11th WCRR 2016
World Congress on Railway Research
29th May – 2nd June
Milan - Italy

SCEPTICS: A Systematic Evaluation Process for Threats to Industrial Control Systems

Rhianne Evans[1], John Easton[1]*, Clive Roberts[1].

[1] Birmingham Centre for Railway Research and Education, School of Engineering, University of Birmingham, Birmingham B15 2TT, UK.

* Corresponding author: j.m.easton@bham.ac.uk

Abstract

The rapid pace of development in Information and Communications Technology (ICT) over the last 30 years has changed the way the rail industry operates. Commercial pressures and the need to share operational information between stakeholders to facilitate cross-border services etc. have gradually pushed the industry away from more expensive, bespoke systems and towards Commercial Off The Shelf (COTS) solutions. Nowhere is this more evident than in the area of industrial control, where examples of the move to standard technologies include the European Train Control System (ETCS) in the signalling domain, and the provision of remote condition monitoring via Supervisory Control And Data Acquisition (SCADA) networks.

Although the move away from bespoke systems has allowed the industry to become more agile, reduce the risks of vendor lock-in, and deliver "more for less" in terms of underlying investment, it also risks increasing the attractiveness of the railways to cyber attackers; much of the off-the-shelf hardware is IP based, and therefore subject to many of the same attack mechanisms as any other modern ICT system. Furthermore, common platforms share common vulnerabilities, meaning exploits that have been realised in one industrial sector, such as the Stuxnet worm used to damage Iran's nuclear centrifuges in 2010, could in theory now be used to attack PLCs used on the railways in the same way.

While the rail industry in the UK and worldwide recognises that there will be an increased risk of cyber attack in coming years, many railway undertakings are unsure of how to begin building an understanding of the extent of the problem they face, or the steps required to address it. Traditional threat analysis techniques used in cyber security research frequently require large amounts of detailed information on specific systems to be gathered before they can be applied, and cyber security specialists speak a different language to rail industry ICT professionals making it difficult to prioritise available resources.

This paper presents outcomes from the SCEPTICS project, an EPSRC funded initiative that is developing a set of common processes that can be applied by ICT professionals within the rail industry to scope their own industrial control systems, allowing them to get a broad understanding of the potential risks of cyber attack, and delivering sets of priority areas / systems to investigate using more detailed threat analysis tools and approaches.

1. Introduction

An Industrial Control System (ICS) is defined by the US National Institute of Standards and Technology as "…a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures" (NIST, 2011). Put simply, an ICS is a set of sensors, actuators and control software that monitor and operate real-world infrastructure, such as a power station, a

production line, or a transport network. Because of their potential to impact on the physical world ICS pose unique challenges from the perspective of cyber security, and as a result the methods needed to defend them against attacks are less well understood than in conventional ICT systems. The motivations behind cyber attacks on ICS are also complex; the presence of real-world infrastructure in the system means that in many cases a physical attack can be a more straightforward method of causing disruption to service, but the impacts of such an attack are also easier to identify and recover from. Cyber attacks by comparison require specialist knowledge to implement, but can lie dormant for long periods before being triggered, and it can be much harder to guarantee a successful resolution / removal / "clean up" after an attack.

Although it can be hard to gather specific technical details on the nature of successful cyber attacks against ICS, often due to commercial sensitivities or the need to protect similar systems from the same attack vector, the existence of such attacks is well documented as is the potential extent of the damage that can result. In 2012 the Shamoon malware virus infected the business systems of the Saudi Aramco oil company. Although the attack did not directly target critical oil production ICS, it wiped 33,000 – 55,000 workstations at the organisation. It is believed that the attack had indirect consequences on oil production and severe financial repercussions (Mackenzie, 2012). An analysis of the virus found that the creators were skilled, but amateurs and that the system had been infected by a disgruntled insider through a USB key (Tarakanov, 2012). There is a need for the rail industry to be better prepared for attacks on business systems as well as safety-critical ICS. In December of 2011, a railway company in the US Pacific Northwest was attacked over a period of two days, suffering disruption to its signalling system, resulting in a 15-minute delay to service. Perhaps most disturbingly, a post-incident analysis suggested that far from being a targeted attack aimed at halting services on the transport network, the delay was in fact the result of a random incident (Zetter, 2012). In 2014 it was reported that a steel mill in Germany had suffered "massive" damage when a cyber attack prevented a blast furnace from shutting down correctly (Zetter, 2015). The attackers had gained access to industrial control systems through a spear-phishing attack on the business network. They had subsequently been able explore the company's networks and access systems controlling industrial processes. The attack highlights the danger of presuming that business networks and industrial control systems are not connected, or that an "air gap" exists between them (Byres, 2012).

The Cyber Security Challenge Facing the Rail Industry

The railways are a classic example of a large scale ICS. Comprising both cyber (ICT, communications networks, and control software) and physical (sensors and actuators) system components, which are geographically dispersed over a wide area, the railways are a technologically diverse environment with a complex set of systems interfaces. As a well-established legacy system, where in the past security was primarily guaranteed by private networks that were physically isolated from outside world by "air gaps", the Internet age means the railway industry is faced with the daunting challenge of identifying potential areas of cyber security vulnerability, and prioritising those areas where mitigating action should take place given the resources available.

In common with the operators of many other long established ICS, there is a recognition from stakeholder organisations within the railways that cyber security is a major challenge to the industry going forwards, however many do not know where to begin quantifying and addressing the risk. The history of the UK rail industry has led to a particularly challenging ICT landscape, with the 2011 report into the value for money offered by the UK rail industry reporting that around 1,700 separate information systems were in use by the industry at that time (DfT, 2011). Despite the technical and commercial challenges, over the last five years the industry has been making significant steps in delivering a focussed vision for cyber security.

In 2012, the Rail Safety and Standards Board published a cross-industry technical strategy for UK rail. As a high-level document, the Rail Technical Strategy (RTS) is understandably light on technical details,

however it does recommend that "…all information systems must be resilient to cyber attacks…" and that "…system security should be maintained and continually checked and tested…" (RSSB, 2012). The following year, Network Rail's own Technical Strategy (NRTS, 2013) referred directly to the need for investment in cyber security, placing an indicative figure of between £1 million and £10 million on developing secure information resources and telecoms over Control Period 5 (2014 – 2019). More recently, at the Institute of Risk Management's 2014 Cyber Risk Summit in London, Network Rail's Professional Head of Cyber Security stated that "[Currently] it is far too difficult to carry out a cyber attack which would have a significant impact on the running of the railway, but we recognise that won't always be the case. The physical threat will remain, but cyber security will be a major issue in the next three to five years" (Finnegan, 2014).

It is clear based on statements of this type that the rail industry is both aware of the risks posed to their ICS by cyber attacks, and keen to take steps to mitigate those risks; however, there is a lack of formal processes outlining the appropriate next steps. Should investment be focussed on newer, but unproven, connected technologies that are secure by design, or protecting legacy systems which were never intended to be connected to the internet? What is the most significant business risk of a successful attack – reputational damage to the industry, the loss of sensitive data, or potentially even loss of life? Where might be the best financial investment for securing systems?

Traditional cyber threat analysis techniques typically require the provision of large amounts of information on the target systems to be gathered by cyber security professionals before detailed evaluations of the domain can take place. However, determining which information about the domain needs to be captured is a complex task and this is particularly true in the case of ICS, where factors including the presence of custom built, legacy hardware mean systems are far more difficult to characterise than the more traditional back-office ICT systems now commonplace in organisations worldwide. Adding to this problem is the differing, and often conflicting, use of language between the ICS domain experts (e.g. railway professionals) and the cyber security experts. The combination of these factors mean that requiring cyber security experts to perform the initial assessment of all the ICT systems in a domain of interest can be an inefficient and resource hungry task.

The SCEPTICS project, part of the UK Engineering and Physical Sciences Research Council (EPSRC) funded Research Institute for Trustworthy Industrial Control Systems (RITICS), aims to address this problem by providing a set of standard processes and tools that can be applied by industry ICT staff to identify and prioritise areas of their infrastructure at risk from cyber attack; this list can then be used by cyber security experts to perform more targeted, detailed assessments of the critical systems. The processes are being developed in conjunction with stakeholders in the UK rail industry, but are designed to be applicable in any industrial control context. Rail was selected as the main focus for the work due to a range of factors, including the complexity of the existing infrastructure, the low level of maturity in this area relative to other infrastructure systems (e.g. oil and gas), and the current high level of interest from stakeholders.

2. A Process for Early Assessment of Cyber Risks

This section presents an overview of the SCEPTICS process, which has been designed to support organisations working within the UK rail industry to make an early assessment of their systems for potential cyber vulnerabilities. It is aimed at developing a broad understanding of risk areas before an organisation invests in more detailed cyber analysis. The process is based on the philosophy that cyber security efforts in the context of ICS should not be restricted to known critical systems of interest (e.g. ETCS), but that cyber threats should be considered as part of the broader context of an organisation.

The proposed process is made up of three distinct phases, named: Identify, Describe, and Assess. Although shown in this document at a very high level, the complete process each phase is presented as

a set of UML activity diagrams, alongside appropriate guidance on methods of information capture and the structuring of outputs.

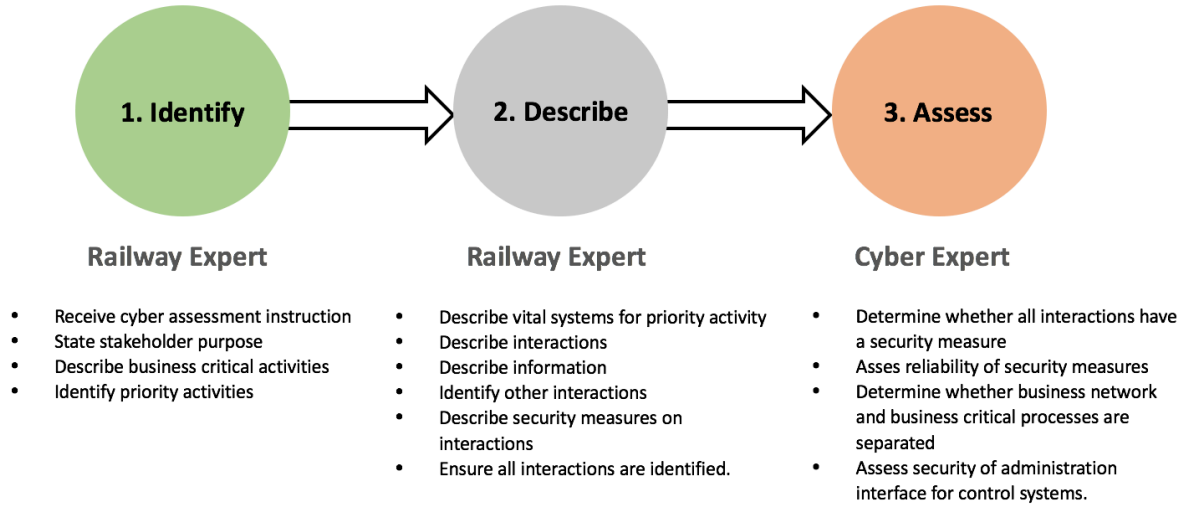

Figure 1: High level overview of the SCEPTICS process.

Stage 1: Identify

The first stage of the process is used to identify which business processes, and therefore which systems, are critical to an organisation's purpose / function. Through the performance of this exercise, it is expected that a stakeholder will identify components of its business network that are more critical to security than originally believed. This phase can be carried out without the need for a cyber security specialist.

Example: Railway maintenance company M depends heavily on the safety and reliability of its maintenance equipment, but also on knowing and correctly applying the maintenance regimes of different stakeholders. The maintenance regime information is stored on the business network and is used to manage rotas, equipment distribution, invoicing, and to record the condition of all of the stakeholder's safety-critical systems.

If the business network were to be hacked, data on the condition of safety-critical systems may become corrupted, leading to inadequate or inappropriate maintenance being carried out. The longer-term consequences of this breach would be likely to include financial and reputational damage.

Stage one of the SCEPTICS process includes the following activities:

- Receive an instruction to assess or investigate cyber security threats to a particular organisation;
- State the purpose of the stakeholder wishing to carry out a cyber security assessment;
- Describe business critical activities;
- Identify priority activities.

Stage 2: Describe

In the second stage of the process, the identified priority activities are described in a way which is understood by both railway specialists and cyber security experts. This phase can also be carried out without the need for a Cyber Security specialist.

Stage two of the SCEPTICS process includes the following activities:

- Describe the systems that are needed to carry out the activity. These might include physical systems, people, IT systems, or anything which converts information during the process;
- Describe interactions (used to transfer/convert information during the process);
- Describe information (transferred during the process. E.g. train number or time);
- Identify other interactions (very important for understanding potential routes to business critical systems. For example: Although it is not part of the NR track access process, the employee leave request process depends on information in the track access database);
- Describe security measures on interactions (e.g. the train number might be encrypted or a firewall may be in place);
- Ensure all interactions are identified.

Stage 3: Assess

The third and final stage of the process focusses on the initial threat assessment the systems, interactions and information which were captured in stages 1 and 2 of the process. Cyber security specialists may be engaged at this stage in order to ensure an effective handover to more in-depth system-specific evaluations.

This phase includes the following activities:

- Determine whether all interactions have a security measure (e.g. encryption, firewalls etc.);
- Asses the reliability of the security measures (engage with cyber security specialists);
- Determine whether the business network is separated from the business critical process;
- Assess the security of the administration interface for control systems (e.g. can users access the USB drive? Do they use it to charge mobile phones? Do they access their emails on the interface? Can the situation be made more secure?).

3. Conclusion

The risks posed to ICS from cyber attacks are very real, and although to date the number of attacks known to have resulted in physical damage to infrastructure is comparably small, reputational damage, financial penalties (for example as a result of delays to service), and loss of sensitive data are all serious concerns. ICS owners are, generally speaking, becoming aware of the risks posed by cyber attacks to their infrastructure, however many are unsure as to how to secure their complex webs of sensors, actuators, and software against such threats.

The necessity to capture significant amounts of domain-specific knowledge before a high-level cyber threat assessment of an ICS is unavoidable, however it is less certain that this work must be performed by cyber security experts. Instead, the SCEPTICS project team believe it is quite feasible for domain experts, who already possess much of the knowledge of the physical and ICT systems needed, to perform these early-stage assessments themselves, producing prioritised lists of key systems based on the core business functions of the organisations involved.

The SCEPTICS project is producing early stage cyber risk assessment processes for ICS. These have initially been developed in collaboration with railway industry stakeholders in the UK, and the team are currently investigating routes for engagement with other railways in Europe and further afield. Moving forward, the SCEPTICS processes will be validated and refined with stakeholders in other similar industrial domains (initially in the context of the power distribution), ensuring that they are as complete and widely applicable as possible within the ICS context.

Acknowledgements

The SCEPTICS project is part of the Research Institute for Trustworthy Industrial Control Systems led by Imperial College London. SCEPTICS is funded by the EPSRC under grant EP/M002845/1.

References

Byres, E. (2012). "Unicorns and Air Gaps – Do They Really Exist? Living with Reality in Critical Infrastructures". Available online from http://pastconferences.auscert.org.au/conf2012/Eric%20Byres.pdf, last accessed 31st January 2016.

Department for Transport (2011). "Realising the Potential of GB Rail: Final Independent Report of the Rail Value for Money Study. Detailed Report". Available online from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/4204/realising-the-potential-of-gb-rail.pdf, last accessed 31st January 2016.

Finnegan, M. (2014). "Network Rail: Cyber security will be 'major issue' as business goes digital". Available online from http://www.computerworlduk.com/news/data/network-rail-cyber-security-will-be-major-issue-as-business-goes-digital-3524405/, last accessed 31st January 2016.

Mackenzie, H. (2012). "Shamoon Malware and SCADA Security – What are the Impacts?". Available online from www.tofinosecurity.com/blog/shamoon-malware-and-scada-security-%E2%80%93-what-are-impacts, last accessed 31st January 2016.

National Institute of Standards and Technology (2011). "Guide to Industrial Control Systems (ICS) Security". NIST Special Publication 800-82, June 2011. Available online from http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, last accessed 31st January 2016.

Network Rail Limited (2013). "Technical Strategy: A Future Driven by Innovation". Available online from http://www.networkrail.co.uk/publications/technical-strategy.pdf, last accessed 31st January 2016.

Rail Safety and Standards Board (2012). "The Railway Technical Strategy 2012". Available online from http://www.rssb.co.uk/Library/Future%20Railway/innovation-in-rail-rail-technical-strategy-2012.pdf, last accessed 31st January 2016.

Tarakanov, D. (2012). "Shamoon the Wiper: Further Details (Part II)". Available online from www.securelist.com/en/blog/208193834/Shamoon_The_Wiper_further_details_Part_II, last accessed 31st January 2016.

Zetter, K. (2012). "Hackers breached railway network, disrupted service". Available online from http://www.wired.com/2012/01/railyway-hack/, last accessed 31st January 2016.

Zetter, K. (2015). "A cyberattack has caused confirmed physical damage for the second time ever". Available online from www.wired.com/2015/01/german-steel-mill-hack-destruction/, last accessed 31st January 2016.