IRSE NEWS

February 2017

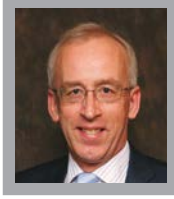
INSTITUTION OF RAILWAY SIGNAL ENGINEERS

Low cost signalling
One view of the future

Lötschberg
Control in the Base Tunnel

Train driving
Tasks of the future

Secure by design: countering cyber threats



Francis How
Chief Executive
IRSE

Robert Stroud
Principal Consultant
Adelard LLP

Railways are in many senses 'mature'. They have been around for 150 years, and wherever they have been introduced they have shaped our lifestyles, work patterns, our towns and cities, industrial activity and much more. It could well be argued that in their time, railways have had a more fundamental influence on society than the present information technology revolution.

But it is information technology that is now leading the way, and the world's railways need to take full advantage of the opportunities that this new revolution offers. In doing so, we also have to recognise the challenges that information technology presents, particularly that of cyber-security. Information technology has made it possible for systems to communicate with each other via computer networks but has also made them vulnerable to attack via those same networks. Cyber-security is concerned with protecting systems against this new threat.

Modern railways are, of course, already heavily dependent on sophisticated data management, control and communications systems. Increasingly they make extensive use of software-based systems that are connected to, or dependent upon, systems outside the railway's 'owned infrastructure', (making use of the internet, GPS, etc.). They also increasingly depend upon commercial 'off-the-shelf' (COTS) hardware, software and firmware that has been developed for multiple applications, many of them not railway-specific. We may eventually even see systems that incorporate situational awareness, self-learning, reasoning and autonomous behaviour, which we have not hitherto seen on the railways.

This progressive sophistication of systems and their integration with non-railway infrastructure and systems will increase the railway's vulnerability to both unintentional and malicious disruption by organisations and individuals intent on causing damage, disruption and threat to life. Attacks on key systems could result in disruption of train services across a widespread area, even if they do not directly jeopardise safety. A poorly designed system could have many weaknesses that make it vulnerable to cyber attack, including:

- Unencrypted communications;
- Insecure software coding practices;
- Insufficient data validation;
- Inadequate security access controls for personnel (both physical and software-based);
- Unsecured third party and remote connections;
- Potential for connection of unauthorised media (USBs etc.);
- Misconfigured firewalls;
- Poor configuration control;
- Inadequate malware protection;
- Poor segregation of high security and other networks (e.g. public wifi on trains);
- Lack of network security event monitoring.

The need for enhanced system security is therefore evident and essential. International Standard IEC 61508-1:2010 (Functional safety of Electrical, Electronic and Programmable Electronic Safety-related Systems) requires *"malevolent and unauthorised actions to be considered during hazard and risk analysis"* (clause 1.2k) and mandates that *"If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out."* (clause 7.4.2.3). It will be interesting to see whether this is reflected in the ongoing revisions of the railway-specific equivalent standard, EN50126.

Defending against cyber threats may necessitate re-thinking our traditional approach to 'fail-safe' design of train control systems, which is at variance with the need to prevent "denial of service" attacks. This design philosophy means that a malfunction involving a fail-safe part of the system (including potentially those caused by cyber attacks) will bring the railway to a standstill. Signalling systems are therefore particularly vulnerable to attacks that aim to disrupt the operation of a railway, even though safety may not be directly threatened.

Building security measures into a system is complex and challenging. Railways are not unique in being a system of systems. Any software-based system is almost certainly composed of sub-systems, components and software that have been sourced from multiple suppliers, including at the most fundamental level, chip designers and manufacturers, operating system suppliers, etc. At the bottom of the hierarchy, these companies are providing general-purpose platforms and building blocks that can be used to construct a range of different systems. They will not necessarily know what their products are being used for, and will at best usually incorporate only generic cyber threat counter-measures into their products. At the other end of the supply chain, the railway infrastructure operator or train operator may understand the overall system of systems for which they are responsible, but they are unlikely to understand all the security measures built into the system, sub-systems, components and

interfaces, nor how they work together effectively. Between these two extremes, there will be system integrators, designers, sub-system suppliers, etc. Each one might reasonably be expected to do their best to ensure security within the scope of their contribution to the overall system (bearing in mind that they may not all know what that larger "system" is).

So we are faced with situations where no one necessarily understands all the counter-measures in the overall system, nor all the vulnerabilities arising from the integration of a number of sub-systems and components that have come from different sources. Nevertheless, the challenge is not insurmountable. There are standards and guidance notes available (see list at end of this article) that aid a systematic, risk-centred approach to cyber threat resilience. Important principles for the specification, design and integration of secure systems include:

a) Using secure methods of system software design and development, with risk-based security assurance.

b) Firewall zoning of vital and non-vital sub-systems within the overall system architecture, to protect those that are the most important from operational and safety perspectives.

c) Protection against the corruption of software, data and messages, including encryption and digital signing of operationally critical data to prevent tampering and illicit use, and robust bounds checking to ensure that malicious data does not cause software to malfunction.

d) Authentication of transmitted data to verify that received data originated from a valid source, not from a fraudulent one (use of cryptographic keys for authentication, etc.).

e) Validation and coding techniques to reduce the likelihood of errors being made by personnel when entering critical data (e.g. on board trains).

f) Physical security, to ensure that only personnel who have been authorised to access or work on the systems are able to do so.

g) System monitoring and behavioural analytics to detect intrusions.

But good initial design is not sufficient. Conventionally, train control systems are designed to be safe. We understand the risks to safety, and we design to prevent or mitigate them. Provided we use those systems within the scope of their intended operation, and we maintain them in good order, they will generally continue to control the risks satisfactorily. The risks arising from cyber threats are different, however. Those who perpetrate such threats are forever looking for new vulnerabilities in systems. The fact that your system was acceptably secure yesterday is no guarantee that it still is today. Vigilance throughout the operational life of systems, and responding appropriately to newly emerging threats , is essential in order to maintain protection and resilience. It also requires good collaboration between organisations and companies, and the sharing of cyber threat knowledge between organisations, in order to keep abreast of changing threats.

Ensuring that a system remains secure during operation therefore requires a proactive approach. Vulnerabilities and threats develop over time and need to be continuously assessed. Formal vulnerability management procedures are required in order to detect, evaluate and react to newly published vulnerabilities and changes to the threat landscape. Security patches cannot be applied to safety-critical system without analysing their potential impact on the safety case, so it is important to assess the impact of each threat and consider whether alternative controls are available. Software vulnerabilities can be very dependent on the exact version of the software, so this requires close collaboration with the vendor, who can advise on whether the system is affected by a particular vulnerability and provide patches that have been tested and certified.

Security is not just about prevention but also includes detection and response. If something goes wrong, it is important to detect it early and respond appropriately as soon as possible. A cyber-security incident response plan should be developed and integrated with other business continuity, disaster recovery, and emergency response plans. An early warning system should be established to detect and respond to security alerts and incidents. All security incidents should be formally reported and reviewed, and lessons learned should be captured and fed back into the incident response plan.

Further guidance on best practice for vulnerability management, incident response, and other key activities for ensuring the security of operational systems can be found in the Centre for the Protection of National Infrastructure (CPNI) good practice guide on Security for Industrial Control Systems.

In summary, therefore, it can be seen that ensuring and maintaining security and resilience in the 'cyber' world requires not only sound technical design, but also strong collaboration between supply chain partners, the sharing of knowledge about changing threats, and unremitting vigilance throughout the operation of the system under consideration. Security should be a concern throughout the entire life cycle of a system, from procurement through design, construction, operation and finally decommissioning and disposal.

Standards and Guidance

IEC 62443 (all parts), Industrial communication networks – Network and system security.

ISO/IEC/TR 19791, Information technology – Security techniques – Security assessment of operational systems.

UK Department for Transport– Rail Cyber Security Guidance to industry: ***http://bit.ly/2hmJtXq***.

National Cyber Security Centre – Security for Industrial Control Systems – A good practice guide: ***http://bit.ly/2hsewxT***.

Work has just started on the development of a new standard on IT Security for railway signalling applications, under the direction of CENELEC group SC 9XA.

Shutterstock/Dragon images.