Automation and Cyber Security Risks on the Railways - the Human Factors implications

Eylem Thron[1] & Shamal Faily[2]

[1]MIMA Group, United Kingdom, [2]Robert Gordon University, United Kingdom

SUMMARY

Automation improves rail passenger experience but may reduce cyber resilience because it fails to adequately account for human factors. Preliminary results from a study on signallers and automation confirms this, but judicious use of modelling tools may ensure design for automation considers this.

KEYWORDS

Cyber Security, Human Factors, Railway, Modelling tools

The Human Factor implications of automation in Rail

Modern railway systems improve passenger experience as data resulting from automation can be shared quickly to keep passengers informed, improve reliability as systems and devices constantly monitor their status, and reduce disruption due to improved checks and maintenance and lower operating costs. Automatic train operation has introduced increasing automation within rail signalling (Balfe et al., 2011). This automation incorporates some measure of resilience should the signalling system malfunction due to intentional or unintentional circumstances, e.g. a way of mechanically stopping trains. There is also a wide belief that automation – such as automatic route setting – significantly reduces the contribution of human error to train accidents. However, as well as numerous benefits, increasing automation and connectivity carries increased security and safety risks that can be realised both in terms of human error, and malicious and non-malicious behaviour.

The rail network is a likely target for future cyber attacks given its criticality, complexity, constant innovation by different threat actors, and the potential for human error and non-malicious intent (Gratian et al., 2018). A security threat can either afford a new hazard or increase the magnitude of a consequence of a pre-existing one; for example, attacking an emergency response during a major rail accident could lead to increased fatalities. Yet, despite active research in rail safety and cyber security, the role HF approaches could play in simultaneously addressing both has been overlooked. Because Human Factors (HF) methods provides data and evidence based on real people, they promote a better understanding of safety and security risk, and provide engineering support to mitigate accidental incidents or malicious threats.

Human Factors are typically not incorporated into most security assessments. This is due to incomplete or complex data regarding humans and their interaction with railway systems, and the time and expertise required to process the data. Moreover, qualitative HF methods often do not give the ‘bigger’ picture of the incidents, nor help to identify ‘unknown’ threats that may be causal factors of cyber incidents. This is problematic as not only are most vulnerabilities and threats ‘unknown’ at this stage, but they can also be a significant factor in operator performance and decision making. Therefore, assessors need new methods to better understand how railway operators’ evolving day-to-day role, tasks and goals may be impacted by potential adversities.

The informed use of user and system modelling to make sense of contributions from various stakeholders, e.g. users, safety, and security experts, could address this problem. Human error intersects cyber security and safety (Altaf et al., 2019); humans could violate rules leading to hazards if non-malicious (unintentional) but can also exploit vulnerabilities that compromise system security if malicious (intentional). Hence a combined effort could aid to identify security related vulnerabilities as well as mitigating strategies. Previous work demonstrated how the integrated modelling of safety, security and HF issues can uncover inter-dependencies between security, safety and HF engineering techniques (Altaf et al., 2019). Visualising and evaluating the data and evidence related to human-system interaction subsequently grounds security goals and better informs security design decisions (Altaf et al., 2019; 2021).

Learning from the interactions between signallers and automation

Few studies exist on the increased risk of automation to both cyber-related threats and human error and how these can impact operator's (e.g. 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. Signallers undertake safety-critical work, and the increasing automation in their day-to-day systems makes cyber security a concern. Cyber attacks often mimic system faults, therefore issues with automation have the potential not only to identify security-related vulnerabilities, but also to explore mitigating strategies for HF related issues (e.g. training gaps). Thus, through investigation of the humans' (e.g. signallers) role, activities and decision-making process for potential cyber security incidents on the railways, unsafe actions can be understood better and in a holistic view, rather than focusing on only 'human failure' or 'technology failure'.

We undertook a study to better understand the interaction between signallers and automation; this considered technology, organisational factors, culture, cognition, complexity and legacy systems. We also considered whether rapid digitisation of railways around the world exposed passengers and operators to new security risks from a 'sociotechnical' point of view (rather than focusing on human tasks and performance alone). We conducted 21 semi-structured interviews with signallers and related stakeholders, where questions considered the HF and cyber security related risks on the railways, the strategies for mitigation from the interviewee perspective, and the role of the signallers and other railway workers during a cyber attack.

Our results identified issues with increasing automation such as direct or indirect consequences of cyber-related threats. In particular, we noted that human factor actions are the vehicle by which security risks become safety hazards. The results also highlighted the socio-technical relationship between (i) people- training- technology; (ii) technology-people-goals; (iii) training-people-organisation. Organisational practices, and operator goals and training needs for automation are also needed, together with clear strategies and simple performance goals to train and support operational staff.

As part of future work, we will conduct a more structured and informative analysis to model and visualise safety, security and human factors data using the Computer Aided Integration of Requirements and Information Security (CAIRIS) security and usability modelling tool[1]. Our tool-support approach will identify differences between a qualitative HF assessment and modelling tools in terms of time to analyse data, completeness, visualisation, details of risk assessment and clarity of conclusions through a multi-disciplinary viewpoint. It will be able to do so proactively, which may not be possible with traditional HF methods often due to incomplete, missing or 'unknown' data.

[1] https://cairis.org

References

Balfe, N., Lowe, E., Hillier, G. and Nock, P., 2011. Applying human factors in the design of future rail systems. Human Centred Automation, pp.239-250.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A., 2018. Correlating human traits and cyber security behavior intentions. Computers & security, 73, pp.345-358.

Altaf, A., Faily, S., Dogan, H., Mylonas, A. and Thron, E., 2019. Identifying Safety and Human Factors Issues in Rail using IRIS and CAIRIS.

Altaf, A., Faily, S., Dogan, H., Mylonas, A. and Thron, E., 2021. Use-Case Informed Task Analysis for Secure and Usable Design Solutions in Rail. In International Conference on Critical Information Infrastructures Security (pp. 168-185). Springer.