Industrial cybersecurity imperatives for rail transport

Courtney Schneider, Cyber Policy Research Manager, Waterfall Security Solutions discusses the importance of cybersecurity for rail transport

© iStock/Remus Kotsell

Top priorities for most rail transport operations include safe, reliable and efficient physical operations. In an increasingly automated industry though, cybersecurity is essential to all of these objectives: without security there is no assurance of safety or reliability. The simplest consequence of a compromised signalling system is a shutdown of part (or even the entirety) of a rail network. Much more serious consequences are possible when an attacker deliberately mis-operates a signalling control system.

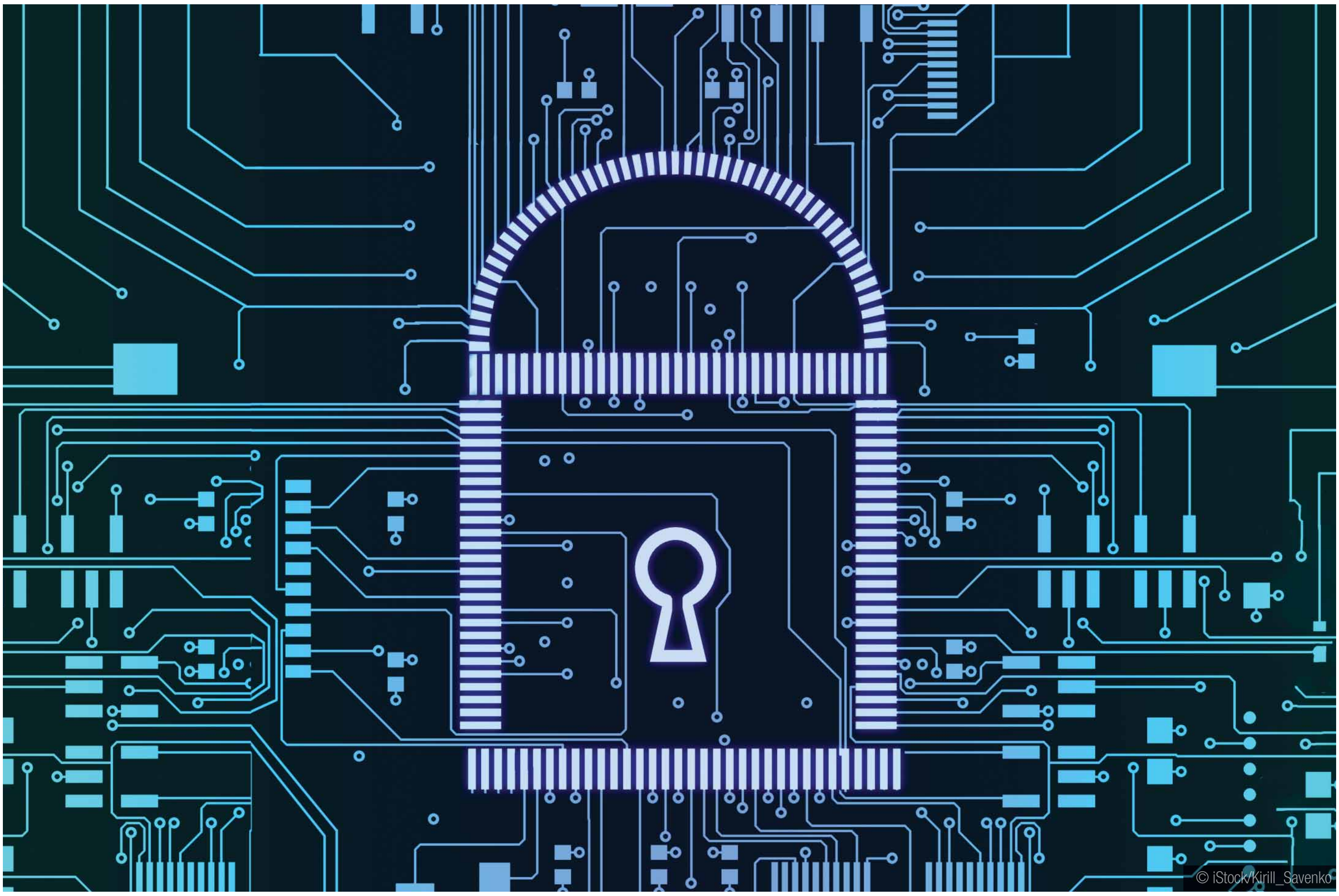
As an industry, we are only slowly coming to grips with cybersecurity. Over the last several decades we have developed sophisticated understandings, requirements and systems for assuring the reliability of safety-critical and reliability-critical signalling system components. The same is not true of cybersecurity.

The fundamental difference between reliability and security is that reliable components do what we need them to do, whereas secure components do nothing else. Components and systems may be very reliable in the face of a wide variety of adverse circumstances, equipment failures and even human errors, whilst at the same time may be woefully insecure.

Targeted ransomware

For example, the trend towards targeted ransomware on IT networks serves as a serious warning to rail system operators. Ransomware is malware that encrypts large parts of file systems and operating systems, rendering them unusable. The operators of the ransomware generally demand money to supply the encryption keys that, hopefully, enable victims to restore impaired computers to an operational state.

Increasingly, ransomware attacks are not simply targeting home users with poor backups who may be willing to pay to restore their photos. Very sophisticated attacks are targeting large networks in institutions such as hospitals (www.healthcaredive.com) and manufacturers (https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/), seeking large sums of money to restore operation to entire networks. Ransomware is emerging as the most reliably profitable class of malware in history, which means that ransomware attacks (both targeted and indiscriminate) will quickly become much more powerful and sophisticated. This is



© iStock/Kirill_Savenko

only one example of the trend towards distressingly sophisticated cyberattacks.

Cybersecurity basics

To signalling system practitioners who may not be familiar with cybersecurity imperatives, the field can seem dauntingly complex. With a bit of perspective though, this complexity vanishes. The most important cybersecurity principles can be summarised as:

1) Nothing is secure – security is a continuum, not a 'yes or no' state. Anyone telling us 'buy X and it will make you secure' is deceiving us. We can always be more secure, or less secure. The question is not 'are we secure?', but 'how secure are we?' and even more importantly 'how secure should we be?'

2) All software can be hacked – all software has bugs after all, both discovered and currently undiscovered. Some bugs are security holes. Therefore, in practice, all software can be hacked.

3) All cyber-attacks are information, and every piece of information can encode an attack – a single message to switch a track can be an attack. Such a message can be exactly the right thing to do at a moment in time, and exactly the wrong thing to do only seconds later.

What we conclude from these principles is that long-standing trends in the computer industry are working against us. In an increasingly automated world, there is ever more software for our attackers to exploit. In an increasingly connected world, there is more and more information flying around for our attackers to use to attack our software.

Automated rail systems

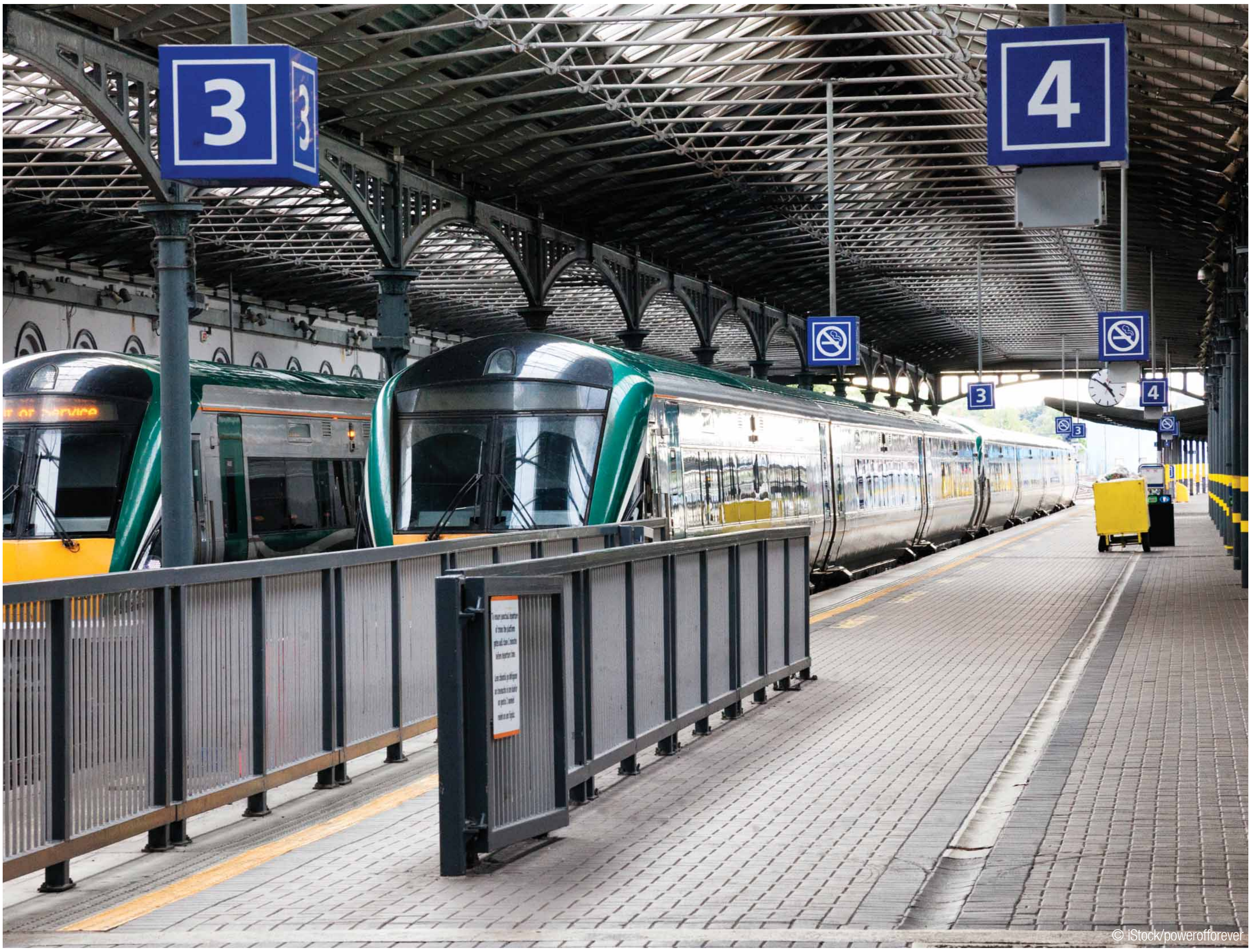
More specifically, rail systems are increasingly automated and connected to improve reliability, efficiency and customer service. Passengers want to be able to use their mobile phones to find out where their trains are and when they will arrive at the next station. Maintenance crews need to see on their phones and wireless tablets which segments of the track are flagged as either 'in service' or 'out of service'. Alongside this, repair crews need to see as immediately as possible when there are outages of escalators in heavily used subway stations. This steady evolution towards both increased automation and increased connectivity have led us to our current, vulnerable state.

Signalling control system networks are unusually vulnerable. Signalling system software is like any other software in that it has defects, some of which are security vulnerabilities. When such vulnerabilities are discovered, reported and repaired, rail system operators are generally unable to apply the security fixes promptly. Signalling systems are always reliability-critical and frequently safety-critical. As a result, no change to their software may be deployed without weeks or more of careful testing and validation by the operator. This means that when software vendors announce both new vulnerabilities and their fixes, there is always a long window of time during which attackers can exploit these public vulnerabilities in our systems.

Secure Operations Technology

While taken together, these truths may seem to describe an insurmountable problem, the opposite is true. Increasingly, rail system operators are turning to Secure Operations Technology (SEC-OT) - a robust industrial control system security methodology. SEC-OT is a perspective, a methodology and a set of cybersecurity best practices used by the world's most secure industrial sites. The methodology is used extensively in the electric power industry and is used increasingly frequently in rail transport signalling and other systems as well.

SEC-OT practitioners define their control-critical industrial networks and carry out comprehensive inventories of all possible online and offline information flows into those critical networks. Since all cyber-attacks are information and all information is a potential cyber-attack, that comprehensive inventory of information flows is also a comprehensive inventory of all possible attack vectors for the critical network. With this



© iStock/powerofforever

list of all possible attack vectors in hand, SEC-OT practitioners start systematically eliminating, inspecting and otherwise disciplining all these attack/information flows.

This is the essence of SEC-OT vs classic IT security: IT security seeks to 'protect the information', while SEC-OT seeks to protect safe, correct and efficient physical operations from information. Again, this is because all information is a potential attack. In addition to this, since security software can also be hacked, SEC-OT teams prefer to apply physical protections against incoming information flows, rather than merely software protections.

Offline and online protections

One of the biggest potential offline information and threat flows for critical rail networks is via removable storage, such as USB drives, CD's and even floppy disks. To address this threat, SEC-OT practitioners work hard to remove, block and control removable media ports and drives on all equipment on control-critical networks. For residual and unavoidable information flows, such as new, tested software versions coming from test beds into production after weeks and months of validation, SEC-OT sites use removable media scanning machines, or sometimes scanning kiosks.

These machines scan suspect media with generally four to eight different anti-virus engines. Files that scan clean are generally copied to brand new media taken from a box next to the scanning system. That media is then carried to a nearby file server, loaded on the file server and so made available via file transfers throughout the critical network. The new and old media can then be discarded.

Protections for online communications are similarly thorough. SEC-OT forbids firewalls between control-critical networks and non-critical networks. All firewalls are software after all, with vulnerabilities and worse, passwords to steal to disable the firewall's software-based protections. Firewalls are used extensively within SEC-OT control-critical networks but are forbidden between critical networks and non-critical networks.

At such connections, SEC-OT requires the use of unidirectional gateway technology. Unidirectional gateways are combinations of hardware and software. The hardware is physically able to send information in only one direction – most commonly from critical networks out to non-critical networks such as enterprise networks and the Internet. Unidirectional gateway software makes copies of servers or otherwise replicates industrial systems to external systems. For example, a Microsoft SQL database in a signalling system is often used to track the location of locomotives, second by second. A unidirectional gateway could replicate that SQL database to an identical database in the enterprise network and keep the two databases synchronised to within a fraction of a second. A web server on the enterprise network could then serve that location information and arrival time predictions out to apps on the cell phones of freight customers and rail system passengers without any risk.

No attack from the internet, no matter how sophisticated, would be able to penetrate physically back into control-critical networks to put those networks at risk. This is because, again, all cyber-attacks are information. If unidirectional gateway hardware is physically unable to send any information back into control networks from enterprise networks or the internet, that hardware is physically unable to send any cyber-attack back either.

© iStock/Nikada

Evolving standards and regulations

Best practice advice, standards and regulations are all increasingly encouraging or demanding the use of these 'protection from information' security techniques, in addition to conventional 'protect the information' cybersecurity approaches. For example, the 2014 French ANSSI standards for critical infrastructure cybersecurity classify critical networks as one of three classes:

1) Class 1: by defintion these include IT networks,

2) Class 2: generally, these involve reliability-critical networks,

3) Class 3: typically, these are safety-critical networks, and rail signalling systems are almost always class 3 networks.

The ANSSI standards demand strict removable media controls and forbid firewalled connections between any class 3 network and any less-critical network, just as does the SEC-OT methodology.

Similarly, the 2016 UK Department of Transport Rail Cyber Security Guidance identify unidirectional gateways as the ideal mechanism for controlling access to signalling networks. Modern advice and standards generally recognise the strength of unidirectional gateway technology and recommend the technology for important control networks. Rail system operators should expect that as cybersecurity expectations for European critical infrastructure mature, unidirectional gateways will increasingly be recommended or required for control-critical rails networks.

Cybersecurity queue jumping

The bad news for the rail transport industry is that many rail systems operators have done very little to address modern cybersecurity threats. The good news is that most rail transport operators now have an opportunity to 'jump the queue' on cybersecurity. Unlike many other industries where most owners and operators have invested large sums of money and effort in software-based industrial security only to discover the inherent weaknesses of such systems, most rail transport operators can transition straight to robust physical cybersecurity protections in the form of SEC-OT-style protections.

Making this transition promptly is important for two reasons. Firstly, very capable cyber threat actors are increasingly targeting rail systems, and so robust cybersecurity protections for safe, reliable and efficient operations are urgently needed. Secondly, deploying robust, physical SEC-OT protections will position rail transport operators as forward-looking and proactive on the cybersecurity front.

The latter perception very much serves to establish good will and a reputation for robust protections with regulators who are becoming increasingly demanding of cybersecurity protections for any operators those regulators see as vital to public safety and national interests. Robust rail transport cybersecurity is both practical and cost effective using modern SEC-OT principles and methods.

Courtney Schneider is the Cyber Policy Research Manager at Waterfall Security Solutions. As a public service, Waterfall Security is currently making copies of the book Secure Operations Technology available free of charge to qualified practitioners at https://waterfall-security.com/sec-ot.

WATERFALL®
Stronger Than Firewalls

Courtney Schneider
Cyber Policy Research Manager
Waterfall Security Solutions

+61 499 315 777

courtney@waterfall-security.com

Reproduced by kind permission of Government Europa, www.governmenteuropa.eu © Government Europa 2019