FOR SENIOR RAIL MANAGEMENT
RAILWAY STRATEGIES

FEATURES

THE SECRETS OF CYBERSECURITY

ISSUE 130 JUNE 2016

VALENTIN GAPANOVICH, senior vice president, Russian Railways, EFIM ROZENBERG, first deputy director general, NIIAS JSC and SERGEY GORDEYCHIK, deputy CTO, Kaspersky Lab, discuss a mission-centric approach to cybersecurity for computer-based railway signalling and interlocking systems

The use of computer-based systems requires digital wire and radio communication systems supporting the TCP/IP protocol to be used on a mass scale. However, since such systems are based on standard system and application software and network protocols they inherit the security problems of the underlying standard components.

Are current systems secure?
A detailed analysis of the security status of widely used ICS/SCADA systems, including RSI CBCS (https:// blog.kaspersky.com/train-hack/10946/), has identified weaknesses and vulnerabilities, which enables cybercriminals and state-sponsored threat actors to not only degrade the key reliability parameters and bypass functional 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 have all the required international, national and industry certificates.

Most industry-wide and international security standards, such as BS EN 50128:2011 and BS EN 50129:2004, aim primarily to ensure reliability and share the IEC 61508 paradigm with regard to reducing the number of random dangerous failures. Although these objectives clearly overlap with those of cybersecurity, the fact that threat models underlying these standards do not account for cyberthreats means that these standards cannot be used as exhaustive guidelines. Some overall ICS/SCADA security requirements are provided in the NIST and IEC documents (such as IEC 62443/ANSI 99). However, the document is based on the familiar concept of providing the 'integrity', 'availability' and 'confidentiality' of information, while the goal of protecting the RSI CBCS is rail traffic safety.

Developing a mission centric approach
To address this discrepancy, we suggest to use missioncentric approach and to define cybersecurity as the process of ensuring the operation of RSI 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 intentional negative anthropogenic IT-related impact directed at RSI CBCS components.

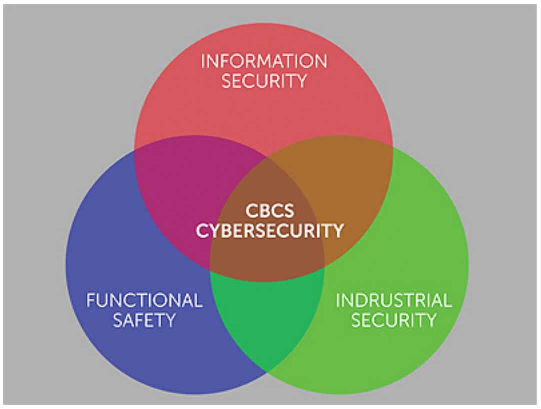
In the process of developing this concept as part of addressing the issue of RSI CBCS cybersecurity, we suggest using the methodology borrowed from three disciplines: rail traffic safety (industrial security), functional safety, and IT security.

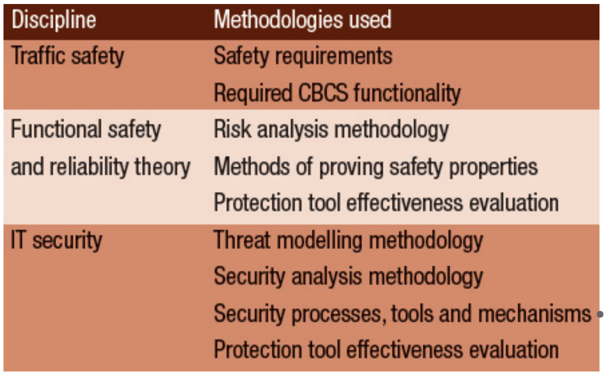
The main advantages of this approach include the ability to integrate cybersecurity into existing RSI CBCS design, development and implementation processes without having to give up proven approaches and solutions. The table opposite shows some methods that can be taken from the above three disciplines and the ways in which they can be used to provide the cybersecurity of such hardware.

Build a strong foundation
Correctly defining threats is the foundation of security. From the cybersecurity viewpoint, there are three main classes of threats to RSI CBCS:

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

This approach to address CBCS cybersecurity enables an aggregated threat model to be built based on the traffic safety and functional safety requirements applied to this class of systems. As an example, consider an aggregated threat model for a computer-based interlocking (CBI) system using requirements set out in the railway technical operation rules. Based on the properties of other systems, the list of threats should certainly be extended.





Discipline	Methodologies used
Traffic safety	Safety requirements Required CBCS functionality
Functional safety and reliability theory	Risk analysis methodology Methods of proving safety properties Protection tool effectiveness evaluation
IT security	Threat modelling methodology Security analysis methodology Security processes, tools and mechanisms Protection tool effectiveness evaluation

Threats that lead to breaches in rail traffic safety are usually the most difficult to put into practice and require the greatest amount of effort from the attacker. To achieve a result, an attacker needs to bypass the functional safety mechanisms implemented in the CBI. However, if this is possible, an attacker can:

- set a less restrictive signal light (eg a green entry signal for a segment with track divergence on switches)
- change a signal light to a clear aspect for an inadmissible route (a route with blocked segments or incorrect switch positions)
- operate a switch with a train passing over it, or
- set conflicting routes etc.

Modelling the threat

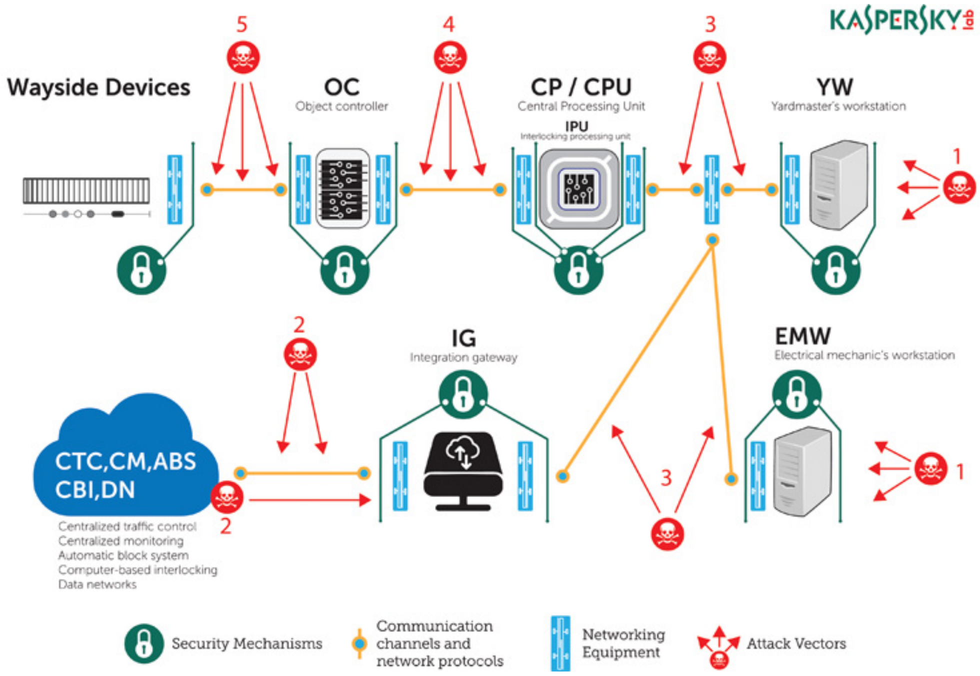
To build a consistent cyberthreat model, attack (access) vectors should be identified, ie the points and objectives of a potential attacker's actions at each phase of an attack. The figure below is a diagram of a CBI model showing possible attack vectors. It can be seen in the diagram that an attack is usually possible where there is an external interface that enables an attacker to manipulate the attack target.

Attacks in details

Attacks can be conducted either locally or remotely. The ability to carry out the former type of attack often depends on the technical implementation of the interface through which an attack is carried out. For example, for vector 1, a threat model usually accounts for a local vector enabling an attacker to apply power to a signal light or switch motor by gaining physical access to the cable connecting the OC with wayside devices. However, if radio control systems are used to control wayside devices, a remote attack can be carried out.

Implementing threats of the 'breach of traffic safety' class via vectors 4, 4', 5, 5' and 3, which are the easiest to put into practice, takes considerable skill on the part of an attacker, because they require consecutive bypassing of the security mechanisms of IG, CP/CPU, IPU and OC. On the one hand, CP/CPU and IPU as a rule implement mechanisms of integrity control and protection against unauthorised interlocking logic modification, which reduce the chances of an attack being carried out successfully. On the other hand, if an attack on communication channels connecting wayside devices, OC and CP/CPU via vector 1 or 2, ie by manipulating data or carrying out a man-in-the-middle attack, is possible, it significantly facilitates the task faced by attackers.

The efficiency of rail transport operations can be reduced, for example by displaying incorrect train positions on the yardmaster's workstation via vector 3 by manipulating the network protocol between the yardmaster's workstation and CP/CPU, provided that it has suitable vulnerabilities. Putting this threat into practice via other vectors would require a multiple-stage attack. The first step could be to compromise the yardmaster's workstation or electrical mechanic's workstation via vector 4 or the integration gateway via vectors 5 and 5'.



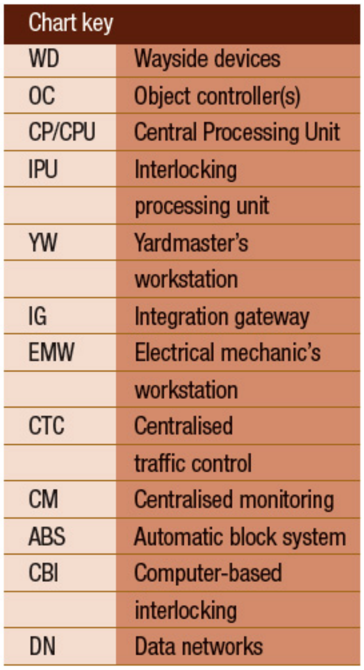


Chart key	
WD	Wayside devices
OC	Object controller(s)
CP/CPU	Central Processing Unit
IPU	Interlocking processing unit
YW	Yardmaster's workstation
IG	Integration gateway
EMW	Electrical mechanic's workstation
CTC	Centralised traffic control
CM	Centralised monitoring
ABS	Automatic block system
CBI	Computer-based interlocking
DN	Data networks

A breach of device functional safety and reliability can be implemented, among other methods, through temporarily putting the CBI out of operation by carrying out an attack via vectors 4, 4', 5, 5' and 3. An attack of this kind could take advantage of vulnerabilities in the operating system on the electrical mechanic's workstation (eg unpatched software or outdated operating system, such as Windows 2000/XP), in CBI application software, simple passwords used in the operating system, etc. Attacks on communication channels and network protocols can also be carried out by reducing communication channel bandwidth (flood), introducing false routes (eg ARP Spoofing), etc. Most of these attacks can be carried out using general-purpose malware designed to infect Windows OS. To carry out an attack via vectors 4 and 4', an attacker can use social engineering methods, getting an operator to connect an infected USB drive to the workstation or perform actions that will put the system out of operation. To carry out an attack via vectors 5 and 5', an attacker will first need to break through the integration gateway's security mechanisms, if this component is present on the system and has built-in security features.

Conclusion

The approach described here, which is based on modelling threats using a CBCS model, helps to identify the most likely attack vectors, the security mechanisms that can block such attacks and the system's weakest components from the cybersecurity viewpoint. Using mathematical models and simulation can help to significantly expand the threat model, helping to optimise the analysis of security and risks of cybersecurity breaches and to make and validate the choice of protection tools.

Defining cybersecurity through the disciplines of traffic safety, functional safety and IT security helps to account for the ways in which the industry operates and assess any negative impact in terms of failures and reliability theory. This in turn can make it possible to integrate cybersecurity-related processes into existing train safety and rail operation efficiency processes.

Valentin Gapanovich is senior vice president, Russian Railways
Efim Rozenberg is first deputy director general, NIIAS JSC – Russia's leading research and design institute for railway transport traffic control and safety systems
Sergey Gordeychik is deputy CTO, Kaspersky Lab

TAGS: Efim Rozenberg Security Sergey Gordeychik Valentin Gapanovich

MORE CONTENT

FEATURES

AN EAR TO THE GROUND

FEATURES

PROS AND CONS OF DRONES IN RAIL SECURITY

Search … SEARCH

ADS

WHY ADVERTISE IN RAILWAY STRATEGIES?

Railway Strategies can help companies to reach their target audience. Whether raising awareness of a new technology, increasing a reputation in the market or looking for new clients, Railway Strategies can help by positioning your company in the right place – in the hands of your future customers.

Schofield Publishing

Schofield Publishing,
10 Cringleford Business Centre,
Intwood Road,
Norwich, Norfolk NR4 6AU

Tel: +44 (0)1603 274130

www.schofieldpublishing.co.uk

OTHER PUBLICATIONS

Energy, Oil & Gas
Manufacturing Today
Shipping & Marine
Construction & Civil Engineering
FoodChain
Health & Safety Monitor

TAGS

AFRICARAIL APPOINTMENTS BIRMINGHAM CONCRETE CONFERENCE CONFERENCES COURSES CROSSRAIL ELECTRIFICATION ENGINEERING ENGINEERS EXHIBITIONS HEART HS2 IET INTERNATIONAL RAILWAY ENGINEERING IMECHE INFRARAIL INFRASTRUCTURE INNOTRANS INNOVATION INSTITUTE INTEGRATED TRANSPORT ITA LONDON UNDERGROUND MAINTENANCE MECHANICAL METRO METROLINK NETWORK RAIL NEWS ORR RAIL REVENUE RAILTECH ROLLING STOCK RSSB SECURITY SOUTH WEST TRAINS STATION STATIONS TECHNOLOGY TICKETING TRAM TRANSPENNINE EXPRESS TUNNEL WHEELSET

Follow us on Twitter