mima

Human Factors - Operators as the last line of defence

Dr. Eylem Thron

Design that connects us

Dr. Eylem Thron

Principal Human Factors Consultant at Mima

Experience

15 years experience in Rail, Aerospace, Defence industries as Human Factors (HF) Consultant / HF Manager / Human-Computer Interface (HCI) Designer / HF Integration Lead / Notified Body Lead Assessor / Accessibility Consultant / User Interface Designer / Visiting Fellow in various organisations

PhD, MSc, Beng, C.ErgHF

We are a human-centred design agency

We design services, experiences, products and spaces making them accessible to all.

Why is user-focused / human-centred thinking important?
We understand that people do not always behave as we expect.
They are not necessarily rational. They find their own path.

What are you going to learn in this talk?

- Cybersecurity risk in the railways
- Railways as a socio-technical system
- The Human element – threat actors, passengers, maintainers and operators
- What are Human & Organisational Factors (HOF)
- The role of HF discipline in prevention, reduction and mitigation against cybersecurity incidents
- Operators as the last line of defence and the role of HF discipline for safe and efficient operations

mima

Cybersecurity risk on the Railways

- There have been numerous cyber-attacks on the railways
- Affects legacy systems, new systems, Wi-fi on the trains, passenger information systems, movement of points under trams, compass ticketing kiosks, signalling, dispatching and other operational systems
- More connectivity and a trend towards more digitization has its benefits but presents **new attack surfaces**
- A security threat can either afford a **new hazard**, or increase the magnitude of a **consequence of a pre-existing one**

Cybersecurity risk on the Railways
Causes

The Rail network is a likely target for future cyber attacks, due to:

- Its extensiveness and complexity
- High value target – politically, financially and from a media exposure point of view
- Constant innovation and increased motivation by organised crime groups, hacktivists, and nation states
- Human error and non-malicious intent, e.g. due to increased digitisation / social engineering and human vulnerabilities (over 80%)

Question

Scenario

Due to cyber attack a train/metro stops in a tunnel...

1. How do you think the people involved might react?
2. Can you think of how those reactions that might effect safety?

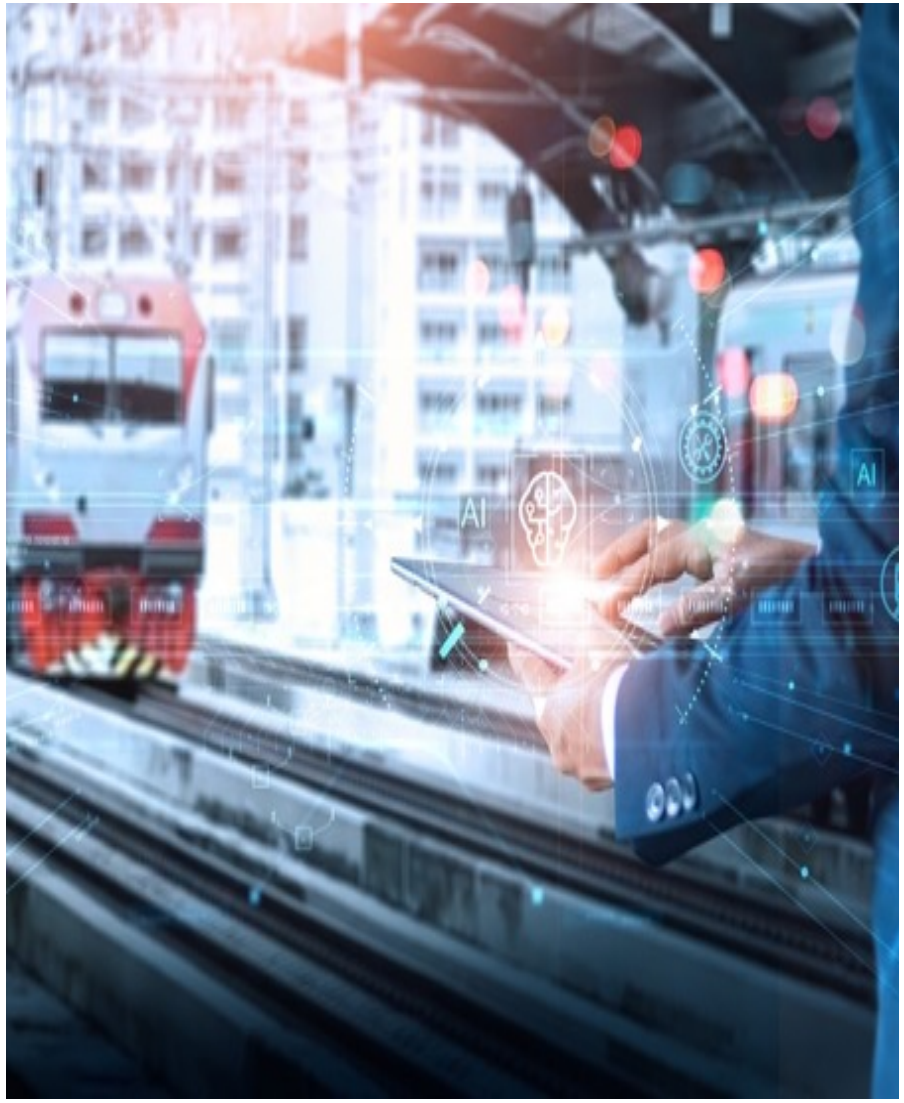
Cybersecurity risk on the Railways
Consequences

- **Passengers**: Fear, confusion, anxiety, frustration, panic, injuries, lose patience and attempt to find their own way out of trains
- **Operators**: Increase in workload, operators have to manage secondary hazards in addition to their existing role
- **Railway staff**: Now dealing with a safety hazard as they attempt to manage the situation and safely return passengers to stations without full system functionality

Human actions are the vehicle by which security risks become safety hazards

HF provides data and evidence based on real people

- HF provides **data and evidence based on real people** and we are experts in understanding **human behaviour**
- So, while system developers and operators often prioritize technical solutions such as passwords, firewalls, and adherence to security standards, we look at factors such as **usability issues, time pressures, organizational ambiguity, inadequate training, and lack of risk awareness**
- These contribute to **human error and pose significant challenges** cyber-security efforts



mima

What is human factors and what can it do to help?

Design that connects us

Human Factors

Human Factors (HF) is a profession and a discipline. We work in multiple industries.

Looks into user **capabilities, limitations, motivations, training - human variability** and their tasks and operational goals and that way aims to prevent incidents

We look at railways as a **socio-technical system**

HF views Railways as a socio-technical system

Thron, E., Faily, S., Dogan, H. and Freer, M., 2024. Human factors and cyber-security risks on the railway–the critical role played by signalling operations. *Information & Computer Security*, *32*(2), pp.236-263.

HF views the railway as a socio-technical system and looks at it with a human-centred lens

Drivers
Using interfaces such as ETCS, CBTC

Passengers
Using interfaces such as CIS, PIS, mobile phones

Maintainers
Using interfaces such as laptops (e.g. system maintainers)

Signallers
Using interfaces in the control room

Threat actors
Using various devices, interfaces

Question

What aspects of cybersecurity do you think Human Factors might be related or contribute to?

Cognitive

Organisational Factors

SOCIETAL AND CULTURAL PRESSURES

LEGAL AND REGULATORY RULES

ORGANISATIONAL AND MANAGEMENT BEHAVIOUR

training

TEAM AND GROUP BEHAVIOUR

INDIVIDUAL BEHAVIOUR
Motivation

INDIVIDUAL DIFFERENCES

PHYSICAL DEVICE
e.g. new railway systems

Personality traits

demographics

judgement

memory

vigilance

Risky beliefs

Attention to detail

skils

knowledge

planning

Employee engagement

monitoring

Shift and work pattern

Goal setting

Communication coordination cooperation

Safety culture

Company policy

Security awareness

Decision making

Perception of responsibility

Security culture

Operational framework

Political pressures

Security legislation

Industry framework and common strategy

reputation

Constraints on system design

Economic pressures

Physical

Environmental

Adapted from Wilson, J.R & Sharples, S. (2015) Method In the Understanding of Human Factors

mima

How HF / HOF can help operators as the last line of defence?

Design that connects us

Cybersecurity risk on the Railways

- **A new way of working** for all operators – from drivers to process operators – changing skilling of the workforce
- Increased automation and less manual checks lead to skill fade and **reduced situational awareness**
- **"Overtrust"** of the system rather than personal experience / knowledge
- **Day to day pressures** to complete jobs on time may lead to not noticing cyber-security related issues
- Where **decisions are time sensitive** and **workload is high**, the risk of human error escalates, especially in **degraded or emergency modes**

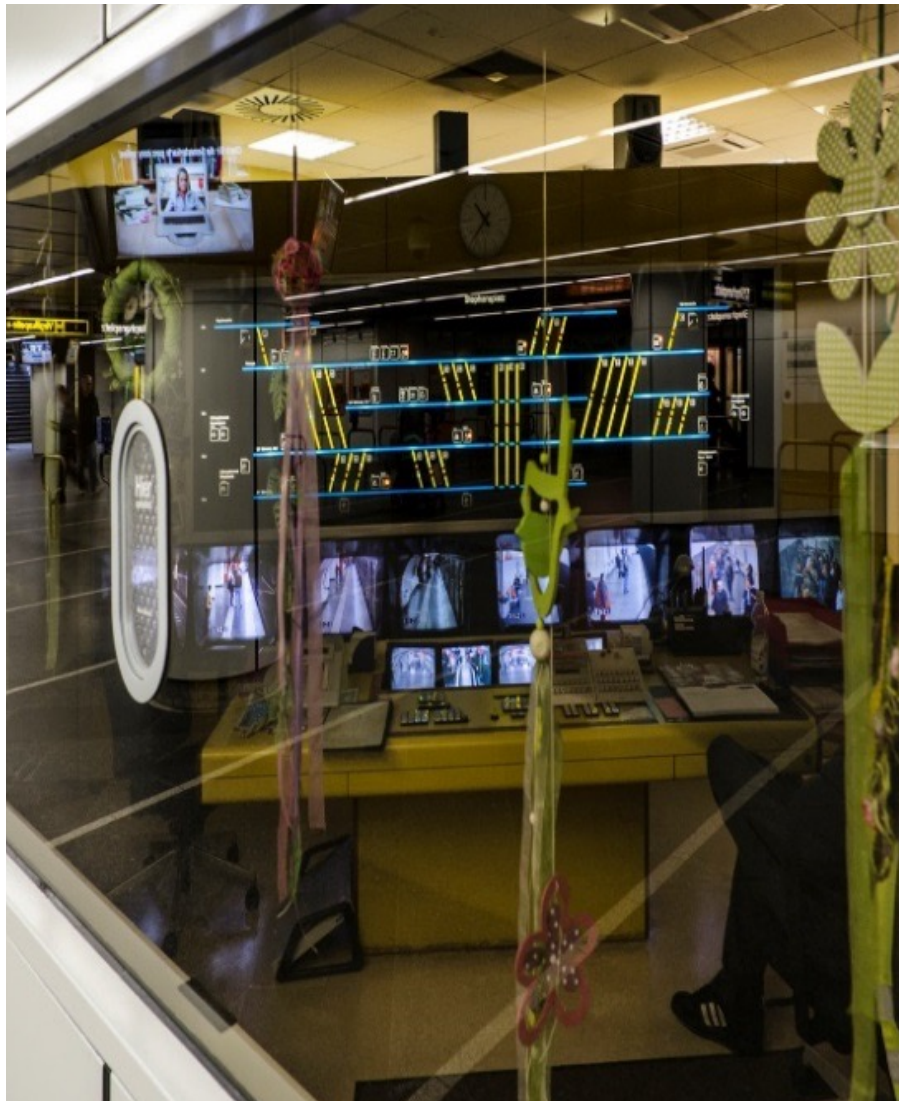
Thron, E., Faily, S., Dogan, H. and Freer, M., 2024. Human factors and cyber-security risks on the railway–the critical role played by signalling operations. *Information & Computer Security*, *32*(2), pp.236-263.

Operator risk post-incidents
Crisis Management

- During **emergency scenarios** (e.g., train stop at a tunnel due to a fault in the system) - HF can help to identify safety hazards as a result of **human factors**
- Unknown risks mean changing role of the station staff (e.g. an attack/system failure may mean panic and **over-crowding of stations due to system failures, secondary risks e.g. stampede)** - HF can support crisis management
- Lack of opportunity for passengers to **contact staff / emergency services** during adversity - HF input to re-education
- **Anxiety, reduced morale, loss of confidence, confusion, lack of information**

Design and process - Operators

- We look at human interaction (e.g. through task analysis), we use scenarios to test operators tasks) - **Job design**
- Increased **workload** may mean **limitation of cognitive reactions** and **more mistakes -Interface design**
- We look at the **processes** and evaluate **e.g. whether the front-line staff have the right privileges**
- **Engineers often design for process/scenario**. We understand the human interaction with the interface and consider intuitiveness, behaviour, cognition, expectation of the users, their operational goals, hence advocate for **expectation-led design**

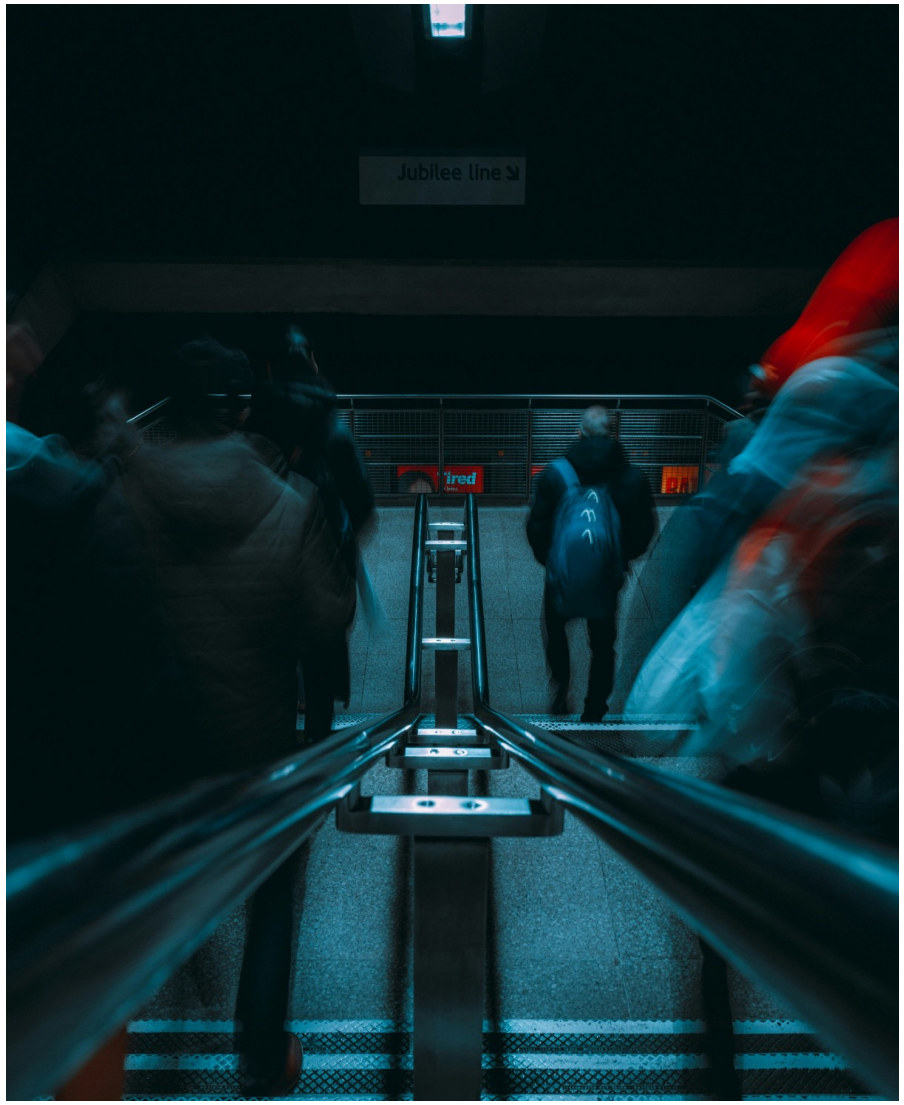


Design

HF input to identify possible thinking of threat actors

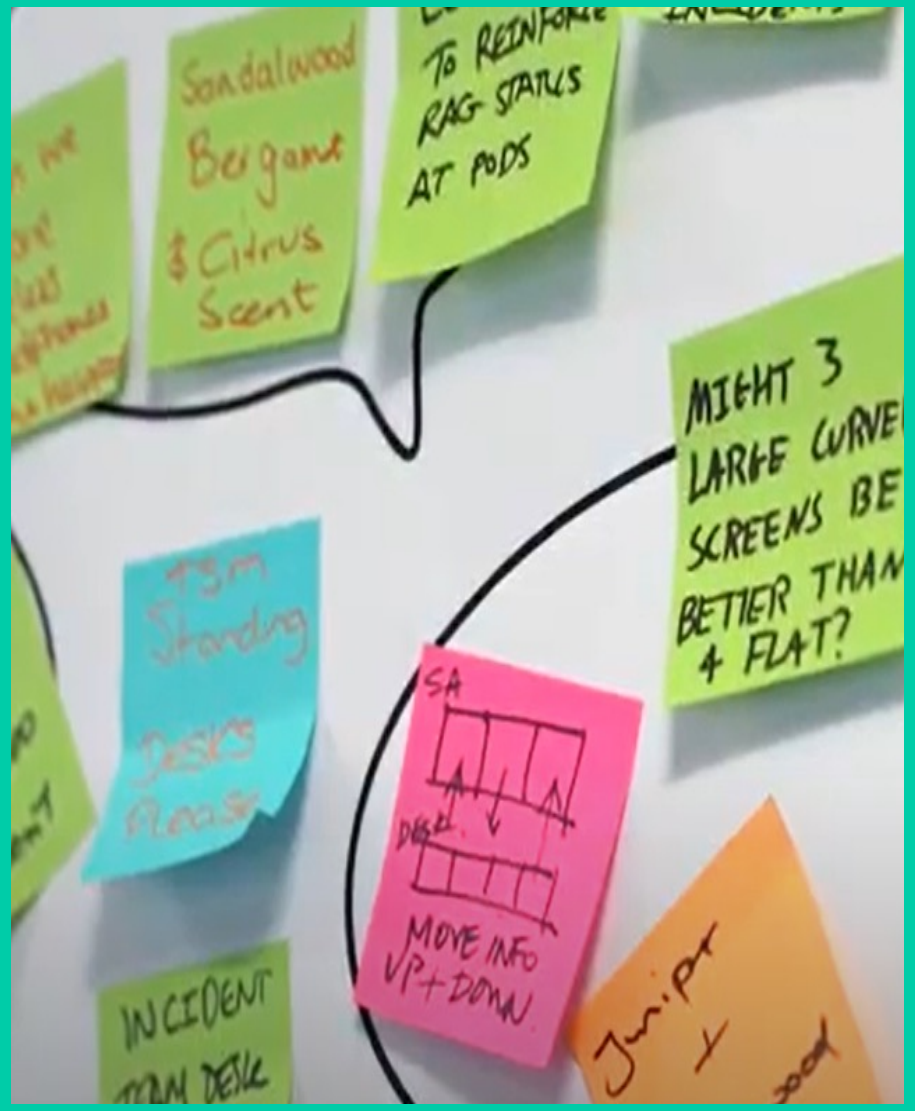
- Human Factors can help to identify possible thinking of threat actors, e.g. through personas - evaluation of skills and characteristics

- We can provide input about an attacker’s motivation, attitudes, attributes, skill set (e.g. through persona development) and help to identify potential risks through visual modelling approach



Cultural change / Education / job design

- Railways are evolving and becoming more connected (new systems / technology, AI, etc)., which will make them vulnerable in ways that it has not been before - **this will require a cultural change and re-education of staff**
- We talk to users - HF tools & techniques support cultural and organisational change, new ways of working
- HF thinking supports gradual education about the changing railways - as one socio-technical system
- Organisational factors must be part of the solution



Targeted Training

- Help Operators to **identify** a risk (cyber-attack or risks operators / process might generate)
- Help Operators to be able to **prevent the situation escalating**
- Help Operators to **mitigate through reversing the situation**

Subsequently **improve operator (e.g. signaller) reactions**, which in turn could prevent adverse events

- Operators (e.g. signallers) are trained individuals with an eye for detail; thus, **they can be an asset to increase railway resilience when all fails**
- Mitigate through reversing the situation with the right tools and authorisation by looking into two areas within digital resilience:
  - Resilience to risks operators **might generate**
  - Risks operators **might be able to prevent**

Final Notes

- Railways are **socio-technical systems** where each group independently interacts with various systems in different and unexpected ways, and they will continue to do so with **increased digitisation** on the railways
- Operators often do not directly cause cyber-related risks but find themselves as the **last line of defence**
- The role of HF has been overlooked to date in cybersecurity, nevertheless and yet HF methods provide **data and evidence based on real people**. So, engineers need to consider the human element in their design
- HF promotes a better understanding of safety and security risk and can help to mitigate against accidental and malicious threats - we can help to **detect, predict, quantify, prevent, reduce** and mitigate against vulnerabilities through well-established tools and techniques
- We can do this through **input to system requirements, design of systems, cultural change, re-education and targeted training**
- We can learn from other industries

Thank you!

Dr. Eylem Thron
Eylem.thron@mimagroup.com

Design that connects us