Creating a world
fit for the future

RICARDO

# Evaluating the Impact of Cyber Security with Human Factors in Rail Using Attacker Personas

**Dr. Eylem Thron**
Senior Consultant
23 October 2019

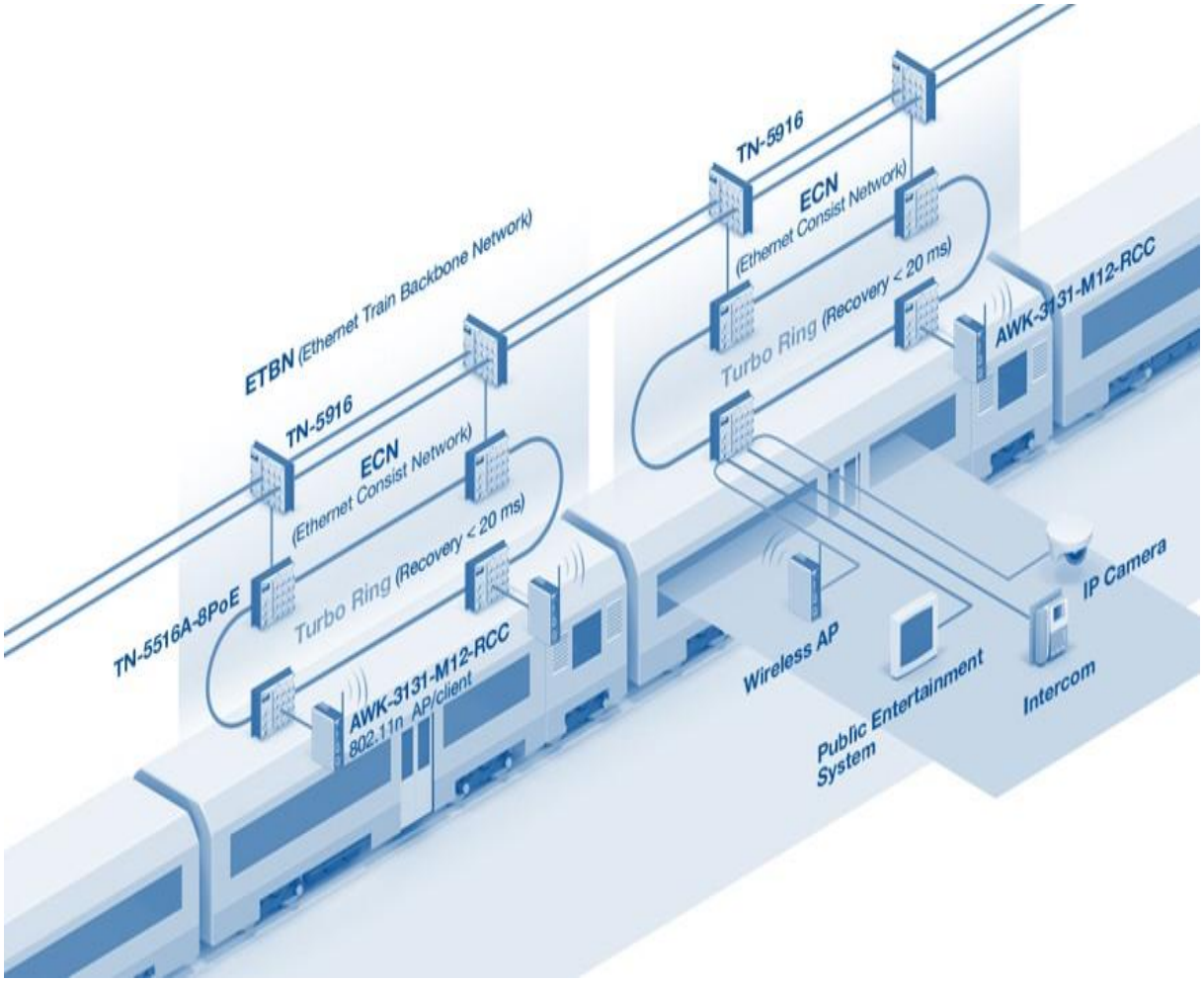


rail.ricardo.com

# Introduction

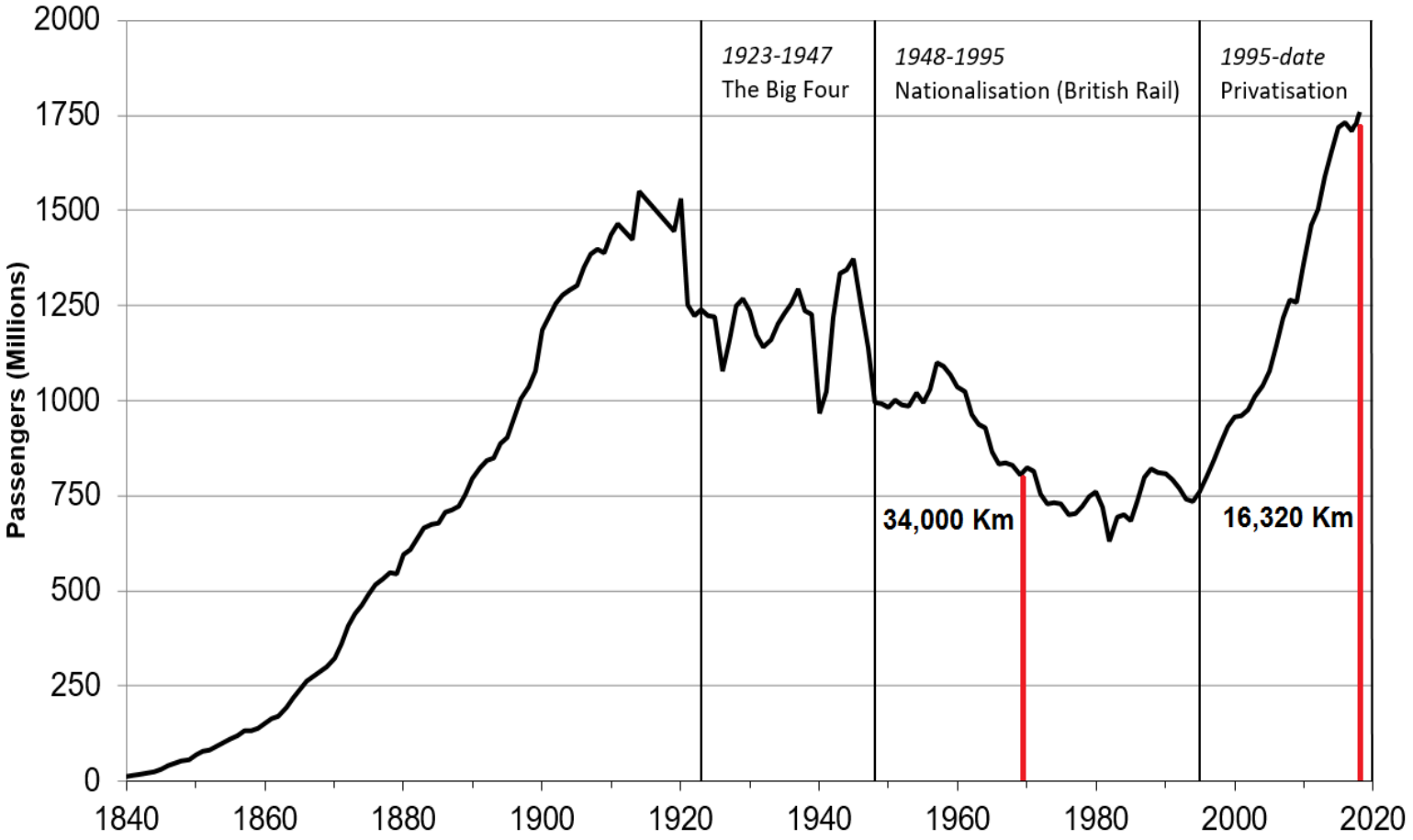
- Human Factors
- Security Engineering

- How changes in technology changes the nature of risk
- Why we need to include Human Factors in Security Engineering
- How these two relate to each-others



# Why Human Factors matter in Cyber Security?

Our railways carry more people than before…



# Why Human Factors matter in Cyber Security?

This means we need better technology to carry these people…

# New Technology, New Risks…

This technology introduces new ways in which humans interact with machines across a rail system

But it also opens new risks that can be exploited… routinely and maliciously

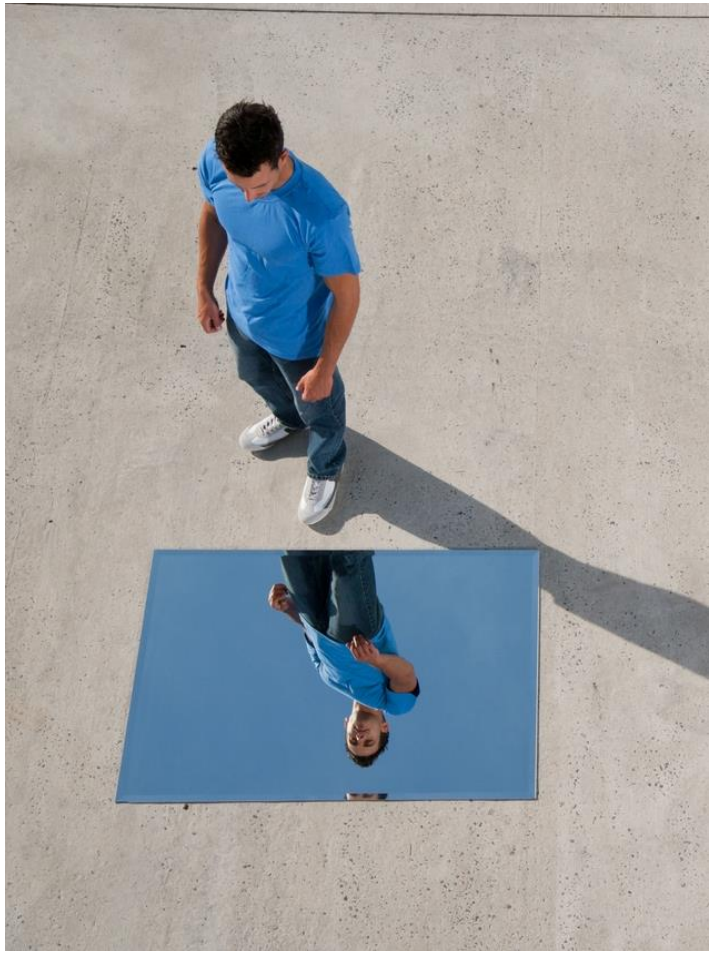
# Human Factors in Cyber Security

- Moving away from the concept of ‘human is the weakest link’
- Moving beyond security ‘fear’
- In human factors we make decisions based on data and evidence
- We should do this for security too

# Human Factors view

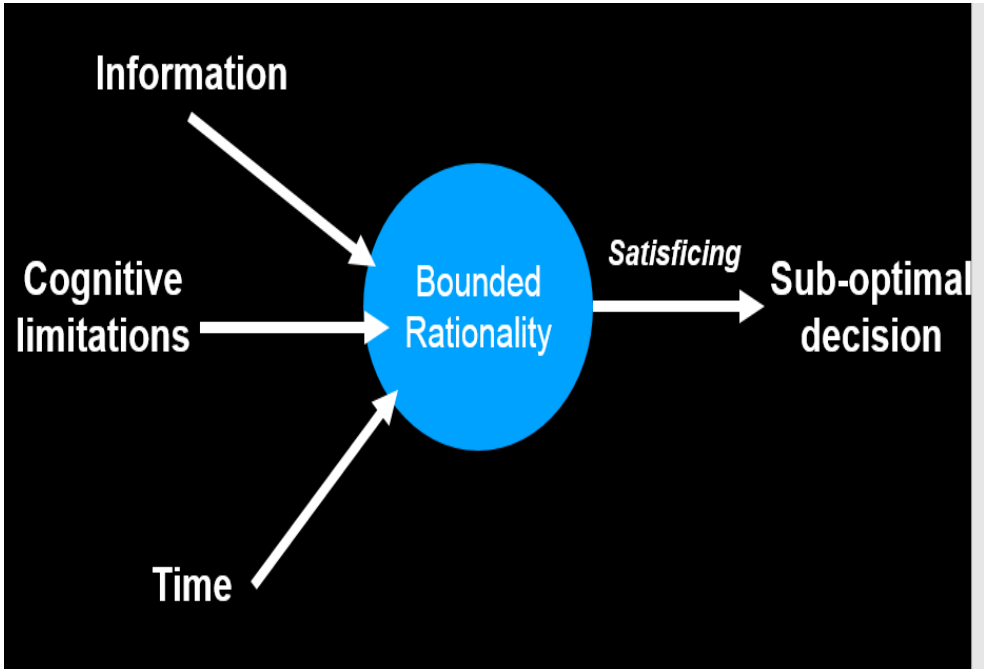
We need to look at human factors in a different way…

- A signaller's view of the system is not the same as an attacker's view
- A human factors engineer's view of the system is not the same as a security engineer's view



# Why we need modelling tools?

- Too much information but the information that exists is still incomplete
- People have limited cognitive ability to process this information
- Even if they did, they wouldn't have much time to process and make a decision.
- People fall back on assumptions because they "*don't know what else to do…*"




## Bounded rationality

*"Decision making limited by the rationality of individuals, the information available, and time"*

- Relying on stereotypes of people and things

# Personas and attacker-centric perspective

- CAIRIS (Computer Aided Integration of Requirements and Information Security) is an open-source modelling tool
- By creating an attacker persona in CAIRIS, we can **rapidly** model intersecting **safety, security, human factors** and **usability** issues affecting the systems at a very **early** stage
- Personas give an idea about the **possible thinking**
- Providing security engineers a better chance to **identify risks**

# Personas

CAIRIS Home System Requirements Risk UX Models Options Search Search Logout

Home / Personas / Adam

Summary | Activities | Attitudes | Aptitudes | Motivations | Skills | Contextual Trust | Intrinsic Trust

Adam is a careless boy who is often found roaming around tram stations and not much concerned about trespassing or breaking any rules. He testified for breaking into the tram network and switching junctions. He is a boy who is just curious and lacks the money to fulfill his curiosity, hence learnt the coding for building infrared remote control from internet. His non-serious behavior as a teenager was responsible for triggering the chaos.
There were problems with Lodz's Network Signaling System reported by the workers. But railway authorities disinterest in improving security provided this loop-hole. Adam was able to exploit this vulnerability by getting into the Lodz Tram Network and derail trams.

+ Environment

− Morning Shift

Roles | Narrative

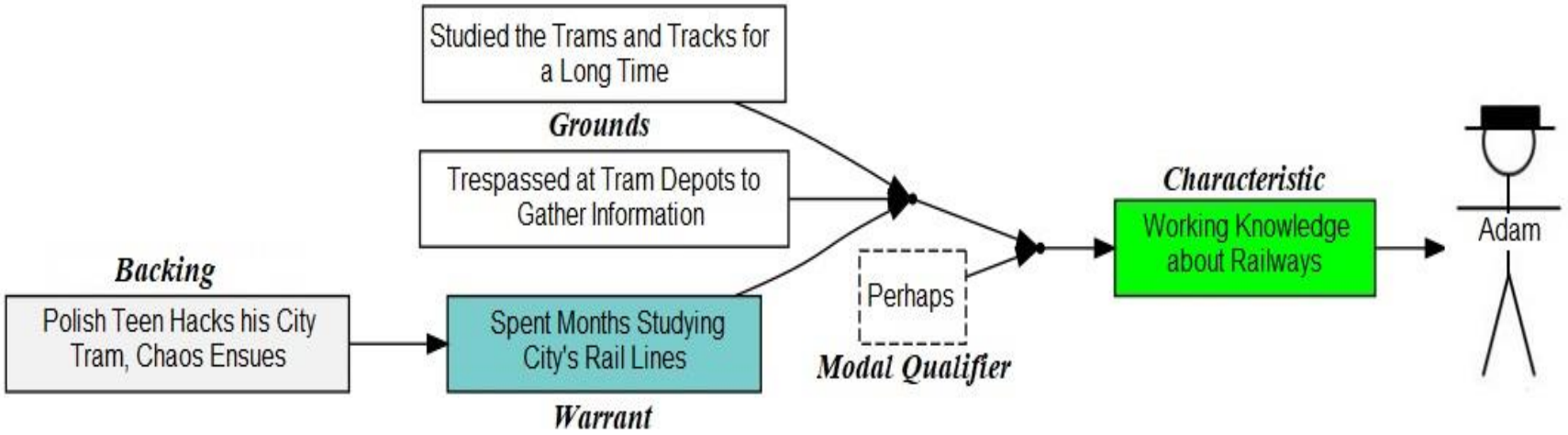
Direct User

| + | Role |
|---|---|
| − | Attacker |

# Example of the Model: Polish Tram Case Study

Visualisation of:

- How several factors influence the malicious behaviour of threat actors
- How the system vulnerabilities are exposed
- How vulnerabilities are used by attackers
- How threats associated with risks cause security breaches



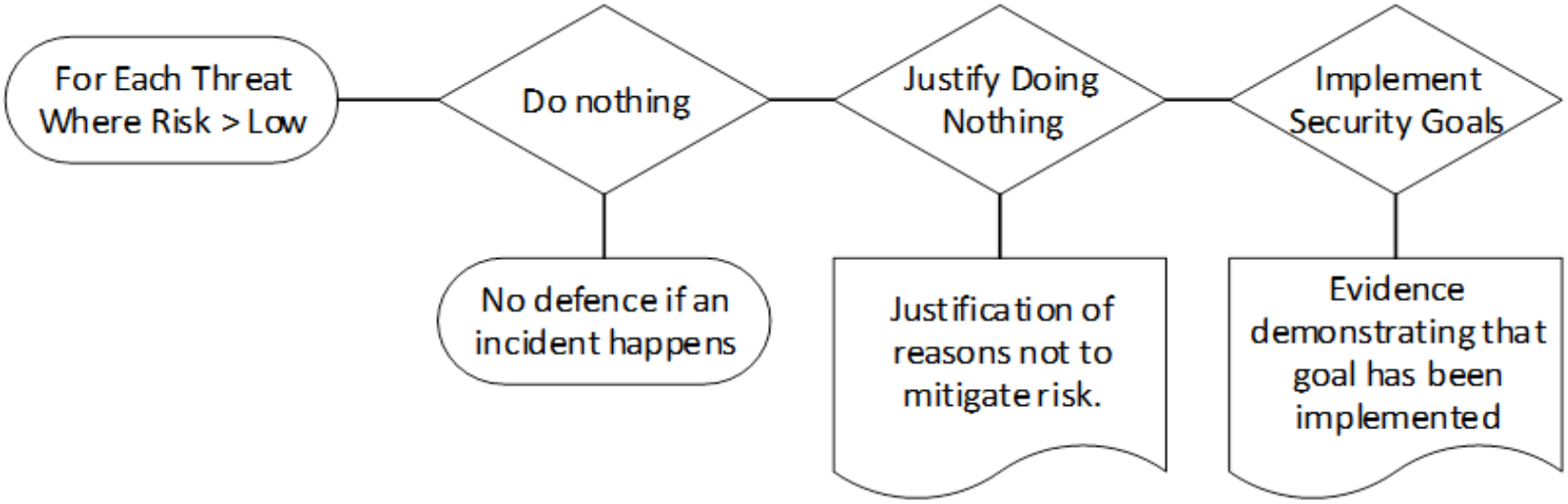
# Lessons learned so far…

- Security engineers identified certain threats/ risks; human factors perspective found other risks which hadn't been viewed/ considered by the security engineers
- Human factors provided input into safety (i.e. do people take more risks?)
- Human factors provided further security goals

We learned to do security assessments differently…

# Future work

- Further embedding this approach into our working practices
- Better communicating the human factors related risk
- Integration of existing Human Factors assessments
- Include human factors in all security and safety assessments



Ricardo Rail is collaborating with Bournemouth University on a PhD research project in Safety, Security and Human Factors in railways.

This approach is being applied to a customer's systems with the open source **CAIRIS** platform.

CAIRIS: https://cairis.org

Dr. Eylem Thron
eylem.thron@ricardo.com
https://ricardo.com/