties currently do not account for any cyber-related training, but it is something that appears to be under consideration.

*4.1.6 System faults/maintenance-related risks.* Computerised rail systems are at risk from human error, such as failures to update and configure software correctly. This includes actions as innocuous as attaching unauthorised devices to networks by maintainers. Each action may also expose, or introduce, vulnerabilities allowing third parties to obtain remote access to systems.

"Maintainers have admin rights so they could potentially be the weak link" (P1).

As well as the potential to expose or introduce vulnerabilities allowing malicious actors to obtain access to systems by maintainers, the role of third-party suppliers is also crucial in these scenarios.

"Maintainers (on the other hand) (can) prevent the problem itself. If, say the issue is with the third party (suppliers)" (P1), (P17).

Physical access to safety-critical systems can be an acute problem when it comes to cyber-security and physical manipulation of rail systems, such as databases. With relatively unprotected modern technology, it is possible to "just follow a maintainer" (e.g. tailgating), have access to the equipment and change a character or cause similar damage. For example, in 2017, a driver on the Cambrian Coast line in North Wales reported a fault with the information provided on his in-cab display (DMI). As a result, temporary speed restrictions (TSRs) were not transmitted to several trains under their control. The TSRs were required on the approach to seven level crossings to provide level-crossing users with sufficient warning of approaching trains so that they could cross safely (RAIB, 2017). No attribution was made to a cyber-attack as the cause for the incident in the report or any other physical access to the systems. However, such a scenario would be feasible, especially in the context of how even a fault in the system or cyber-attack can turn into safety concern due to HF.

### *4.2 Mitigation strategies*

*4.2.1 Signallers' role as "safety catalyst" following an adversity.* A common theme during the interviews was a signaller's role when all else fails. They deal with the day-to-day consequences should the whole railway be attacked. One mitigation strategy is approaching adversity as a "fault" in the system and preparing signallers on that basis. As signallers lack a high level of privilege on the systems they use, they are unlikely to directly cause or expect a cyber-security-related breach, but they could potentially observe one due to their (technical) knowledge and experience.

"Signallers are trained individuals with an eye for detail; thus, they can be an asset (to increase railway resilience)" (P5).

According to HF railway experts, signallers are well-trained and capable, so they can "save the day" when "everything else fails". Thus, we need to consider the questions:

*Q6.* What signallers might generate?

*Q7.* What signallers might prevent?

In this case, targeted signaller training to identify these issues can help them mitigate (through reversing the situation or adversity), but only with the right level of access control.

"Signallers could notice things maintainers missed. Maintainers have access (to the systems), but they (signallers) don't". (P1)

*4.2.2 Building on current mitigation strategies.* Another mitigation strategy that builds on existing mitigation strategies entails signallers manually "taking over" during adversity, where they would, in the words of one interviewee, "call the drivers one by one", but with more preparedness for unfamiliar issues. This classic approach of "calling the right people" benefits from learning experiences between generations of signallers:

"Nowadays younger ones (signallers) are more "technologically savvy"; however, they lack the knowledge of "who to call and when". "Older ones (signallers) would have the benefit of more training and knowledge" (P3).

"Signallers would know what they should be doing and when, who to call and when to call" (P12).

### *4.3 Summary of findings*

Interviews with the industry representatives, signallers and academics showed that ever-increasing and evolving automation comes with some adverse effects, including:

- Signallers are covering larger geographical locations, which risks increasing their workload and decision-making.
- Automation, interconnected networked systems and software issues have the potential to bring more sophisticated and evolving cyber-threats and system vulnerabilities.
- Often the issues may not be restricted to one system or piece of equipment but rather they may affect or spread across several networked systems – e.g. the way they work together; including legacy and new systems; as well as human-system interaction.
- It may not be possible to notice an unusual event or one may miss safety-critical information due to an adversity event leading to catastrophic errors for the drivers or other operators (e.g. track workers) in certain scenarios (e.g. TSR setting).
- Physical manipulations of the system (e.g. changing data in a system), unplugging some critical equipment or downloading malicious data (e.g. during maintenance) can cause risks which may directly impact signallers.
- When there is an incident, it is not possible to know whether there is a fault within the system or the risk is an attack to the system that already has a fault in it (e.g. whether there is a technical or functional vulnerability).

Although cyber-security is very much a threat in itself, this study found that a bigger threat may be adverse safety implications (e.g. in a scenario where an underground train stops in the middle of a tunnel), the outcome may be catastrophic due to heat, electrified rails, panic or poor crisis management. Thus, both the unavailability of railway systems as a result of security-related attacks, and environmental risks and management issues can combine to create a very unsafe operating environment.

## 5. Results

Our findings from both the literature review and the interviews, and their interpretation within the socio-technical framework are summarised in Table 3. They outline a framework that enables us to connect previously diverse factors within the digital resilience on the railways to develop mitigation strategies. This approach allowed us to identify key relationships between various factors within the HF and cyber-security areas. Below, we illustrate those relationships and describe how the insights can identify mitigating strategies for the identified risks.

The approach helped us to identify key relationships between various factors within the areas of HF and cyber-security. Our findings showed that there may be several HF, system and organisational attributes related to human error/accidental insider, as well as external cyber-security risks on the railways.

Those attributes are in line with the socio-technical system level described by Wilson (2007). For this study, these attributes include the following:

- Technology/digital and physical devices: new railway systems, e.g. ERTMS.
- Individual characteristics, e.g. personality traits, risky beliefs (e.g. over trust) and behaviour (malicious or non-malicious).
- Operator goals.
- Team and group behaviour, e.g. related to trainings.
- Organisational and management behaviour, e.g. security culture.
- Infrastructure.

| Socio-technical systems | Summary of findings | Socio-technical theory | Potential mitigation strategies |
|---|---|---|---|
| People | Malicious attacks | • Unknown threat actors, often without a clear plan or goal and poor traceability of an attacker, make rail transport a relatively easy target for cyber-attacks<br>• Malicious attackers (e.g. nation state, terrorist and even organised crime) with very clear plans/goals can cause economic disruption or serious harm<br>• Social engineering techniques, such as concealing a cyber-attack as a fault in the system, can be an issue combined with HF issues such as workload and distraction (e.g. a particularly busy day can lead to not noticing changes in the system) | Further HF evaluation, re-design and training opportunities |
| | Human error | • HF-related issues can include human error (e.g. accidentally sharing information)<br>• Heavy cognitive load, stress and workload can cause human error (e.g. mistakes and slips) | |
| | Non-malicious | • Non-malicious risks (e.g. not recognising a fault in the system or becoming an accidental insider/ non-malicious threat actor [e.g. through unintentionally tampering with the system]) due to a number of factors, including training<br>• Cyber-security-related risks can originate from other parties, e.g. maintainers or third-party suppliers during maintenance activities on the railways | |
| Organisational factors/culture | Lack of awareness | • Organisational factors can increase cyber-related risks to the railways due to a lack of security culture and awareness (i.e. lack of systematic review of maintenance activities, training or monitoring) | HF input to organisational strategies around cyber-security, including job design, training and awareness |

(*continued*)

**Table 3.**
Summary of findings within the within the socio-technical framework

| Socio-technical systems | Summary of findings | Socio-technical theory | Potential mitigation strategies |
|---|---|---|---|
| | Lack of "buy-in" from senior management | • Management may not provide sufficient consideration for cyber-security, which may lead to a "relaxed security culture"<br>• The key role of senior management to mitigate against cyber-security risks may not be fulfilled, so mitigation strategies are not fully explored. These may include, e.g. development of safety requirements around security, fit-for-purpose design, goal/task-oriented system design, etc | |
| Technology | New technology-related risks | • Implementation of new technologies such as ERTMS and increased connectivity bring new opportunities for attackers and cyber-criminals as both driver assistance and control systems present new attack surfaces<br>• Computerised rail systems are also at risk from human error, such as failures to update and configure software correctly. This includes actions as innocuous as attaching unauthorised devices to networks (e.g. by the maintainers)<br>• Risks around integration of new systems with legacy systems<br>• Re-design limitations of the legacy systems | HF input to re-design; training opportunities |
| Infrastructure | Infrastructure risks (e.g. physical access threat) | • Physical access is another threat to safety-critical systems, such as railway systems. Modern technologies in rail transport being relatively unprotected can cause this risk<br>• Rail systems may also expose or introduce, vulnerabilities allowing third parties to obtain remote access to systems (maintenance-related risks) | HF input to re-design; training opportunities |
| Goals | Railway operators (e.g. signallers) goal-related risks | • Day to day pressures to complete the jobs on time may lead not noticing cyber-security-related | Training and job design opportunities |

(*continued*)

**Table 3.**

| Socio-technical systems | Summary of findings | Socio-technical theory | Potential mitigation strategies |
|---|---|---|---|
| | | risks (both signallers and maintainers) | |
| Training | Problems distinguishing between a system fault and a genuine cyber-attack not being prepared for an attack | • Cyber-attacks or social-engineering-related manipulation can mimic system faults<br>• Signallers are often not able to distinguish whether an issue within the system is due to a cyber-attack or fault in the system<br>• Signallers are not prepared for a cyber-attack as they are not "expecting one"<br>• As the signallers are not able to distinguish whether an issue within the system is due to a cyber-attack or fault in the system, they are also not specifically trained for the aftermath of a cyber-attack<br>• The role of the signaller following an attack on the infrastructure often has direct or indirect consequences on their day-to-day activities<br>• If digital systems fail, signallers have to take control "manually"; however, the individual steps for mitigation are not clear | Further HF evaluation and training opportunities |

**Table 3.** **Source:** Created by authors

We combined those factors as themes in the next sections to show the interrelations between them. Below, we illustrate those interrelationships and describe how the insights they provide can be used to identify mitigating strategies for the identified risks.

*5.1 Technology – people (malicious attacks) – training issues*

As well as numerous benefits, increasing automation and connectivity carries increased risk. The ever increasing power of new technologies means that, mounting an attack on the fail-safe nature of systems is much easier because all the attackers need is a data signal or Wi-Fi.

Often, the attacks are not on the infrastructure but rather on the new and specific systems, which can be attacked by implanting small devices with wireless connectivity in or near the systems, e.g. DMI, line side systems, passenger information systems and signallers' TMS in control rooms.

For example, in safety-critical tasks such as a line blockage, automation may not be provided due to an attack on the signaller's workstation (e.g. TMS). In such a scenario (e.g. where all screens go blank due to an attack) signallers, cannot know where the trains are.

Our results show that the signallers are ill-prepared for such an attack. In this case, the vulnerability is due to the lack of training of the signallers for such an attack, as they will be unable to use safety-related functionalities (e.g. ARS), and may use incorrect settings due to flawed system integration.

The socio-technical relationship between technology, people (malicious threat) and training is illustrated through a diagram originally introduced by Christina *et al.* (2015); see Figure 2.

*5.2 Technology – people (human error) – goals*

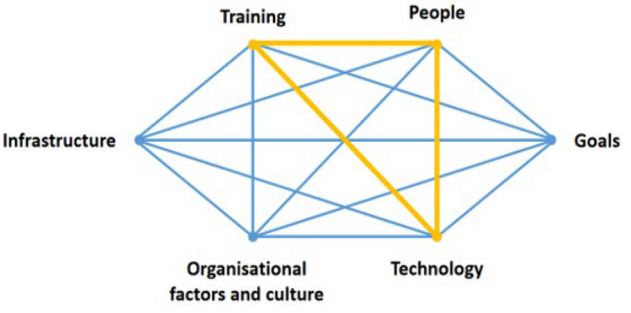
New technology such as ERTMS includes safety critical interlocking systems, where the system provides an increasing role for automation within rail (Sharples *et al.*, 2011). They often have some level of security implemented (a way of mechanically stopping trains) should the ERTMS system malfunction due to intentional or unintentional circumstances. Safety engineers currently address security issues by implementing various controls for hazards through this system. However, there is still a risk that signalling-related errors could disturb railway services significantly – directly or indirectly.

Another reason for human error could be due to social engineering (Hadlington, 2017), which could increase signaller workload, hence cause confusion, mistakes or lapses. This may challenge signallers' situational awareness, which, in turn, impacts their safety-critical decision-making. These issues, combined with the equipment not indicating whether there is an issue with the system (e.g. through an indication), leads to problems distinguishing between system faults attacks, thereby interfering with signallers "day-to-day" activities and goals. The socio-technical relationship between technology, people (human error) and operator goals is illustrated in Figure 3.

*5.3 Organisational factors and culture – infrastructure – training*

Cyber-related risks can originate from other parties, e.g. maintainers or third-party suppliers during maintenance activities. This could include malicious physical access due to unprotected infrastructure. The issues can be extensions of organisational factors such as a lack of a security culture and awareness or a lack of systematic review of maintenance activities. Signallers' lack of training can also lead to these issues going unnoticed, as reported in some past incidents.

Issues related to skills, motivations and awareness could lead to cyber-threats, not only due to maintenance errors but also due to potential physical attack (e.g. through tailgating). One of the crucial factors for such a malicious or non-malicious threat is the access rights certain parties may have (e.g. third-party suppliers).




**Source:** Created by authors

**Figure 2.** Socio-technical relationship between technology – people (malicious threat) – training issues

One common theme appearing from the discussions and publications is the key role of senior management "buy in" to security to mitigate against a "relaxed" security culture. Making cyber-security a priority by keeping platforms up to date, for example, with the latest software, while promoting awareness for the importance of security in their organisations, could eventually help the identification of and reaction to emerging threats and vulnerabilities.

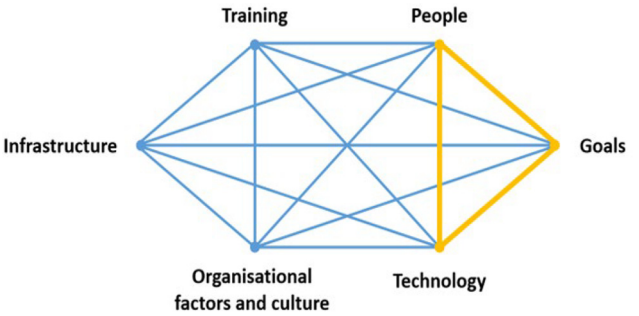
The socio-technical relationship between organisational factors and culture, infrastructure and training are shown in Figure 4.

## 6. Conclusion

In this study, we considered HF and cyber-security issues on the railways, particularly around rail signallers, providing an opportunity to explore the relationships between socio-technical factors of interest to security and HF practitioners. This led to an exploration of issues arising from security awareness, training or education, particularly where multiple goals and different access privileges are present.

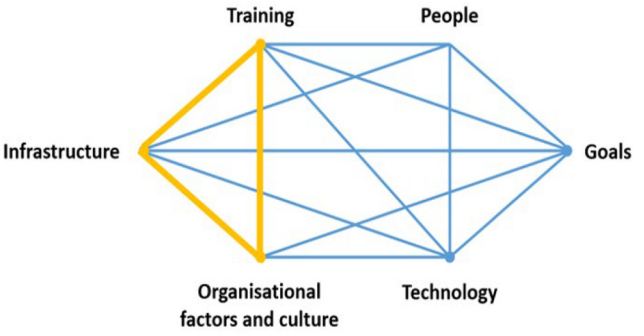
This study showed the socio-technical relationship between:

- technology-people-training;
- technology-people-goals; and
- organisational factors and culture-infrastructure-training on the railways are particularly prominent within railway CPS applications and human actors.




**Source:** Created by authors

**Figure 3.**
Socio-technical relationship between technology – people (human error) – goals




**Source:** Created by authors

**Figure 4.**
Socio-technical relationship between organisational factors and culture – infrastructure – training

In particular, our work highlighted the inter-relationships which exist between individual autonomy, goal-setting and key socio-technical variances.

Our study found that in terms of cyber-security risks and consequences of a cyber breach, railway CPSs and the role of signallers have similar challenges to other critical infrastructure and their operators. Nevertheless, the findings around signallers' day-to-day tasks and challenges make this area worth investigating further.

The main reason for this conclusion is that the study found that signallers are at the heart of the railways, and they are the "decision makers". In other words, even though signallers do not have to manage cyber-security incidents or be security experts, they still need to deal with the consequences of adversity; hence, they often find themselves as the last line of defence in responding to or dealing with issues in the system. New technology brings the need for security to fit around the already complex and demanding work that signallers do, and cyber-security attacks could interfere with safety critical functions that signallers use as part of their day-to-day activities. Our study also showed that cyber-related issues may be due to various other factors, including other roles such as third-party suppliers.

Identifying specific cyber-security-related vulnerabilities and threats on the railways is problematic as most vulnerabilities and threats are simply "unknown" at this stage. These unknown "unknowns" can be a significant factor in operator performance and decision-making. Therefore, new methods are needed to evaluate those to be better informed about how signallers' and other operators' evolving day-to-day roles, tasks and goals may be impacted by potential adversities on the software-based technology they increasingly use and develop mitigating strategies.

Potential for opportunities for signallers as part of mitigating strategies can include the following:

- Signallers are trained individuals with an eye for detail; thus, they can be an asset to increase railway resilience.
- Signallers often do not directly cause cyber-related risks, but the risks can originate from other parties, e.g. threat actors, maintainers or third-party suppliers during maintenance activities.
- There are cases where signallers found a fault within a system by chance due to their technical knowledge and experience, as discussed with one of the industry interviewees.

Therefore, targeted training of signallers to notice cyber-related risks can help them mitigate through reversing the situation with the right tools and authorisation by looking into two areas within digital resilience:

(1) Resilience to risks signallers might generate; and

(2) Risks signallers might be able to prevent.

### *6.1 Future work*

There needs to be further studies to better understand the potential risks and various mitigations that can be developed to train and support operational staff for all critical infrastructure and their CPSs. These can include opportunities for tailored HF evaluation of (new and legacy) systems to understand operator-related cyber-security risks, which will provide a sound basis for clear strategies and performance goals, and well-structured, consistent and responsive interventions (e.g. through identification of re-design opportunities, training needs or organisational issues). Based on previous cyber incidents and our study, it would be useful to collate and test some scenarios to try to identify gaps in the security systems currently in place (e.g. usability and operability of the systems in the context of cyber-security).

The study can also be repeated for other operators on the railways, in particular to understand the impact of increasing automation on "safety critical communications" and "decision making" of railway staff (e.g. train drivers and line-side maintainers). Issues may range from not achieving complete "integration" of new and legacy systems; systems and humans; or issues such as over-trust on automation; skill fade; issues with monitoring, and so on. Cyber-security threats around system maintenance activities and third-party suppliers are other challenges found in this study, which is another area worth exploring in future studies.

Tailored HF methods focused on usability and training needs analysis (TNA) can be introduced to mitigate against cyber-security issues on the railways. This could help to identify the predictive training needs of the signallers, rather than waiting to learn from a cyber-attack retrospectively, and a systematic approach which considers both safety and security factors.

A TNA can help to prepare the signallers when they are the last line of defence to manage crises on the railways. Specifically, it may inform on more onerous checking – e.g. for mismatches in sets of information. It could identify better communication as a solution – e.g. checking the speed with the driver or notify the signallers/drivers of the issues in some way. A targeted cyber-security training analysis together with tailored usability evaluation could help the signallers to:

- understand vulnerabilities and threats;
- perform meaningful checks that still allow them to complete their tasks in an efficient manner;
- identify discrepancies/unusual changes in the system; and
- be part of the response and keeping the railway safe if a cyber-attack was suspected; in other words, "be prepared" and support crisis management proactively.

Potentially, a visual modelling approach could be used for a detailed analysis, e.g. through systems-theoretic accident model and processes/systems-theoretic process analysis (Friedberg *et al.*, 2017; Young and Leveson, 2014). Such a study could lead to improved system design or signaller training that might have prevented past incidents, e.g. the ERTMS Cambrian line incident (RAIB, 2017).

## References

Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S. and Salonitis, K. (2023), "Predicting cybersecurity threats in critical infrastructure for industry 4.0: a proactive approach based on attacker motivations", *Sensors*, Vol. 23 No. 9, p. 4539.

Altaf, A., Faily, S., Dogan, H., Mylonas, A. and Thron, E. (2019), "Identifying safety and human factors issues in rail using IRIS and CAIRIS".

Antoni, M. (2018), *Overview of UIC Cybersecurity Activities*, Presentation, International Union of Railways.

Baker, G. (2008), "Schoolboy hacks into city's tram system", *The Telegraph*, Vol. 11, p. 2008.

Bastow, M.D. (2014), "Cyber security of the railway signalling and control system", *9th IET International Conference on System Safety and Cyber security*, IET, pp. 1-5.

BBC (2018), available at: www.bbc.co.uk/news/technology-43725640 (accessed July 2023).

BBC (2023), available at: www.bbc.co.uk/news/uk-northern-ireland-66445452 (accessed July 2023).

Biernacki, P. and Waldorf, D. (1981), "Snowball sampling: problems and techniques of chain referral sampling", *Sociological Methods and Research*, Vol. 10 No. 2, pp. 141-163.

Brooks, J., McCluskey, S., Turley, E. and King, N. (2015), "The utility of template analysis in qualitative psychology research", *Qualitative Research in Psychology*, Vol. 12 No. 2, pp. 202-222.

Caire, J. (2017), "Human factors in cybersecurity for transportation systems", *WIT Transactions on the Built Environment*, Vol. 176, pp. 405-414.

CBC News (2020), available at: www.cbc.ca/news/canada/british-columbia/translink-debit-creditpayment-down-1.5826868 (accessed November 2021).

Chen, B., Schmittner, C., Ma, Z., Temple, W.G., Dong, X., Jones, D.L. and Sanders, W.H. (2014), "Security analysis of urban railway systems: the need for a cyber-physical perspective", *International Conference on Computer Safety, Reliability, and Security*, Springer, *Cham*, pp. 277-290.

Christina, S., Waterson, P., Dainty, A. and Daniels, K. (2015), "A socio-technical approach to improving retail energy efficiency behaviours", *Applied Ergonomics*, Vol. 47, pp. 324-335.

CYRail (2018), "CYRail recommendations on cybersecurity of rail signalling and communications systems", Horizon 2020, European Union Funding for Research and Innovation.

Digital Railway (2018), "Digital railway strategy", available at: https://cdn.networkrail.co.uk/wp-content/uploads/2018/05/Digital-Railway-Strategy.pdf (accessed February 2021).

Euronews (2022), available at: www.euronews.com/next/2022/11/03/denmark-cybersecurity (accessed March 2023).

Evans, M., Maglaras, L.A., He, Y. and Janicke, H. (2016), "Human behaviour as an aspect of cybersecurity assurance", *Security and Communication Networks*, Vol. 9 No. 17, pp. 4667-4679.

Fachot, M. (2018), "Protecting railway networks from cyber threats", International Electrotechnical Commission, available at: https://iecetech.org/index.php/Technology-Focus/2018-02/Protectingrailway-networks-from-cyber-threats (accessed January 2023).

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D. and Sezer, S. (2017), "STPA-SafeSec: safety and security analysis for cyber-physical systems", *Journal of Information Security and Applications*, Vol. 34, pp. 183-196.

Gabriel, A., Brauner, F., Lotter, A., Fiedrich, F. and Mudimu, O.A. (2018), "Cyber security flaws and deficiencies in the European rail traffic management system towards cyber-attacks", *Proceeding of the 15th ISCRAM Conference*.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S. and Baker, T. (2018), "Security threats to critical infrastructure: the human factor", *The Journal of Supercomputing*, Vol. 74 No. 10, pp. 4986-5002.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. (2018), "Correlating human traits and cyber-security behavior intentions", *Computers and Security*, Vol. 73, pp. 345-358.

Guardian (2022), available at: www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup (accessed July 2023).

Guest, G., Bunce, A. and Johnson, L. (2006), "How many interviews are enough? An experiment with data saturation and variability", *Field Methods*, Vol. 18 No. 1, pp. 59-82.

Guest, G., MacQueen, K.M. and Namey, E.E. (2011), *Applied Thematic Analysis*, sage publications.

Hadlington, L. (2017), "Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours", *Heliyon*, Vol. 3 No. 7, p. e00346.

Hadlington, L. (2018), "The 'human factor' in cybersecurity: exploring the accidental insider", *Psychological and Behavioral Examinations in Cyber Security*, IGI Global, pp. 46-63.

IRJ (2022), available at: www.railjournal.com/infrastructure/italian-railway-itsystem-suffers-major-cyber-attack/ (accessed June 2023).

Jeong, J., Mihelcic, J., Oliver, G. and Rudolph, C. (2019), "Towards an improved understanding of human factors in cybersecurity", *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, IEEE, pp. 338-345.

Ki-Aries, D. and Faily, S. (2017), "Persona-centred information security awareness", *Computers & Security*, Vol. 70, pp. 663-674.

Kour, R., Aljumaili, M., Karim, R. and Tretten, P. (2019), "eMaintenance in railways: issues and challenges in cybersecurity", *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, Vol. 233 No. 10, pp. 1012-1022.

Kvale, S. and Brinkmann, S. (2009), *Interviews: Learning the Craft of Qualitative Research Interviewing*, Sage.

Leveson, N. (2020), "Are you sure your software will not kill anyone?", *Communications of the ACM*, Vol. 63 No. 2, pp. 25-28, available at: https://cacm.acm.org/magazines/2020/2/242342-are-yousure-your-software-will-not-kill-anyone/abstract (accessed March 2023).

Maglaras, L.A., Kim, K.H., Janicke, H., Ferrag, M.A., Rallis, S., Fragkou, P., Maglaras, A. and Cruz, T.J. (2018), "Cyber security of critical infrastructures", *ICT Express*, Vol. 4 No. 1, pp. 42-45.

Malatji, M., Von Solms, S. and Marnewick, A. (2019), "Socio-technical systems cybersecurity framework", *Information and Computer Security*, Vol. 27 No. 2, pp. 233-272.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. and Giannakopoulos, G. (2014), "The human factor of information security: unintentional damage perspective", *Procedia – Social and Behavioral Sciences*, Vol. 147, pp. 424-428.

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. and Guerri, D. (2022), "Leveraging human factors in cybersecurity: an integrated methodological approach", *Cognition, Technology and Work*, Vol. 24 No. 2, pp. 371-390.

RAIB (2017), "Report 17/2019: loss of safety critical signalling data on the Cambrian coast line", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/920663/R172019_191219_Cambrian_Coast_line.pdf (accessed March 2023).

RailEngineer (2021), available at: www.railengineer.co.uk/railway-signals-in-middlesbrough-now-controlled-from-york-after-successful-reliability-upgrade/

RailTech (2017), available at: www.railtech.com/digitalisation/2017/12/11/wannacry-virus-was-wake-up-call-for-railway-industry/?gdpr=accept (accessed June 2023).

Reuters (2022), available at: www.reuters.com/world/europe/russian-attacks-rail-system-fail-paralyze-lifeline-ukraine-2022-05-08/ (accessed August 2023).

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M.A., Amir, A., Vuda, K.V. and Sarwat, A.I. (2023), "Impact, vulnerabilities, and mitigation strategies for Cyber-Secure critical infrastructure", *Sensors*, Vol. 23 No. 8, p. 4060.

Sharples, S., Millen, L., Golightly, D. and Balfe, N. (2011), "The impact of automation in rail signalling operations", *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, Vol. 225 No. 2, pp. 179-191.

Sky (2016), available at: https://news.sky.com/story/four-cyber-attacks-on-ukrailways-in-a-year-10498558 (accessed June 2023).

Statista (2023), available at: www.statista.com/topics/9918/cyber-crime-and-thefinancial-industry-in-the-united-states/#topicOverview (accessed July 2023).

Thaduri, A., Aljumaili, M., Kour, R. and Karim, R. (2019), "Cybersecurity for eMaintenance in railway infrastructure: risks and consequences", *International Journal of System Assurance Engineering and Management*, Vol. 10 No. 2, pp. 149-159.

The Local (2017), available at: www.thelocal.se/20171011/trains-delayed-after-it-glitch-hits-rail-services (accessed December 2023).

Tyagi, A.K. and Sreenath, N. (2021), "Cyber physical systems: analyses, challenges and possible solutions", *Internet of Things and Cyber-Physical Systems*, Vol. 1, pp. 22-33.

Widdowson, A.J. (2016), "CHEAT: an updated approach for incorporating human factors in cyber security assessments", *Engineering and Technology Reference*.

Wikipedia (2017), available at: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (accessed June 2023).

Wilson, J.R. (Ed.) (2007), *People and Rail Systems: Human Factors at the Heart of the Railway*, Ashgate Publishing.

Wilson, J.R., Farrington-Darby, T., Cox, G., Bye, R. and Hockey, G.R.J. (2007), "The railway as a socio-technical system: human factors at the heart of successful rail engineering", *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, Vol. 221 No. 1, pp. 101-115.

Wright, A. and Jun, G.T. (2019), "Human and organisational factors in cybersecurity: applying STAMP to explore vulnerabilities".

Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A. and Malli, M. (2020), "Cyber-physical systems security: limitations, issues and future trends", *Microprocessors and Microsystems*, Vol. 77, p. 103201.

Young, W. and Leveson, N.G. (2014), "An integrated approach to safety and security based on systems theory", *Communications of the ACM*, Vol. 57 No. 2, pp. 31-35. Accessed in January 2020.

## Further reading

Clegg, C.W., Robinson, M.A., Davis, M.C., Bolton, L.E., Pieniazek, R.L. and McKay, A. (2017), "Applying organizational psychology as a design science: a method for predicting malfunctions in socio-technical systems (PreMiSTS)", *Design Science*, Vol. 3.

Gapanovich, V., Rozenberg, E. and Gordeychik, S. (2016), "Signalling cyber security: the need for a mission-centric approach", *International Railway Journal*, Vol. 56 No. 7.

## About the authors

Eylem Thron is a Principal Human Factors Consultant at Mima with over 15 years' experience in the application of human factors and design expertise within safety-critical industries. She is a Chartered Ergonomist and Human Factors Specialist currently leading a number of major projects in the rail industry. She holds an MSc in Human Factors and Ergonomics from Loughborough University, a BEng in Computer Systems Engineering and a Doctorate in Engineering from the University of Kent. She is also interested in Cyber-security/Digital Resilience issues in the rail sector and contributed to various research projects and publications in that area. Eylem Thron is the corresponding author and can be contacted at: eylem.thron@mimagroup.com

Shamal Faily is a Principal Scientist at Dstl, and a Visiting Fellow at Bournemouth University with over 25 years of experience in software and security engineering research and practice across multiple domains. He holds a DPhil in Computer Science and PGCert in Software Engineering from the University of Oxford, PGCert in Education Practice from Bournemouth University, and a BSc in Business Computing Systems from City, University of London.

Martin Freer is Head of Human Factors at Mima with over 35 years' of applied consulting experience across a wide range of sectors, including road, rail and air transport, defence, process control, chemical and pharmaceuticals and command and control systems and interfaces. He holds a BSc in Ergonomics from Loughborough University, with Diploma in Professional Studies, and is a member of the Chartered Institute of Ergonomics and Human Factors. He has spent much of the past 20 years working in railway related projects concerning railway signalling and control systems, rail vehicles and stations.

Huseyin Dogan is an Associate Professor and the Director of the Computing and Informatics Research Centre at Bournemouth University (BU). Prior to BU, he worked as a Research Associate at Loughborough University. He has eight years industrial experience working as a Higher Scientist for BAE Systems Advanced Technology Centre. Dr Dogan received his Engineering Doctorate (EngD) in Systems Engineering from Loughborough University, MSc in HCI with Ergonomics from University College London and BSc in Computer Science from Queen Mary University of London.