Signalling cyber security: the need for a mission-centric approach

Written by Valentin Gapanovich, Efim Rozenberg and Sergey Gordeychik

International Railway Journal , July 12, 2016

http://www.railjournal.com/index.php/signalling/signalling-cyber-security-the-need-for-a-mission-centric-approach.html

While the implementation of computer-based control systems, particularly railway signalling and interlocking tools, is helping to increase capacity, speed, and optimise train operation, maintaining the cyber security of such devices is of paramount importance. Valentin Gapanovich, senior vice-president, Russian Railways (RZD), Efim Rozenberg, first-deputy director general, NIIAS, and Sergey Gordeychik, deputy CTO, Kaspersky Lab, outline their optimal approach to railway signalling cyber security.

THE use of computer-based control systems (CBCS) requires the use of digital wire and radio communication systems supporting the TCP/IP protocol on a large scale. However, since they are based on standard systems, application software and network protocols, and make extensive use of remote management tools, wireless networks and internet technologies, they inherit the security problems of the underlying standard components. This means that new requirements for communications infrastructure need to be put in place in order to guarantee its safety.

 Research into the IT security of industrial control/supervisory control and data acquisition systems (ICS/Scada) shows that the methods and approaches commonly used to breach information and computer security can be successfully employed to disrupt functional safety, reliability and industrial process safety.

Today's complicated geopolitical situation and the evolution of tools for carrying out attacks against computers necessitate a revision of the threat models used to analyse security status and build security tools. Havex, a sophisticated cyber attack carried out last year enabled attackers to compromise the websites of ICS/Scada component manufacturers, and replace the software distribution packages available for download. This allowed unsuspecting operators to download specialised malware from manufacturers for installation in ICS segments.

A detailed analysis of the security status of widely-used ICS/Scada systems, including railway and interlocking CBCS, has identified faults and vulnerabilities, which allow cyber criminals to not only degrade key reliability parameters and bypass safety mechanisms, but also to carry out attacks which directly affect rail traffic safety. Remarkably, these systems meet all of the relevant IT security and functional safety requirements and all have the required international, national and industrial certificates.

The main difference between such attacks and false readings, familiar to signalling experts, is the ability to carry out attacks remotely, and the ease with which evidence can be concealed, preventing the causes of an incident from being identified.

It is self-evident that railway CBCS should be designed with the possibility of attack in mind to avoid adversely affecting railway safety and operations.

The main objective of railway cyber security is to ensure safety. Until recently, research and development focused primarily on achieving sufficient CBCS reliability and functional safety. Human threats were limited to operator and auxiliary personnel errors, which is justified if large-scale remote attacks are ruled out. However, this ignores the possibility of remote attacks against computer devices using distributed communication systems and wireless technologies, which makes it impossible to get an unbiased view of rail traffic safety.

Security standards

Most industry and international security standards aim to ensure reliability and reduce the number of random dangerous failures. Although these objectives clearly overlap with those of cyber security, the fact that the threat models underlying these standards do not account for cyber threats means that these standards cannot be used as exhaustive guidelines.

Some overall ICS/SCADA security requirements are based on the familiar concept of ensuring the integrity, availability and confidentiality of information, while the goal of protecting railway CBCS is safety.

In other words, regulatory, organisational and technical issues related to the IT security of signalling CBCS systems are being poorly addressed. This creates a discrepancy between IT security approaches and methods, and railway safety issues.

We therefore suggest defining cyber security as the process of ensuring the operation of signalling CBCS in which dangerous failures and inadmissible damage are ruled out, and a given level of economic efficiency, functional safety and reliability is provided in the event of an IT attack directed at signalling CBCS components.

We suggest using the methodology borrowed from rail traffic safety (industrial security), functional safety, and IT security, in order to use existing research and methodology tools, as none of these disciplines alone can address the issues. For example, functional safety is concerned with random system failures rather than targeted threats, while IT security provides the integrity, availability and confidentiality of information, not directly connected with railway safety.

The main advantages of this approach include the ability to integrate cyber security into existing signalling CBCS design, development and implementation without having to give up proven

approaches and solutions. Table 1 (opposite) shows some of the methods that can be taken from the three disciplines to guarantee the cyber security of such hardware.

Defining threats

Correctly defining threats is the foundation of security. From a cyber security viewpoint, there are three main classes of threats to signalling CBCS:

- breaches of train movement safety
- reduced efficiency due to factors affecting track and carrying capacity, and other economic efficiency parameters, and
- other breaches of functional safety and reliability that indirectly affect railway safety and operation.

This enables an aggregated threat model to be built based on the railway and functional safety requirements. For example, consider an aggregated threat model for a computer-based interlocking (CBI) system using the requirements set out in railway operating rules. Based on the properties of other systems, the list of threats should certainly be extended.

Threats resulting in railway safety breaches are usually the most difficult to put into practice and require the greatest effort by the perpetrators. To be successful, an attacker must bypass the CBI's functional safety mechanisms. If object controllers cannot be manipulated directly, for example by using the radio channel's vulnerabilities, such attacks require modifying the operating logic of the main CBI modules concerning switch and signal interlocking and compliance with traffic safety requirements, which is complicated. However, if it is possible, an attacker can:

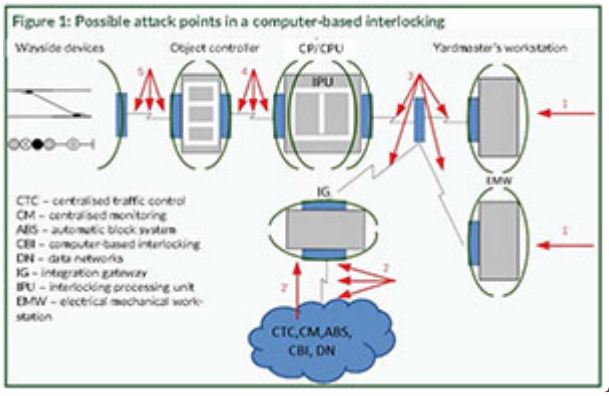
- set a signal to a less-restrictive aspect such as green for a section with track divergence on switches
- change a signal aspect to green for an inadmissible route which has blocked sections or incorrect switch positions
- operate a switch with a train passing over it, and
- set conflicting routes.

Threats aimed at disrupting rail transport do not usually require the attackers to be highly professional and can be put into practice using standard malware. Such threats include putting non-redundant components out of operation, spoofing or blocking network interaction between the yardmaster's workstation and CBI components, thereby blocking the system's ability to send commands. Such an attack requires a switch to manual operation, which reduces efficiency.

Threats that indirectly affect railway safety and efficiency include putting the electrical mechanic's workstation out of operation or forcing the central processing unit (CPU) or the yardmaster's workstation to reboot.

To build a CBI threat model, the object to be protected must be described correctly and the CBI components (functional modules) vulnerable to threat identified. The components should have their own security mechanisms to make an attack more difficult while they themselves can become objects of attacks.

In attacks on lineside equipment such as switch motors and signals, an attacker seeks to interfere with their control. However, such devices lack sufficiently advanced control interfaces to be a direct target, unless they are radio-controlled which makes them vulnerable, so the threat model should take this into account.



A central processor (CP/CPU) receives information from workstations and other systems, processes it and verifies whether specific commands are admissible based on train positions and the state of signalling and interlocking devices. As a rule, the CP/CPU has dedicated software running on a standard operating system (OS) and provides the main functional safety and fail-safe mechanisms which makes a high-priority target for attackers.

The interlocking processing unit (IPU), which is usually part of the CP/CPU, performs the main tasks related to controlling switches and signal interlocking and complies with railway safety rules.

Object controllers (OC), which receive commands from the central processor, convert them to control signals to actuate wayside equipment and send information on the state of the objects back to the CP/CPU. Object controllers may perform certain functional safety and interlocking functions and, depending on their type, could be high-priority attack targets because they can be used to bypass the interlocking system.

Operations and service staff workstations perform human-machine interface (HMI) functions and can monitor train positions and the state of signalling devices, as well as send commands to change the aspect of signals or operate switches.

Workstations usually have specialised software, sometimes with built-in security, on personal computers running general-purpose operating systems such as Windows. They have a large attack

surface, since they have various network and hardware (USB) interfaces and interact extensively with all components of the interlocking and personnel which means attackers can use psychological manipulation to influence operators.

Network communications are prone to attack because the equipment interacts between components and may support both standard and specialised or obsolete protocols, with significant computational capabilities, and remote administration tools.

Network protocols interact between CBI components, so a cyber threat model should account not only for transport protocols such as Ethernet, TCP/IP, and GSM, and protocols implementing the CBI logic, but also auxiliary protocols used for diagnostics, remote administration, OS and database interaction.

A CBI also has communication channels based on current loop, wireless and backbone communication channels which integrate it with other systems while making it vulnerable to attack.

Signalling integration junctions and gateways (IG) enable information on device status and train positions, as well as control commands, to be exchanged with adjacent systems. This makes them prone to attack, since they make the CBI part of a distributed system. Security requirements for a CTC system are usually lower than those for a CBI, which needs to be kept in mind when integrating these systems.

Personnel

One more important CBI component should be considered - the service and operations personnel. A variety of techniques can be used to prevent signalling and interlocking staff, train dispatchers, yardmasters, system administrators, and maintenance staff from being tricked or deceived into doing something wrong, while attackers can use different tactics, such as passing themselves off as other people, distracting a worker's attention, or building up psychological tension.

When performing an in-depth analysis for attack simulation it should be kept in mind that many components are not uniform. For example, a CP/CPU consists of several logical units which use different hardware and copies of the operating system. These units implement fail-safe mechanisms by using result comparison with majority circuits to test availability and implement control and interlocking algorithms, while the CP/CPU is a multiple-component system with clearly-defined security perimeters.

To build a consistent cyber threat model, attack access points should be identified. Figure 1 is a diagram of a CBI model showing possible attack points. An attack is usually possible where an external interface allows an attacker to manipulate the attack target.

Attacks can be either local or remote. The ability to carry out a local attack often depends on the type of the interface through which an attack is carried out. For example, where an attacker is able to apply power to a signal light or switch motor by accessing the cable connecting the OC with wayside devices. However, a remote attack can be carried out where wayside devices are radio controlled.

While it is relatively easy to breach traffic safety, such attacks take considerable skill because they require consecutive bypassing of security mechanisms. While CP/CPU and IPU have mechanisms to control integrity and protect against unauthorised interlocking logic modification, which reduce the chances of a successful attack, an attack on communication channels connecting wayside devices is much easier if data can be manipulated or carried out by a man-in-the-middle.

Train operations can be disrupted by displaying incorrect train positions on the yardmaster's workstation if the network protocol between the yardmaster's workstation and CP/CPU can be manipulated. Using other means would require a multiple-stage attack which would start by compromising the yardmaster's or electrical mechanic's workstations.
Device functional safety and reliability can be breached by temporarily putting the CBI out of operation by taking advantage of vulnerabilities in the operating system on the electrical mechanic's workstation, in CBI application software, or by using passwords which are too simple.

Communication channels and network protocols can be attacked if communication channel bandwidth is reduced, or by introducing false routes. Most of these attacks can be carried out using general-purpose malware designed to infect Windows OS, or by getting an operator to connect an infected USB drive to the workstation or perform actions that will put the system out of operation. But an attacker will first need to break through the integration gateway's security mechanisms, provided it has built-in security features.

Modelling threats using a CBCS model helps to identify the most likely forms of attack, the security mechanisms that can block them and the system's weakest cyber security components. Using mathematical models and simulation can help to significantly expand the threat model, helping to optimise the analysis of security and risks of cyber security breaches and to choose protection tools.

Defining cyber security through traffic and functional safety, and IT security helps to understand how the industry operates and assesses any negative impact in terms of dangerous failures and

reliability theory, thereby making it possible to integrate cyber security processes into existing railway safety and operations processes.