Cyber Resilience of Railway Signaling Systems

Sergey Gordeychik
serg.gordey@gmail.com

ABSTRACT

Recently published information on the cybersecurity assessment of railway computer and communication-based control systems (CBCS) identified several weaknesses and vulnerabilities, which allow threat agents to not only degrade system reliability and bypass safety mechanisms, but to carry out attacks which directly affect the rail traffic safety. Despite these findings, remarkably these systems meet all relevant IT security and functional safety requirements and have the required international, national and industrial certificates.

The paper shows the link between information security and industrial. Railroads is a complex systems and process automation is used in different areas: to control power, switches, signals and locomotives. At this paper author analyze threats and vulnerabilities of fundamental rail-road automation systems such as computer based interlocking, automatic train control and automatic train protection. All examples based on hands-on security exercises and most of issues are confirmed and processed by vendors.

KEYWORDS

railway, industrial control systems, traffic safety, security, implementation security, cybersecurity, threat intelligence, scanning, fingerprinting, cloud networks, vulnerabilities

Table of Contents

INTRODUCTION

Rail traffic security is one of the most important problems in railway service. Railway signaling systems, systems of railway telemechanic and automation (RTA) considerably influence the carrying and traffic capacity and provide traffic safety. Currently, Computer-Based Interlocking (CBI) and Centralized Dispatching Control (CDC) systems, as well as locomotive protection systems such as Continuous Automatic Cab Signaling, Automatic Brake Control, and Integrated Train Protection systems are widely used to control the transportation service. Automatic Train Operation systems are under test now. Computer-Based Automatic Switching systems make it possible to optimize train classification and review the list of cars not safe for classification, which results in huge economical advantage. Computer-based systems are also introduced into locomotive management to control the locomotive electric transmission, as well as into power division management and relay protection systems.

Application of the above-mentioned systems requires communication infrastructure development, which results in wide-scale introduction of digital TCP/IP-based wireline and radio communication systems.

Computer-Based Control Systems (CBCSs) provide powerful capabilities for transportation optimization, management scaling, and control and monitoring automation. However, combination of general-purpose system and application software and network protocols, common ICS/SCADA technologies along with remote and centralized traffic control results in cyber security problems inherited from all these typical components.

Among important issues are deep integration with Data Communication Networks (DCNs), wide use of wireless technologies, and deployment of interactive information services, which expands the attack surface and increases the number of sources of security threats.

Researches in IT security of Industrial Control/Supervisory Control and Data Acquisition (ICS/SCADA) systems and a number of incidents showed that

an attacker can use common methods and approaches to affect functional safety, reliability, and industrial process safety.

An impulse to change the attitude to CBCS security was a series of high-scale attacks against various ICS/SCADA systems. The Stuxnet computer worm uncovered in 2010 involved usual methods to spread, interact with the attacker, and resist detection and was designed to affect industrial processes. The malware exploited vulnerabilities of Microsoft Windows Operating Systems (OSs) and features of SCADA Siemens SIMATIC WinCC and PLC S7-400 to change the operating condition of centrifuge engines at the uranium enrichment facility at Natanz (Iran). The attack provoked centrifuge runout which resulted in accelerated wear-out[1]. A number of sources report that Stuxnet ruined 1368 out of 5000 centrifuges at the enrichment plant.

These attacks showed that traditional methods and approaches to IT and cyber security violation can be used to affect functional safety and reliability.

These days, geopolitics is an essential factor. Railway service represents a strategic sector of national economy. It provides military transport and must remain functional if attacked by other countries. At the same time, the world's leading states are developing their military cyber forces.

Consequently, designers, developers, and deployers of CBCS-based RTA systems should consider the possibility of remote targeted cyber-attacks performed by malicious persons to affect the traffic safety, carrying and traffic capacity and equipment reliability.

This work is aimed to develop methodological guidelines for improving the RTA CBCS cyber resilience and to define the promising directions for RTA CBCS cyber security development with respect for IT security, functional safety and railway operation safety requirements. To reach the identified goals, the following basic problems are set:

[1] Ralph Langner. To Kill a Centrifuge. // [langner.com] URL: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

1. To define the tasks for improving the RTA CBCS cyber resilience; to evaluate the attacks' influence on functional safety, rail traffic safety, and economic viability of the railway service.
2. To define approaches to the establishment of RTA CBCS cyber resilience assurance processes taking into account today's threats, regulatory system and rail traffic safety requirements.
3. To develop and test RTA CBCS security analysis techniques taking into account the influence of vulnerabilities and defects on RTA CBCS cyber resilience, rail traffic safety, and reliability.
4. To develop requirements to special-purpose RTA CBCS security features.

As a result, the paper formulates the key stages of cyber resilience assurance processes; it proposes and evaluates a technique for RTA CBCS threat modeling, a technique for security analysis of CBCS software and hardware complex; the paper also lists technical features of the most promising CBCS security tools.

The work is to a great extent based on the real-life experience of the author and his group. Based on the findings from dozens of projects aimed at cyber resilience analysis of various ICS/SCADA systems including railway-specific systems, the inductive approach was applied to develop security analysis techniques, cybersecurity requirements, partial threat models (for computer-based interlocking systems, network interface modules, etc.), and requirements to advanced security tools. The latter requirements are based on the automata theory and the simulation modeling approach.

1. Problem of Railway cyber resilience

Overview

Practical analysis of cyber resilience of various widely used RTA CBCSs revealed weaknesses and vulnerabilities that allow an attacker not only to affect reliability and bypass functional safety mechanisms, but also to conduct attacks directly against the traffic safety. Remarkably, these systems meet all relevant IT security and functional safety requirements and have all required international, national and industry certificates.

The main difference between attacks against RTA CBCSs and usual unauthorized straps is that the former attacks may be remote (without direct physical access) and the evidences can be easily hidden.

Today, the scientific and engineering communities all over the world intensively discuss the influence of IT security on modern ICS/SCADA systems. The main trends here are the attempts to adapt the existing experience in IT security to the ICS/SCADA cyber resilience. There are three directions:

1. To analyze and evaluate the ICS/SCADA security and the influence of vulnerabilities on the industrial processes' reliability.
2. To develop regulatory and methodological systems.
3. To develop special-purpose methods and tools to improve cyber resilience.

Analysis and evaluation of ICS/SCADA cyber resilience are not performed on a regular basis. These projects often are a part of corporate contracts, so the investigation results cannot be published. However, sometimes vulnerabilities are publicly discussed at research-to-practice conferences. In 2013, a report on Siemens SIMATIC vulnerabilities[2] was presented at SCADA Security Scientific

[2] Sergey Gordeychik, Gleb Gritsai. SCADA strangelove or: How I learned to start worrying and love nuclear plants

Symposium; meanwhile, the railway automation system Siemens Sibas PN is based on the SIMATIC core components[3].

One of the problems is that efforts in ICS/SCADA security development are not coordinated. Computer emergency response teams (CERTs) are trying to solve this problem. The most recognized one is the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) within the United States Department of Homeland Security. This team is tracking the updates of ICS vulnerabilities and coordinates interaction between vendors and researchers. In the European Union, the European Union Agency for Network and Information Security (ENISA) does the same; they consider the railway service as a public transport sub-system in so-called smart cities[4].

Beside the open institutions, there are organizations that reveal and resell information about vulnerabilities and methods to conduct attacks. The examples are Exodus Intelligence in the USA, and ReVuln and Vupen (Zerodium) in Europe. In this case, the community of security professionals and even vendors do not receive information about vulnerabilities and attack vectors for a long time, which prevents urgent elimination of the weaknesses.

The number of revealed vulnerabilities and attack methods increases continuously. In 2012, there were less than 100 known defects[5]; as at the beginning of 2015, there already were more than 800[6]. According to SCADA StrangeLove team as they reported at Chaos Communication Congress in Germany, most vulnerabilities were revealed in products of the major vendors

[3] Sergey Gordeychik, Gleb Gritsai, Aleksandr Timorin. The Great Train Cyber Robbery. SCADA StrangeLove

[4] Cyber security for Smart Cities. An architecture model for public transport // [European Union Agency for Network and Information Security] URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/intelligent-public-transport/smart-cities-architecture-model/at_download/fullReport

[5] Gleb Gritsai, Alexander Timorin, Yury. Goltsev, Roman Ilin, Sergey Gordeychik. SCADA safety in numbers

[6] Oxana Andreeva, Sergey Gordeychik, Gleb Gritsai, Olga Kochetova, Evgeniya Potseluevskaya, Sergey I Sidorov, Alexander A Timorin. Industrial control systems vulnerabilities statistics

such as Siemens, Honeywell, and Schneider Electric. Notably, only 65 % of the revealed vulnerabilities have been eliminated; 35 % have no solution.

The current situation is conductive to the increase in the number of successful attacks, because uneliminated vulnerabilities make it cheaper to develop and conduct them. For example, the Sandworm malware relied on known weaknesses of GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC platforms used for ICS/SCADA systems. One of the attack development vectors exploited SCADA projects containing malicious elements. The attack conducted on December 23, 2015 resulted in outage of seven 110 kW electric substations and twenty-three 35 kW substations in Ukraine; 225 000 customers were affected.

As to the regulatory systems for ISC/SCADA resilience purposes, the most prominent example is the ANSI/ISA-62443 guidance series. Industrial documents regarding ICS security are best reworked for the energy industry. Most of them are based on the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards[7]. The railway service has ill-defined cyber resilience requirements. The documents usually specify high-level requirements that reduce to providing resistance to cyber viruses, unauthorized access, denial of service, data storage, input/output and processing errors, and accidental data modification. As one can see, this is not about targeted attacks, but rather about random influence. However, an authorized access is mentioned, which implies human participation.

GOST R 52980-2008 specifies software requirements for devices and systems providing railways safety. It also covers software used to develop security systems. However, this standard doesn't provide requirements to software security and quality regarding targeted cyber-attacks.

[7] NERC CIP Standards // [North American Electric Reliability Corporation] URL: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Taking into account that the most important cyber resilience problem for railway services is traffic safety, it is necessary to consider the RTA CBCS security research and practical experience. Analysis of issue-related papers shows that until recently, the trend area of research and development was providing sufficient reliability and functional safety of CBCSs.

In most investigations, human threats were reduced to operator and maintenance staff mistakes. The approach was reasonable enough until large-scale remote impacts became possible. Today, this simplified model leaves out critical threats such as remote cyber-attacks and consequently doesn't allow researchers to develop a true traffic safety picture considering CBCSs. Introduction of distributed communications systems, wireless technologies, and centralized traffic and dispatch control systems requires security concept review.

Thus wise, regulatory, organizational and technical issues of modern CBCS cyber resilience regarding railway services are being poorly addressed. There is a gap between IT security approaches-and-methods and railway traffic safety practices.

Railway Cyber Resilience

To choose the directions for development of RTA CBCS cyber resilience methodological support with respect for IT security, functional safety and railway operation safety requirements, it is necessary to determine the development purposes and tasks.

RTA cyber resilience can be defined as a process of RTA CBCS maintenance that excludes dangerous failures and unacceptable damages and provides the target functional safety and reliability levels, particularly in case of cyber-attacks against the CBCS components.

To develop this concept, we suggest using the methodology borrowed from the following three disciplines: rail traffic safety (industrial security), functional safety, and IT security[8].

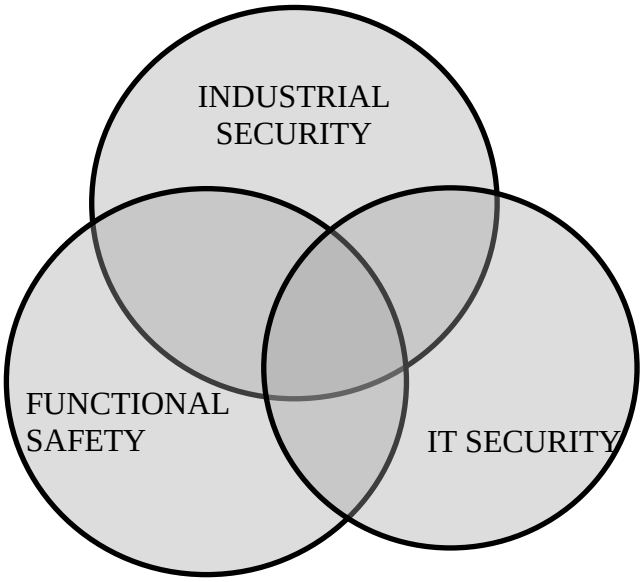


Figure 1. Disciplines concerning RTA CBCS cybersecurity

We are going to fuse different scientific fields to benefit from their best practices, while neither of these disciplines can independently meet the challenge. For example, functional safety considers unintended denial-of-service accidents, while leaving targeted threats out. Meanwhile, IT security is aimed at providing information integrity, availability, and confidentiality, which doesn't directly affect the rail traffic safety.

The main advantages of this approach include the ability to integrate cybersecurity into the existing RTA CBCS design, development and implementation processes without having to give up the proven approaches and solutions.

8 Sergey Gordeychik, Mission-centric approach to ICS/SCADA cybersecurity

RTA CBCS safety through cross-disciplines

Discipline	Addressed problems
Traffic safety	Safety requirements Required CBCS functionality
Functional safety and reliability theory	Risk analysis methodology Methods of safety proof Efficiency evaluation of protection tools
IT security	Threat modelling methodology Security analysis methodology Security processes, tools, and mechanisms Efficiency evaluation of protection tools

Defining tasks of CBCS cyber resilience via the disciplines of traffic safety, functional safety and IT security allows us to consider the industry context and evaluate the influence of negative impacts in terms of critical failures and reliability theory, which enables integration of cyber resilience processes into the existing traffic safety and transportation efficiency processes[9].

Let us use the IT security conceptual construct to have a better grip of CBCS cyber security regarding railway services.

[9] Valentin Gapanovich, Efim Rozenberg, Sergey Gordeychik, Signalling cyber security: the need for a mission-centric approach

Threat classification

The foundation for providing RTA cyber resilience is reasonable definition of threats that may lead to industry-essential risks. Let us define three main classes of RTA CBCS threats based on the corresponding loss expectancy:

1. Traffic safety incidents. Security implications directly affect the traffic security.

2. Loss of transportation productivity. Security implications reduce carrying and traffic capacities, as well as other transportation economic figures.

3. Other threats. Security implications do not affect traffic safety, but implicitly affect quantitative and qualitative characteristics of transportation processes, reliability, and security (Safety Integrity Level, Run-to-Failure, etc.).

Most dangerous threats involve violation of safety rules defined in railway operating rules, railroad signaling regulation, rail traffic safety instructions, and other ruling documents. Overspeeding on a curve, setting conflicting routes, changing station and wayside signals – these situations can be caused by cyber-attacks bypassing the existing rules and functional safety mechanisms.

Since information control systems are widely used to optimize the transportation process, interruption of CBCS normal operation can affect the efficiency. For example, collision avoidance systems supporting high-speed trains usually use a radio channel to transfer information between locomotives and the centralized traffic control center, as well as to send data on recommended speed, signal states and block sections along the road. Meanwhile, intrusion into the radio channel (e.g. ISM or GSM/GSM-R band countermeasures) will disable it and force the system to switch to three-aspect signaling, which limits speed to 160 km/h. It will adversely affect the section working capacity. In a number of European countries, the speed limit of 40 km/h or even complete stop is applied in case of radio channel failure; it concerns European Train Control Systems (ETCS) level 2 and 3 when track circuits are not used to transfer signaling information.

Transportation efficiency can be also reduced by cyber-attacks targeted at supporting systems such as ticketing, check-in, passenger-count and information systems. In November 2016, two thousand systems of San Francisco Municipal Railway (the so-called MUNI) were hacked. The attackers wanted 100 bitcoins (about $ 73 000) to undo the damage. As a result, MUNI ticket machines were disabled and the agency had to carry passengers for free during that day, while the IT team was working to resolve the situation. Beyond that, the ransomware encrypted administrator panels, CAD workstations, payment systems, SQL databases, terminals at lost-and-found offices, mail and print servers, the employees' workstations, and computers in ticketing cabins.

Cyber-attacks can degrade functional safety and reliability. If proper security mechanisms are not implemented, even general-purpose viruses will be able to affect the CBI elements, e.g. to decrease performance, to block or disable Windows-based yardmaster workstations. It shortens the run-to-failure time for yardmaster workstations and affects the overall CBI functional safety.

Let us consider the Wannacry worm attack in May 2017 as a simple refresher. The worm exploited vulnerability MS17-010 (EternalBlue) in Windows OS and encrypted data on the infected computers to obtain a ransom. According to a number of sources, the attack disabled several Russian Railways computers supporting the URAL train sheet application. Beyond that, a number of passenger information systems have failed at German railroad stations.

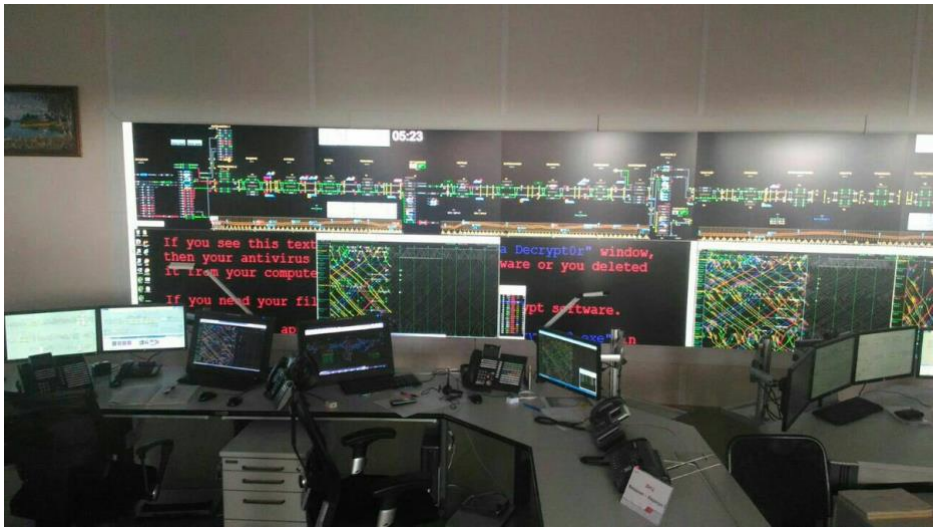


Figure 2. The result of Wannacry attack against railway systems

The mission-centric approach to threat classification considers the purposes of a process or a system to be protected as safety tasks; further policy is developed on the basis of these tasks. This approach allows developers of CBCS safety mechanisms to take into account a partial threat model and traffic safety and functional safety requirements applied to this class of systems.

An example of applying this approach to threats for improving RTA CBCS cyber resilience is given in section *CBCS Model and CBCS Threat Model*.

Attacker model

Today's complicated geopolitical situation and the evolution of cyber-attack methods force us to review the attacker models used for security analysis and protection development. Havex, a sophisticated cyber-attack carried out in 2014 enabled attackers to obtain unauthorized access to the websites of ICS vendors and to replace the software distribution packages available for download. As a result, malware was downloaded from the official vendor repository and was installed to ICS segments by unsuspecting authorized operators. It shows that man-induced threat sources (i.e. coordinated targeted attacks) are urgent today.

To consider man-induced threats, the intruder's capabilities are included into the attacker model. Here, it is reasonable to use the traditional classification:

- 1 - an external attacker who has no accessories in the organization;
- 2 - an internal attacker who is not a system user;
- 3 - an internal attacker who is a system user;
- 4 - an attacker engaging specialists who have developed and analyzed the target system;
- 5 - an attacker who works with research institutes that have developed and analyzed the system;
- 6 - foreign intelligence agencies.

Analysis of threats and vulnerabilities should assume maximal intruder capabilities. These attacker capabilities are defined by the following factors: motivation, qualification, technical features, methods and tools, and preconditions for threat activities

Maximal intruder capabilities

	Description
Motivation	At worst, an attack against the CBCS is conducted as act of terror or sabotage. In this case, the intruders represent a group from the cyber division of foreign armed forces or an international terrorist organization. These attackers are motivated both by their patriotic or religious feelings and high payments. At that, intruders can reckon on remote attack vectors (exploiting vulnerabilities in CBCS front-end or agents), which will protect them from the law enforcement authorities of the state-under-attack. Thus, an intruder is highly motivated to use all available means, while limiting factors such as human losses and criminal prosecution are not a problem.
Qualification	At worst, the intruders represent a group of high-skilled specialists who are able to detect both known and 0-day vulnerabilities. If necessary, they can engage outside experts who will even not know the real goal of investigation. For example, these experts can perform reverse engineering of separate source-code fragments and interaction protocols or develop exploits for certain vulnerabilities.

	Description
Technical features	The intruder can use both open-source and commercial software and hardware. Tools used to develop and conduct an attack can list as follows: ● software and hardware that are identical or analogous to those used in the CBCS; ● automated vulnerability detection tools (scanners, reverse-engineering tools, development and debugging facilities, etc.); ● network sniffing tools; ● password and username dictionaries, special-purpose software and computation capacity to brute-force passwords; ● exploits for known vulnerabilities.
Methods and tools	The intruder can use the following methods and techniques to detect and exploit vulnerabilities published in open and special-purpose sources: ● methods and techniques to detect typical code errors; ● methods and techniques to detect typical web application vulnerabilities; ● methods and techniques to analyze network protocols; ● methods and techniques to analyze password security; ● methods and techniques of cryptanalysis; ● methods and techniques to identify object code modifications introduced by software updates; ● methods and techniques of reverse engineering; ● methods and techniques to detect typical mistakes in information system design and operation.

	Description
Preconditions	The intruder can receive remote access to external CBCS interfaces where user authorization is not required. When accessing the system, the intruder is outside of the state-under-attack and can use anonymizing tools (proxy, TOR, botnets, rented computing facilities). The intruder can engage the employees of the target organization, its affiliated and service companies, software/hardware developers and vendors to take separate actions. At that, the employees may not understand the consequences of these actions and the real attacker's goal. Note: within this model, the intruder doesn't engage CBCS software developers, CBCS administrators and other employees who have more capabilities to obtain authorized access then the intruder. It is supposed that the employees act without explicit, willful and material security breaches and CBCS misuse.

As one can see from the model, intruders' level 4--6 have considerable capabilities. These data cannot be ignored, especially given the situation in railway services all over the world where foreign-developed systems are widely used.

2. Vulnerabilities of railway automation

Security assessments of RTA systems conducted in various regions of the world revealed multiple vulnerabilities in CBCSs and related subsystems used by railroad operators. This section reviews typical CBCS weaknesses and corresponding attack vectors. Since it usually takes rather long time to eliminate vulnerabilities from industrial automation systems, we will avoid describing the essential technical details of vulnerabilities according to the general practice of responsible disclosure[10]. This precaution is aimed to prevent malicious exploitation of the weaknesses.

In IT terms, CBCSs represent application systems. In IT security, such systems are decomposed into the following levels:

- Network level. Safety of communications between CBCS components, as well as between the CBCS and other systems.
- Operating system level. Safety features and vulnerabilities of the OS used by CBCS components.
- Data level. Safety of CBCS information during its storage, communication, and processing.
- Application level. Safety of automation of application tasks; security mechanisms implemented at the level of application system.
- Stuff level. Issues related to the human factor (here, humans are system developers, operators, administrators, etc.).

In this section, the focus is on technical vulnerabilities, i.e. defects of design, implementation and maintenance of software and hardware used by CBCSs and corresponding information systems. OS, data, and application levels are considered in the *Application level* section.

10 "Устранение уязвимостей в компьютерных системах: исследователь, владелец, пользователь", Гордейчик Сергей Владимирович, Доклад на VII Международной конференции «Право и Интернет», http://www.securitylab.ru/analytics/241826.php

Network Level

Network communications are an essential part of modern CBCSs and RTA systems. These are network communications that made it possible to widely introduce monitoring and supervisory control, to stop using track circuits for train localization and data communication in automatic block systems for high-speed trains, to computerize optimization of train schedule and ticketing.

At the same time, network technologies allow attackers to act remotely, i.e. without direct physical access to the target object, which enlarges the scope of possible intruders and complicates identification of the attackers and the attack source. If special-purpose protection tools are not implemented, then network attacks leave very few pieces of evidence for forensic investigation. These features motivate attackers of various levels, from criminal organizations to intelligence agencies of different countries to develop new methods of network penetration.

In view of the above, implementation of proper protection mechanisms for network communications is a primary measure to improve the RTA CBCS cyber resilience.

As a rule, the initial stages of any security assessment include analysis of interaction between the components of the system. In a modern railway control system, there are multiple levels of network communications: from internal interaction to public network connections. For example, Internet systems are used to provide information to the clients, to purchase tickets and transportation services, to provide infotainment, etc.

To classify communication systems, let us divide them into the following groups:

- **Local communication systems** are used within a certain CBCS to connect subsystems and components or local groups of systems. For example, a local communication system can be used to provide

interaction between an induction-motor control system, a driver information system, and a Computer-Based Interlocking System (CBIS).

- **Internetwork communication systems** are used to connect different CBCSs. For example, they can be used to provide interaction between several CBISs in one section or between a Centralized Traffic Control System (CTCS) and a Supervisory Control System (SCS).
    - *Wireless internetwork communication systems* do not require interaction points to be connected with wire. In RTA systems, wireless internetwork communication is widely used to provide interaction between moving objects such as trains and locomotives and trackside devices.
    - *Global (public) internetwork communication systems* access the Internet or other networks with unregulated number of users.

Systems of each group have their features in implementation, their specific vulnerabilities, and provide certain capabilities to attackers. Let us consider them in further detail.

Local Communications

Local communications are implemented within a certain CBCS or a certain group of CBCSs to transmit data between different subsystems and components. Local communications are included into CBCSs of all types, e.g. locomotive, station and line systems.

Local communications are usually implemented using either various buslines (such as HDLC, Canbus, and Profinet) or Ethernet-based technologies. In rare cases, local and personal wireless technologies are used, e.g. PAN solutions based on the IrDA standards or LAN solutions based on the 802.11 protocols. They usually choose wireless networks to connect mobile objects (e.g. cars of one train) or stationary but distant objects (e.g. CBI controllers and signals/switches).

In the systems that do not directly affect the traffic safety, the TCP/IP protocol stack is often used with Ethernet as the link-layer protocol. Among such

systems are CTCSs, SCSs, passenger information systems at the stations, and ticketing systems.

Let us consider local CBI communications by the example of the system Ebilock 950[11].

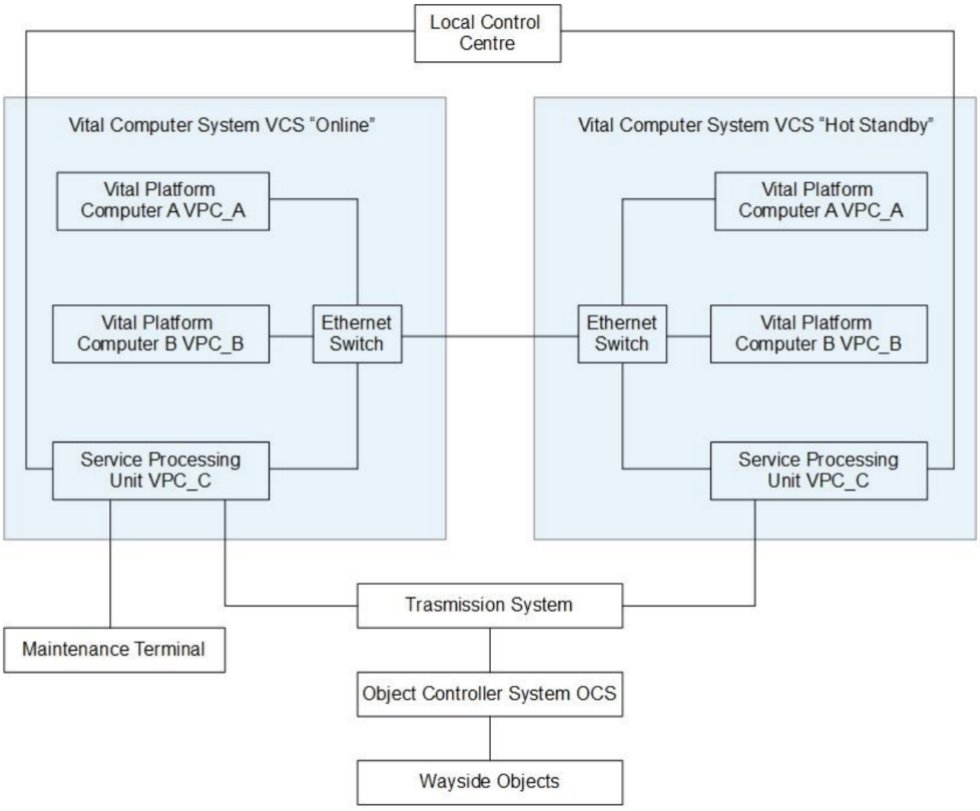


Figure 3. CBI block diagram

The system involves three type of local communications: an asynchronous serial channel UART (Universal Asynchronous Receiver/Transmitter) using the RS-232 interface; current loops based on the HDLC (High-Level Data Link Control) protocol using the RS-422 interface; a local Ethernet network.

[11] Houshang Kheiri Sadigh, CITYFLO 350 Signaling System. Interface between ATP Telegrams and Brake curve. Istanbul new Metro Line Study case https://web.uniroma1.it/cdaingtrasporti/sites/default/files/Thesis_Kheiri_MTRR_29ott18.pdf

The UART (RS-232) and HDLC (RS-422) protocols are used to provide interaction between the central processor modules and communication modules (communication hubs), as well as to send commands and receive diagnostics information from object controllers.

Regarding safety issues, the UART and HDLC protocols do not implement any protection mechanisms. Consequently, an attacker obtains an opportunity to intercept the information being transmitted and inject malicious commands. Since these protocols provide interaction with controllers, an attacker can inject safety-related commands bypassing the interlocking logic. It is possible, because the central processor solely implements the interlocking logic, while the controllers receive only the final instructions. Object controllers do not implement additional functions of command analysis; in fact, they are merely computer-based relays that operate switches or power certain traffic-light lamps depending on the commands received from the central processor.

As a result, an attacker who can modify bus-wire data and inject specially crafted commands will be able to control trackside devices, inject safety-related commands and falsify diagnostics data such as the switch status. However, an important restriction for an attacker is the necessity to connect to the HDLC bus, which requires physical interaction with the corresponding hardware or communication channels. In other words, to conduct an attack, the intruder must attach a special-purpose device to the cable between communication modules and object controllers or use a cable break to tap into. These cables lay in electrical signal towers or along the tracks (if object controllers are situated in the yard neck), so the described attacks are not CBI-specific. An attacker can change the immediate switch or signal commutation just as well. However, if Ethernet is used to communicate with object controllers, then the attacker's opportunities considerably increase.

If the CBI network is integrated into the station Local Area Network (LAN) with a more complex network topology, then the system inherits all known

Ethernet vulnerabilities. It enables an attacker to apply tools and methods widely used against the enterprise local networks. An important feature of these attacks is the opportunity to use not only physical connection, but also almost any compromised host in the station network. To develop an attack, an intruder can use the yardmaster workstation, the signal technician workstation, the central processor, and even network equipment such as modems, switches, and routers.

The most common attacks are:

- Attacks against the data-link service protocols and network resilience mechanisms such as Spanning Tree Protocol (STP), Dynamic Trunking Protocol (DTP), Hot Standby Router Protocol (HSRP), 802.1Q и VLAN Trunking Protocol (VTP), and Local Link Discovery Protocol (LLDP).
- Attacks against the protocols of name and address resolution such as Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Bootstrap Protocol (BOOTP).
- Attacks against the application-layer service protocols such as Web Proxy Auto-Discovery (WPAD)[12], NetBIOS, and SMB.

These attacks have been described in details by many authors and are implemented in various utilities such as Yersinia[13], Cain & Abel[14], and Intercepter-ng[15].

As an example, let us consider an ARP Spoofing attack. ARP is used to map MAC addresses of Network Interface Controllers (NICs) and IP addresses of the corresponding devices in a local network segment. To start IP communication, a device sends a broadcast ARP request to be answered by the host with the requested IP address. If the response is received, then communication is possible. Further, the devices insert the corresponding entries into their ARP mapping tables and use them to generate data-link core headers.

12 WPAD Name Collision Vulnerability, https://www.us-cert.gov/ncas/alerts/TA16-144A

13 Yersinia for Layer 2 – Vulnerability Analysis & DHCP Starvation, http://kalilinuxtutorials.com/yersinia/

14 Cain & Abel tool, Official Site, http://www.oxid.it/cain.html

15 Intercepter-ng, Official Site, http://sniff.su/

Since ARP communications do not involve authorization, an attacker can intercept a broadcast ARP request and send a specially-crafted ARP response. Thus, the attacker's MAC address is associated with the IP address of another host, e.g. a router.

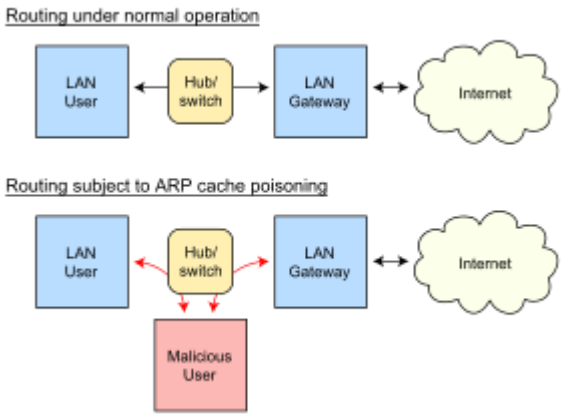


Figure 4. ARP Spoofing attack

As one can see from above, an attacker can now intercept, modify, and block traffic between any local network hosts. An attacker can block interaction between different systems by receiving but not forwarding data to the real destination host. This situation can also raise casually in case of a failure during the attack. Most of the above-listed attacks provide a malicious person with similar capabilities; these are only the details of attack process and applicability in different situations that vary.

As to the practical results for intruders, a successful attack will allow them to:

- intercept and modify authentication protocol data such as NTLM (Windows passwords for yardmaster and signal technician workstations), Telnet, and SSH (passwords for remote access to the central processor);
- conduct attacks of authentication session relay (NTLM Relay or Pass-the-Hash[16]) aimed to access network resources without passwords recovery;
- intercept and modify application protocol traffic, e.g. information about train positions sent from the central processor to the yardmaster

16 Pass the hash, https://en.wikipedia.org/wiki/Pass_the_hash

workstation, diagnostics data sent to the signal technician workstation, or commands sent from different workstations, CTCSs and SCSs to the central processor.

Most of the investigated CBI systems used special-purpose data-link protocols to provide interaction between workstations, CTCSs and SCSs without implementing source authentication and data integrity control mechanisms. Taking into account the opportunities for man-in-the-middle attacks, a malicious person who has local or remote access to the CBI network is able to:

- spoof commands to operate switches and shunting, entrance, or exit signals;
- send false train information (e.g. signal states and track occupancy) to the yardmaster workstation;
- send false diagnostics information about switch and signal states to the yardmaster workstation (e.g. a false lamp open-circuit alert).

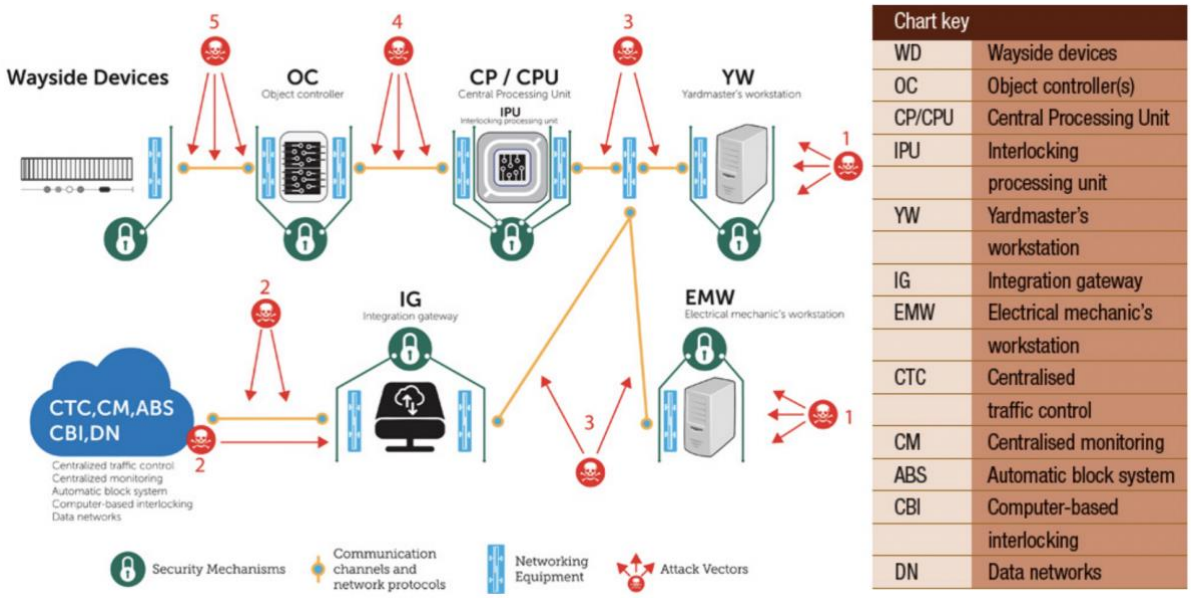


Figure 5. Vector 3 - Spoofing of commands and diagnostics data in a local network

Successful attacks against local communication channels often allow an intruder to proceed with more complex threats. For example, the author once analyzed a computer-based marshaling yard interlocking system, in which initialization of system modules involved remote operating system loading via

the BOOTP/TFTP protocol using Preboot eXecution Environment (PXE). In this case, an attacker who has remote access to the local network will be able to gain full control over the CBCS. To do so, an attacker can use the following algorithm:

- Analyze network traffic and discover the TFTP-server IP address and the names of operating system images.
- Load operating system images from the TFTP server and modify them as necessary.
- Intercept a broadcast request from a host being initialized and send a specially-crafted BOOTP response specifying the address of the malicious TFTP server .
- The host being initialized will download and execute the specially-crafted malicious operating system image.

Vulnerabilities of local network protocols usually do not allow an attacker to implement traffic safety threats (e.g. to operate a switch with a train passing over it or to set conflicting routes). It is the CPU that performs security checks of commands and implements the interlocking logic; that's why a specially-crafted command sent from the yardmaster workstation and aimed to violate traffic safety will by simply rejected. However, communication channels between the CPU and object controllers or operating devices provide an attacker with such opportunities.

Nevertheless, even spoofing of commands that do not directly affect the traffic safety (e.g. setting the entrance signal to red light instead of green one) combined with opportunities to display false train information on the yardmaster workstation allow an attacker to degrade the train-handling capacity and weaken the transportation economic efficiency.

In some cases, an intruder can exploit advanced CBI features aimed to support off-design operation. In some systems, the mechanisms of route canceling combined with execution of safety-related commands allow an attacker to operate a switch with a car passing over it.

Local communications of locomotive CBCSs are poorly regulated. Depending on vendors, railway systems and trains, a wide variety of technologies can be used such as Train Communication Network, CANBus, CANopen, WorldFIP, LonWorks, and Profibus. Nowadays, high-speed Ethernet Train Backbones (ETB) with Ethernet Consist Networks (ECN) based on IEC61375-2-5 and IEC 61375-3-4 standards are gaining currency.

Let us consider implementation of local communications by the example of Siemens Velaro E[17] platform.

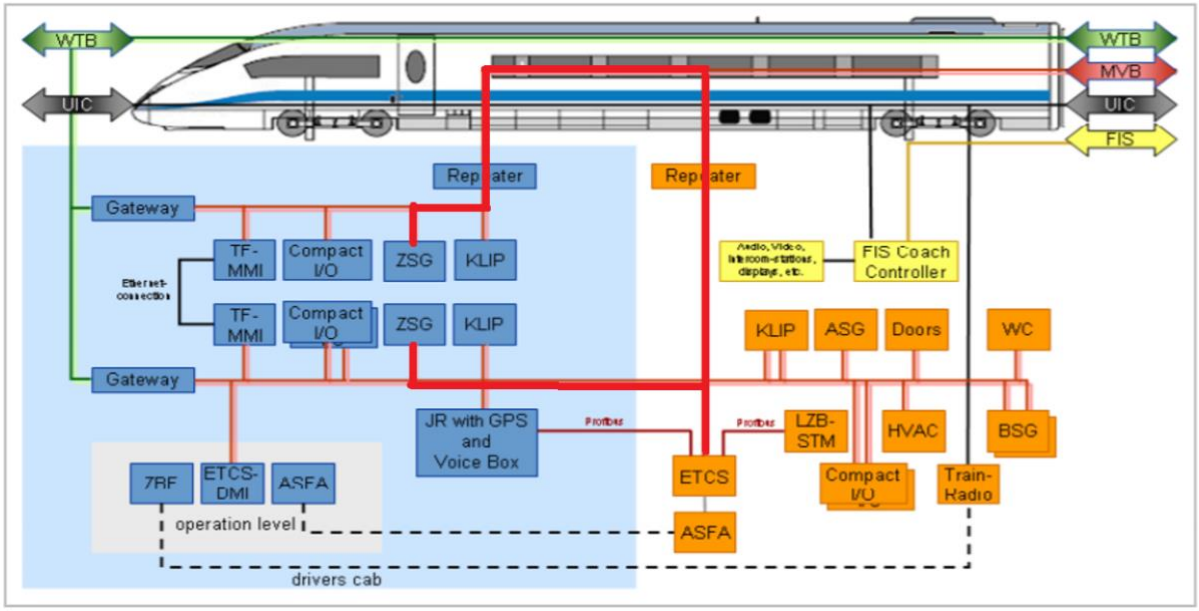


Figure 6. Block diagram of interaction between locomotive CBCSs by the example of Velaro E

Interaction between different CBCSs is implemented via a Train Communication Network (TCN), which is described in IEC 61375. TCN represents a two-level communication network with hierarchy structure. The network consists of a Wired Train Bus (WTB) used to connect several cars and a Multifunction Vehicle Bus (MVB) used to provide communications within a

17 "Solutions for High Speed Trains for future demands in Europe and Asia", Christian Schlegel, http://uic.org/cdrom/2006/wcrr2006/pdf/292.pdf

locomotive or a car. Passenger information and infotainment services are provided by a separate network.

At the physical layer, WTB uses a duplicated shielded twisted pair RS-485 with the rate of 1 Mbps. At the data-link layer, High-level Data Link Control (HDLC) is used.

In MVB, the physical layer is implemented with: (i) Optical Glass Fibres (OGF) up to 2000 meters long, (ii) RS-485 shielded twisted pairs Electrical Medium (EMD) up to 200 meters long and (iii) simplified connections without galvanic isolation Electrical Short Distance (ESD) up to 20 meters long.

As one can see from above, MVB provides communications between safety-related CBCSs such as brake control systems (Announcement of Signals and Automatic Braking, ASFA[18]), driver awareness systems (European Train Control System — Driver Machine Interface, ETCS-DMI), drive control units (ASG), and central control units (ZSG). Besides that, some supporting systems are also connected to this bus, e.g. ventilation and conditioning systems (Heat Ventilation and Air Conditioning, HVAC) and door control systems (Door).

In MVB topology, the Master-Slave principle is applied: one of the devices serves as the Bus Administrator. The Master performs time synchronization, address checking, collision prevention and resolution. The Master regularly issues a General Event Poll[19] frame; the Slaves can answer it with an Event Identifier Response containing the event identifier and thus notify the Master there are data to transmit. In this case, the Master issues an Event Read request and the Slave sends back the available data, which can be read and used by other bus devices. If several devices answer the General Event Poll request, then a collision occurs.

18 «Automatic Braking and Announcement of Signals», https://en.wikipedia.org/wiki/Anuncio_de_Se%C3%B1ales_y_Frenado_Autom%C3%A1tico

19 «Train Communication Network IEC 61375 – 3, Multifunction Vehicle Bus", http://lamspeople.epfl.ch/kirrmann/Pubs/TCN/IEC61375-3-MVB.ppt

The Master resolves it by performing group polling first (before the collision occurs) and communicating with every group device separately after that.

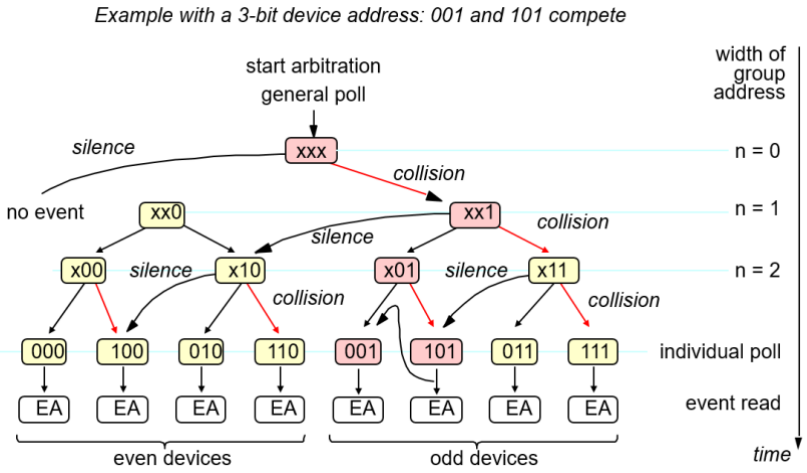


Figure 7. MVB collision resolution

MVB implementation provides high availability but lacks security mechanisms such as authentication and integrity control. Nevertheless, experiments show that an attacker will hardly benefit from frame injection and spoofing, since communication is sensitive to delays and collisions. However, an approach was proposed[20] to demonstrate practical attacks using one of the failure-safety mechanisms (mastership transfer namely).

MVB is designed to support several Bus Administrator devices at a time; however, only one of these devices can serve as the Master. Any device can apply for this role when being registered in the network. To do so, the device sets the BA (Bus Administrator) flag in the response to the current Master's request. The Master updates its Bus Administrator List; every four seconds, it asks the devices from this List to take the Master token. If the current Master becomes unavailable, the arbitration process is initiated. One of the Bus Administrators becomes the new Master and creates a Master token to be transferred to another Bus Administrators after a while.

20 "Abusing the Train Communication Network or What could have derailed the Northeast Regional #188?", Moshe Zioni, https://www.slideshare.net/moshez/abusing-the-train-communication-network-or-what-could-have-derailed-the-northeast-regional-188

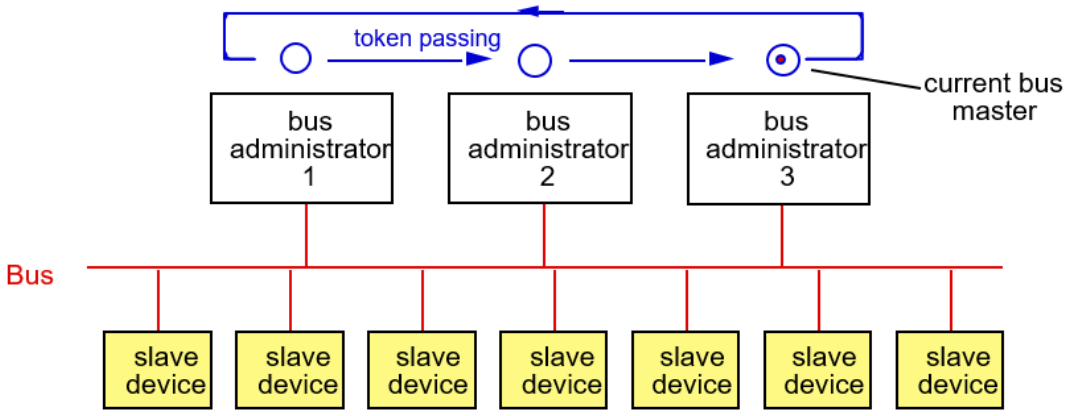


Figure 8. The mechanism of MVB Master change

To conduct an attack, a malicious person first connects a sniffer to the network. By analyzing the Slaves' responses, the attacker understands the addressing scheme (MVB uses a standard mechanism to generate the Device List) and selects an unoccupied address with the least value. The malicious device then waits for a Device Status request from the current Master and identifies itself with the BA flag set to 1. Thus, the malicious device becomes a Bus Administrator. Now it can wait for a mastership-transfer request and become a new Master. This role will allow an attacker to bypass the network logic and inject specially-crafted frames into traffic.

WTB networks are prone to similar mastership hijacking attacks[21], since they also use the Master-Slave mechanism. When the system launches, the first device that detects there is no traffic in the network becomes a Master. Now this device is to control addressing and communication processes. However, the protocol implements a so-called fast inaugurate mechanism to change Masters. Any device can claim to become a new Maser. When a new Master is being selected, the most likely segment (a range of devices connected to the WTB) to

21 «The Great Train Robbery: Fast and furious», Sergey Sidorov, https://www.slideshare.net/SergeyGordeychik/the-great-train-robbery-fast-and-furious

win is the one containing the maximal number of hosts. Thus, a malicious device can apply for mastership by claiming to have the largest number of hosts in its segment.

However, this attack has significant restrictions, thanks to a master conflict resolution mechanism implemented in the protocol. This mechanism involves addressing the application and, in some cases, even requires operator intervention. For example, this mechanism is used when two locomotives are connected to one WTB and it is necessary to decide which one will be pilot, and which one will be rear-coupled. If it fails to resolve the conflict, then the bus is divided into several segments, each controlled by its own Master.

In such a manner, the described attack against WTB can be identified and prevented by an operator; even if the attacker succeeds (depending on application implementation), the only result will consist in network segmentation with no benefits for the intruder.

To provide local communications between locomotive CBCSs, Controller Area Network (CAN bus, CANopen) is often used. CAN vulnerabilities and methods to exploit them are well elaborated[22], because this technology is also widely used in automotive industry. The main weakness is the lack of forgery protection, which allows a malicious device to gain control over network communications.

Ethernet Train Backbones (ETBs) with Ethernet Consist Networks (ECNs) provide a high rate (100 Mbps and more) and support a wide range of applications including real-time video and audio transmission. These applications can use both standard TCP/IP protocols and special-purpose protocols such as the Train Real Time Data Protocol (TRDP).

Regarding network topology, different CBCSs within one car are included into a broadcast Ethernet segment (Consist Network). Consist Networks are in

22 «Car Hacker's Handbook», OpenGarages, http://opengarages.org/handbook/

turn united via Network Nodes (EBTN) into Consist Units. At that, segments are connected successively, which makes the network topology easier to understand.

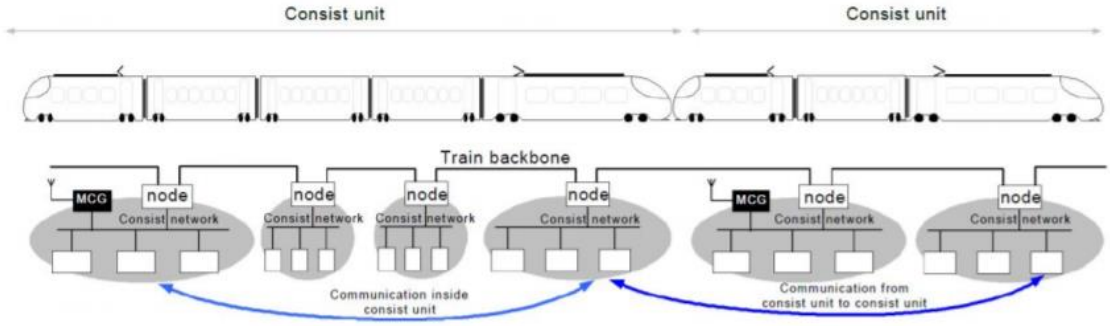


Figure 9. ETB topology and Ethernet Consist Networks

As for safety, ETBs are prone to all above-mentioned data-link attacks typical for Ethernet networks and the TCP/IP stack. Besides that, there are ETB-specific vulnerabilities. Let us consider the Train Topology Discovery Protocol (TTDP), which is used to control IP addressing and Network Address Translation (NAT) within train cars. TTDP defines two main types of Ethernet frames. A service frame HELLO uses the source MAC address as the main information and is sent to an adjacent EBTN to determine whether communication is possible. Once the system is on, every EBTN checks the communication channel state and, if possible, starts sending HELLO frames to receive responses from adjacent devices. If a response is received, the device switches to the inauguration mode.

To generate a network topology table, the second frame type is used, TOPOLOGY. These frames transmit the entire list of all identified MAC addresses. At that, every EBTN has right and left network interfaces in accordance with the physical topology. If a TOPOLOGY frame is received on the right interface, then the EBTN supplies this frame with already known MAC addresses and transfers it to the left interface (and also the other way around). This process stops when the topology lists on all devices coincide. After that, the topology is fixed, and IP addresses are assigned according to the car order.

The only mechanism of authorization and integrity control implemented for TOPOLOGY frames is the checksum. Therefore, a compromised EBTN can modify frames passing through, add false hosts and delete already identified hosts from the topology table. These activities allow an attacker to impose a false network topology and cause a denial of service by forcing a topology table overflow or preventing the inauguration process from termination.

TTDP includes a mechanism that can reduce the efficiency of these attacks. According to the standard, it is the operator who decides whether to terminate the inauguration process at the stage of topology generation. Similarly, the protocol requires operator intervention if the topology changes after inauguration (e.g. a device becomes degraded). However, not many devices implement the protocol properly in real life, which allows the topology table to be (re)generated without human involvement.

An application-layer Train Real Time Data Protocol (TRDP) runs over TCP/IP and usually uses two ports: 17224/UDP for Process Data (PD) sub-protocol and 17225/UDP or TCP for Message Data (MD) subprotocol.

The packet headers in both sub-protocols contain a Sequence Counter field to be checked by the receiver.

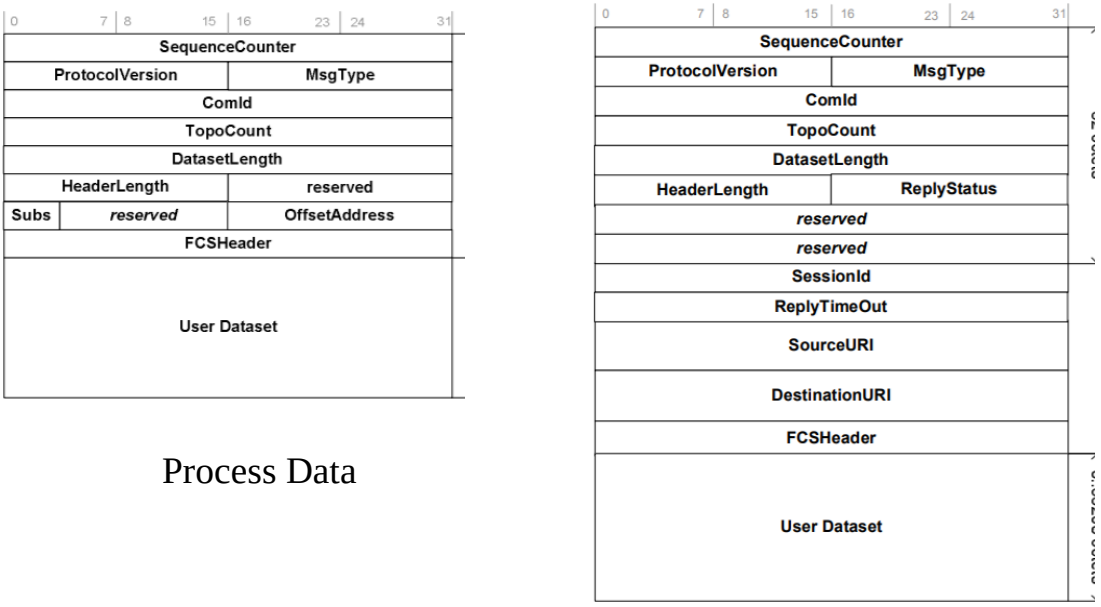


Figure 10. TRDP packet format

This field could be used to implement additional protection against Frame Forgery and Session Hijacking, but specification defines this field to be initiated with zero value and to be incremented with every packet sent. Thus, a malicious user who even doesn't have opportunities to intercept packets and obtain session data from them is nevertheless able to guess the current Sequence Counter value and inject false data. It should be mentioned though that if TDRP Message Data uses TCP with proper randomization of the Initial Sequence Number, the above-described attack is hardly implementable.

TDRP uses the TRDP Safe Data Transmission mode to transmit critical dat. In this mode, an extra 32-bit header containing the Safety Message Identifier is added to the packet. Furthermore, the packet is supplied with a checksum CRC32, which is however by no means an effective mechanism to prevent packet forgery. As of the Safety Message Identifier, there is no available data on its generation algorithm, so it is impossible to estimate the efficiency of forgery protection provided.

Internetwork Communications

Internetwork communications are used to connect different CBCSs. For example, they provide communication between CBI systems of one district and connection with CTCSs and SCSs. In this paper, we also consider local wireless communications to be internetwork. From the safety viewpoint, this assumption is reasonable enough, because wireless networks can be attacked from outside the physical security perimeter. For example, if amplifiers and directional antennas are used, then 802.11-standard networks can be attacked from a source located several kilometers away. This distance is much longer than the coverage area dimensions defined as tens of meters at the stage of network design.

Physical access to the carrier is free, which enlarges the scope of possible intruders and complicates their identification for forensics purposes.

Network equipment used to provide operation of communication channels can serve as an attack vector for possible intruders. Modern network equipment usually represents a complex hardware and software system based on a common or a special-purpose OS and provides rich features of remote control.

Sergey Pavlov in his report on Network Infrastructure Security Assessment described the most common vulnerabilities that can be found in IP-based communication networks. These are:

- default passwords to access management interfaces (SNMP, Telnet, SSH, Web);
- errors in configurations of network devices;
- lack of security updates.

Default passwords to management interfaces represent a well-known problem and administrators usually try to reset them regularly. However, service protocol passwords (e.g. SNMP) that are used for machine-to-machine interaction often contain default strings (private, pubic, etc.). Meanwhile, these interfaces provide powerful capabilities. For example, Cisco network devices operating under Cisco IOS allow one to download a device configuration from a TFTP server via SNMP.

If successful, an attacker becomes able to change settings and configuration parameters, redirect traffic (using command *debug ip packet*), configure remote access to the network using VPN technologies such as PPTP, GRE, L2TP, etc.

In some cases, SNMP implementation contains errors that allow one to obtain sensitive information using minimal privileges. For example, a weakness was revealed in a number of H3C and Huawei devices[23] that allows an attacker to obtain user passwords using *public* privileges. Further, the obtained passwords can be used to gain full control over the network device

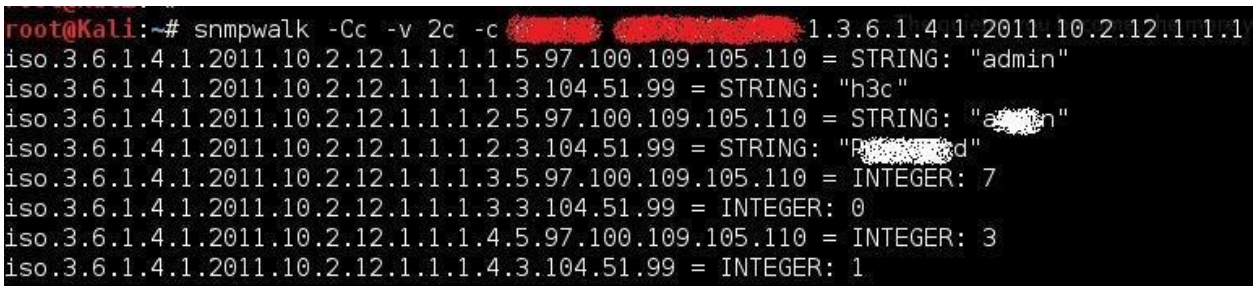


Figure 11. Obtaining an administrator password on HP/H3C and Huawei devices via SNMP

Some Cisco network devices also contain buffer overflow vulnerabilities CVE-2016-6367 and CVE-2016-6366[24] named EPICBANANA and EXTRABACON. These vulnerabilities allow an attacker to execute arbitrary code on Cisco ASA, PIX, and Firewall Services Modules serving as firewalls. Moreover, there is a ready-to-use exploit for these weaknesses, which makes an attack available for any malicious person.

23 Прокачай SNMP на устройствах Huawei и H3C, Евгений Строев, https://habrahabr.ru/company/pt/blog/247355/

24 The Shadow Brokers EPICBANANA and EXTRABACON Exploits, Omar Santos, https://blogs.cisco.com/security/shadow-brokers

Figure 12. Setting an empty administrator password on a Cisco firewall using an SNMP vulnerability

Analogous attacks can be conducted using the ROCEM vulnerability (CVE-2017-3881)[25] in implementation of Cisco Cluster Management Protocol (CMP) in a number of Cisco Catalyst switches.

25 CVE-2017-3881 Cisco Catalyst RCE Proof-Of-Concept, Artem Kondratenko, https://artkond.com/2017/04/10/cisco-catalyst-remote-code-execution/

```
$ python c2960-lanbasek9-m-12.2.55.se11.py 192.168.88.10 --set
[+] Connection OK
[+] Recieved bytes from telnet service: '\xff\xfb\x01\xff\xfb\x03\xff\xfd\x18\xff\xfd\x1f'
[+] Sending cluster option
[+] Setting credless privilege 15 authentication
[+] All done
$ telnet 192.168.88.10
Trying 192.168.88.10...
Connected to 192.168.88.10.
Escape character is '^]'.

catalyst1#show priv
Current privilege level is 15
catalyst1#show ver
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(55)SE11, RELEASE SOFTWARE (fc3)
```

Figure 13. Obtaining remote access to a Cisco switch via an SNMP vulnerability

As one can see, all vulnerabilities revealed in network equipment should be eliminated on a regular basis.

Moreover, special-purpose network devices used in industrial automation systems can also have various weaknesses.

Figure 14. Multifunction locomotive network device Netmodule NB3701

For example, it was reported[26] that a number of network devices by such vendors as Netmodule, Bintec elmeg, Digi, Moxa, and Sierra Wireless contain

26 The Great Train Cyber Robbery, Sergey Gordeychik, Alexander Timorin Gleb Gritsai. http://scadastrangelove.blogspot.com/2015/12/32c3-slides.html

default engineer passwords, fixed keys for encrypted control protocols (SSH/HTTPS) and web interface vulnerabilities that allow an attacker to execute arbitrary code in the system or change device configuration.

```
----------

Dear customer,

Due to recent software updates and deviating
from the information in the user manual there
are two possible combinations of the default
administrator password:

   User name: admin
   Password: funkwerk

or

   User name: admin
   Password: admin
```

Figure 15. Information about default values of network equipment credentials

This information was first provided to the vendors, so that they could develop patches before vulnerabilities are publicly reported.

```
    <form id="pingForm">
        <div class="pingHost">Host IP/DNS : <input name="host" type="text" /></div>
        <div class="pingNow">
          <input class="fbtn" type="submit" value="Ping Now" />
        </div>
        <div style="clear:both"></div>
    </form>

if [ "$FORM_host" != "" ]; then
    ping -c 5 "$FORM_host"
fi
```

Figure 16. OS command injection vulnerability in web control module for network equipment

Unfortunately, experience has shown that security updates are being rarely installed in industrial systems. It allows an attacker to exploit well known vulnerabilities that have been already fixes by vendors. Meanwhile, most network devices support wireless communications, which expands opportunities for an attack even more (this problem is considered further in the article).

An effective solution to prevent exploitation of such vulnerabilities is to divide a control segment and a data segment. In this case, an attacker who accessed the data segment will not be able to exploit vulnerabilities in control interfaces of network devices, because they are located in a logically or even physically separated network.

However, even proper design and implementation of such network segmentation loses its efficiency after a while in real-life environments. The case is that modern networks represent complex systems with topology that is variable, because dynamic routing protocols (BGP, OSPF) are used and administrators can modify device configurations to perform process tasks. In real-life networks you can often find test devices and settings that have been introduced to try some technology or complete some tasks for the purposes of a certain project and then were not removed. A widespread situation is when a contractor asks to temporary switch off filtering rules on a firewall to deploy an automated system. If these rules are not reactivated after works completion, then the firewall will fail to provide protection and will become a simple router.

To prevent such situations, it is recommended to use security analysis tools such as security scanners. They allow one to identify unauthorized use of control protocols in a data network (black-box and pen-test modes) and control modification and introduction of critical parameters in network equipment configurations (white-box and audit modes).

More progressive products are represented with systems that discover network topology by analyzing routing and filtration rules implemented in routers and switches. Some systems use the mechanisms of passive traffic analysis based

on packet interception or network equipment logs collection. These features allow administrators to analyze and optimize information flows with respect to various systems and applications.

To conclude, the safety of internetwork communications is an important part of RTA CBCS safety. It is necessary to provide it to ensure a sufficient security level of the whole system.

Wireless and Global Communications

Development of high-speed trains and Communication Based Train Control (CBTC) technologies lead to wide introduction of wireless communications into railway services. These communications do not require the interacting points to be connected with wires and are used in RTA systems to transmit information between moving objects (locomotives and cars) and trackside devices.

It is notable that wireless communications are often used together with public networks such as the Internet or other networks with unknown number of users. A widespread example of such combination is represented with Passenger Entertainment Systems that allow passenger to access the news and video content. These systems usually provide broadband access to the Internet for the passengers' devices, including those supporting Wi-Fi.

Internet access is often combined with Passenger Information Systems (PAS/PIS) at the network layer. In this case, vulnerabilities of a wireless access point allow an attacker to gain unauthorized access to information systems and more critical locomotive CBCSs or even trackside devices.

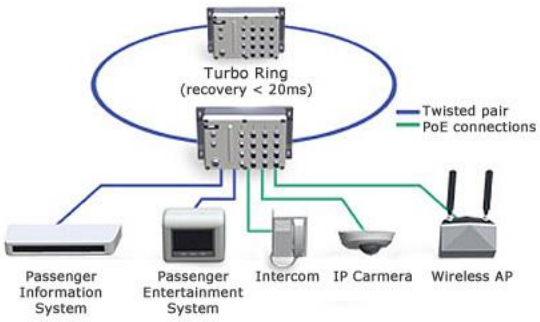


Figure 17. Wireless access and PAS/PIS (www.sphinxcomputer.de)

For example, when one wireless network is used both to provide passenger access and to communicate telemetric data with trackside devices[27], an attacker can gain unauthorized access to the wireless router and then use the obtained parameters (such as APN) or exploit network-layer vulnerabilities to access other locomotive devices or the Radio Block Centre (RBC, provides interaction with automatic blocking and CBI systems).

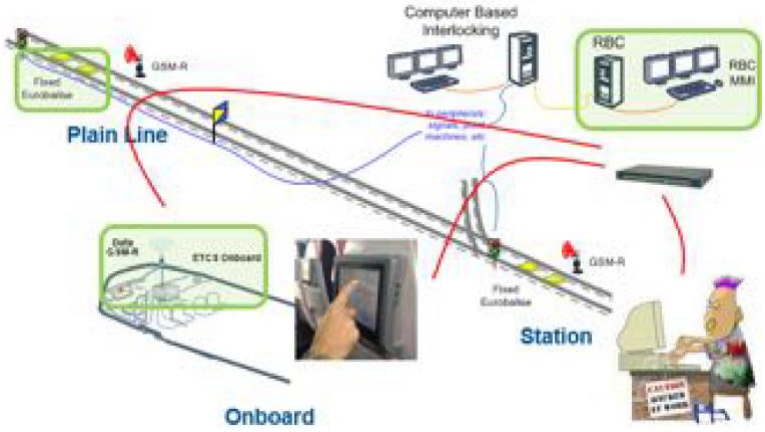


Figure 18. Attacks via PAS/PIS

These attacks usually require access to the wireless network deployed aboard, but sometimes certain elements of Passenger Entertainment Systems are available from the Internet and can be identified by an attacker using Open Source Intelligence (OSINT) methods. An expert in network devices can analyze

27 Power of Community, "The Great Train Cyber Robbery", Gleb Gritsai, Sergey Gordeychik, http://www.powerofcommunity.net/poc2016/gleb.pdf

addressing, domain names and even use search engines to detect control interfaces.

Figure 19. Identifying an Internet interface of a Passenger Information System using Google

A local wireless network can be used as a Wireless Ethernet Train Backbone to provide interaction between the cars of one train. This approach sufficiently simplifies the process of making trains up, but also raises a number of safety issues. The problem is that 802.11 (Wi-Fi) wireless networks have a rich vulnerability background and attacks against them are well developed[28].

28 Wireless Security, SV Gordeychik, VV Dubrovin

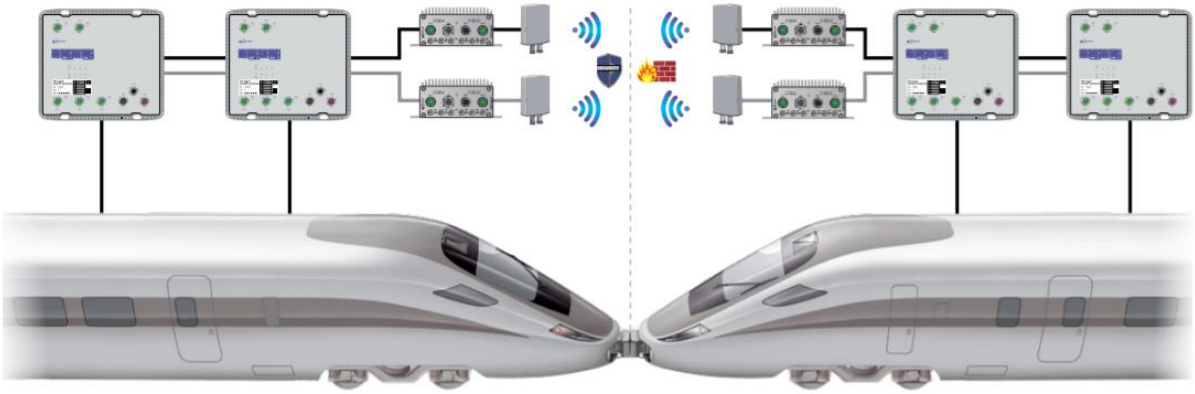


Figure 20. Using WLAN as a Selectron Wireless Ethernet Train Backbone

A usual problem of wireless network application is authentication parameter control. In most cases, WPA-PSK or WPA2-PSK[29] protocols are used to provide security. In these protocols, a pre-shared key (PSK) is used to perform authentication and generate a session key, which means that an attacker can intercept an authentication session and find the PSK value using *aircrack-ng* and *cowpatty*[30] utilities. Further, the obtained key can be used to access the wireless network. In most systems, PSK value changes rarely, which is an important benefit for an attacker.

In some cases, public wireless networks are used to directly address the CBI system. The examples are Driver Information Systems and Automatic Train Operation Systems[31].

29Selectron Wireless Ethernet Train Backbone, http://www.selectron.ch/selectron-wAssets/docs/flyer/en/Flyer-Wireless-Ethernet-Train-Backbone_EN.pdf

30 Cracking WPA2-PSK Passwords with Cowpatty, https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-with-cowpatty-0148423/

31 Automatic Train Operation Systems, Tikhonov DA.

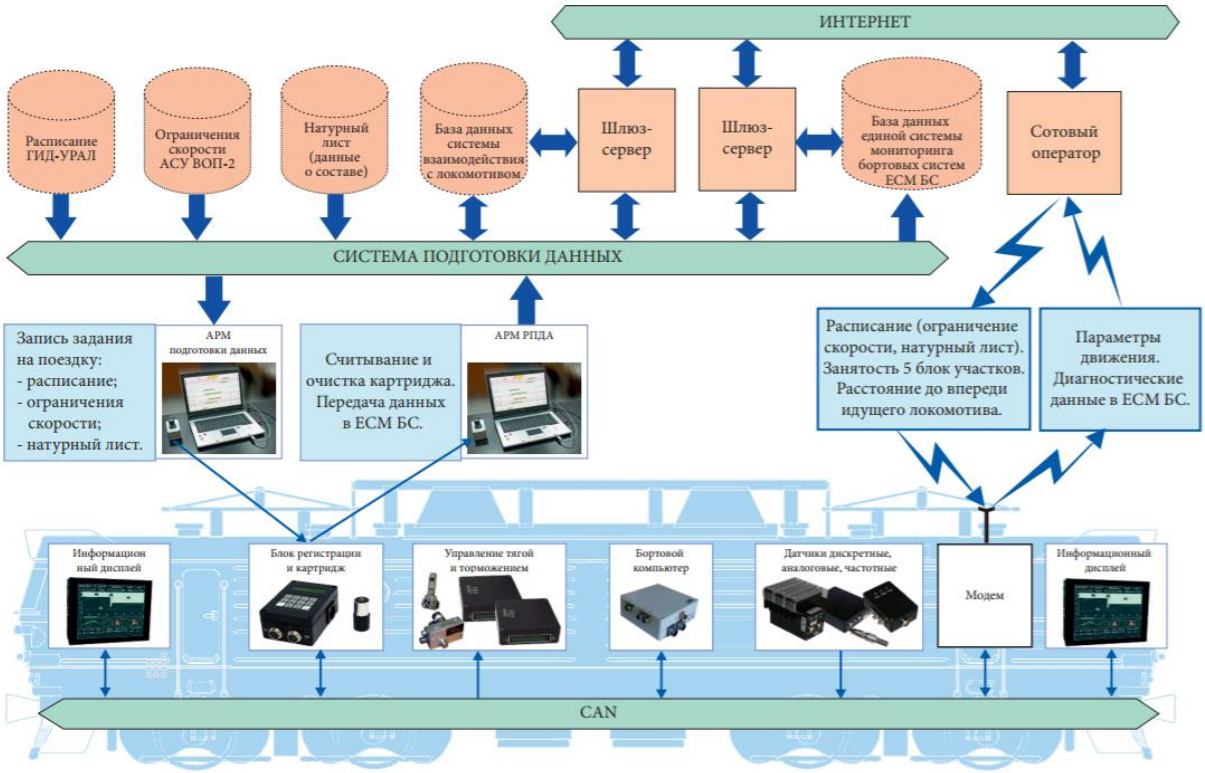


Figure 21. Block diagram of the Unified System of Automatic Local Train Operation

As one can see from the information flow chart, interaction with the locomotive CBCS is implemented through a wireless mobile communications network, which in turn provides access to the Internet. In fact, the information required to calculate the optimal train speed (i.e. speed limit, consignor list, occupancy of block sections, distance to the next locomotive) is published on an Internet server to be downloaded by locomotive systems. At that, interaction between the modem connected to the Internet and other locomotive CBCSs such as information displays, pick up units, and on-board computer is implemented via a CAN bus.

If such architecture is used, then even greater attention should be paid to the safety issues, since the attacker's capabilities considerably increase.

Vulnerabilities of cellular networks have been highly researched. Various components of cellular communications can be successfully attacked using revealed vulnerabilities.

Vulnerabilities of A5 encryption protocols that are used in GSM/2G allow malicious users to conduct active and passive attacks aimed at traffic interception. In active attacks, a false base station is used, and encryption is disabled by forcing mobile equipment to use the A5/0 protocol. This mechanism is implemented in various IMSI catchers, which are widely used by law-enforcement agencies. However, such devices can be also developed using available hardware and software such as OpenBTS[32].

Passive attacks against A5/1 and A5/2 encryption protocols used in 2G networks are also easy to conduct. An open-source utility set Kraken[33] allows one to perform a precomputation attack, which makes the time of intercepted data decryption realistic enough.

To attack advanced protocols used in 3G and 4G networks, one can use a man-in-the-middle method involving femtocells. A femtocell is a small portable cellular base station. A femtocell implements its own radio interface and transmits information to the operator network via an encrypted channel over the Internet (IPSec is usually used). A number of researchers showed[34] that it is possible to compromise a femtocell and access its OS to intercept and modify voice calls and data sent by the device. The attack has restrictions, since an attacker must stay within a radius of several tens of meters from the target system and be capable to switch the locomotive modem to the malicious base station. It makes an attack against a moving locomotive hardly possible. However, the restrictions are lifted when a locomotive stop over a station.

32 Base Station Security Experiments Using USRP, Retterstøl, Torjus Bryne, https://brage.bibsys.no/xmlui/handle/11250/2359801

33 Breaking GSM phone privacy, Karsten Nohl, https://srlabs.de/bites/decrypting-gsm/

34 Adventures in Femtoland, Alexey Osipov, Alexander Zaitsev, https://www.slideshare.net/arbitrarycode/adventures-in-femtoland-350-yuan-for-invaluable-fun

Another attack vector is provided by network-layer and application-layer vulnerabilities. It is a rather usual situation when locomotive devices exchange information with a station system through the Internet, accessing it via GPRS or high-speed analogues. In this case, an attacker can connect the operator network and obtain access to the server or gateway used to transmit data to the locomotive CBCSs. Depending on server implementation, network and application interfaces can have vulnerabilities that allow a malicious person to access the data processing network. Sometimes, vulnerabilities can be found not in the server applications, but in the network environment systems, e.g. in network devices or infrastructure protocol services (such as DNS). An intruder can use these systems as intermediate hosts to develop an attack[35].

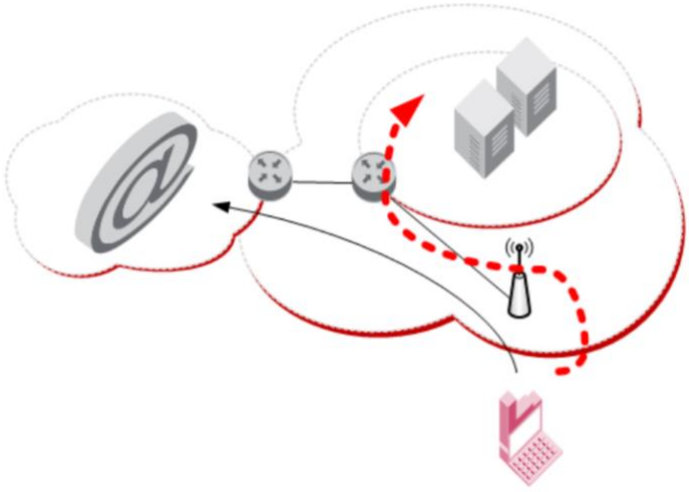


Figure 22. Attacks against the server using network equipment vulnerabilities

If attackers know the parameters of network devices and applications used by the server part, they can use special-purpose search systems such as Shodan or Censys to find the Internet connection points.

There are ready-to-use packages[36] of search engine requests (the so-called Google dorks or Shodan dorks) aimed to automate identification of special-

35 How to hack a telecom and stay alive, Sergey Gordeychik, https://www.slideshare.net/qqlan/ss-10347896

36 Internet connected ICS/SCADA/PLC, SCADA StrangeLove, http://scadastrangelove.blogspot.com/2013/12/internet-connected-icsscadaplc30c3.html

purpose systems connected to the Internet and detection of vulnerability symptoms[37]. Some knowledge bases contain even extended information such as network fingerprints that allow one to identify the device type, its vendor, the firmware version, the installed components, etc.

Novus	Novus 0001	modbus	Novus 0001
Nivus	OCM Pro CF	modbus	OCM Pro CF
Ouman	Ouman 20340DRF	modbus	Ouman 20340DRF 05.20
Ouman	Ouman 203mbH	modbus	Ouman 203mbH xxxxxx V1.00
Ouman	Ouman 686Electric BMX	modbus	Ouman 686Electric BMX
Ouman	Ouman 686Kontakt 34	modbus	Ouman 686Kontakt 34
Ouman	Ouman 686 Kontakt 34	modbus	Ouman 686 Kontakt 34
PEWEU	PEWEU FPWEBD V2.1 www.peweu.de FP-WebServer	modbus	PEWEU FPWEBD V2.1 www.peweu.de FP-WebServer
proconX Pty Ltd	proconX Pty Ltd FT-MBSV EXPERIMENTAL	modbus	proconX Pty Ltd FT-MBSV EXPERIMENTAL
PRODUAL OY	PRODUAL OY PDSMB	modbus	PRODUAL OY PDSMB
Schneider Electric	Schneider Electric 15210	modbus	Schneider Electric 15210
Schneider Electric	Schneider Electric 15211	modbus	Schneider Electric 15211
Schneider Electric	Schneider Electric A9MEM3150	modbus	Schneider Electric A9MEM3150
Schneider Electric	Schneider Electric A9MEM3155	modbus	Schneider Electric A9MEM3155

Figure 23. A knowledge base containing the network fingerprints of industrial systems

Vulnerabilities can be also found in the mobile operator infrastructure. An attack can be directed against edge devices used by Packet Core and MME Core, e.g. a Gateway GPRS Support Node (GGSN) or a Serving GPRS Support Node (SGSN). A number of investigators[38] have demonstrated attacks that allowed one to gain unauthorized access to the devices processing voice and packet traffic of mobile subscribers.

Sometimes, the interfaces for remote control of network devices in the mobile operator infrastructure are available from external networks[39]. To identify them, one can use network scanners or Internet search services.

37 Google Hacking Database, https://www.exploit-db.com/google-hacking-database/

38 Hacking HLR/HSS and MME Core Network Elements https://conference.hitb.org/hitbsecconf2013ams/materials/D1T2%20-%20Philippe%20Langlois%20-%20Hacking%20HLR%20HSS%20and%20MME%20Core%20Network%20Elements.pdf

39 Bootkit via SMS, Timur Yunusov, Kirill Nesterov, https://conference.hitb.org/hitbsecconf2015ams/materials/D1T1%20-%20T.%20Yunusov%20K.%20Nesterov%20-%20Bootkit%20via%20SMS.pdf

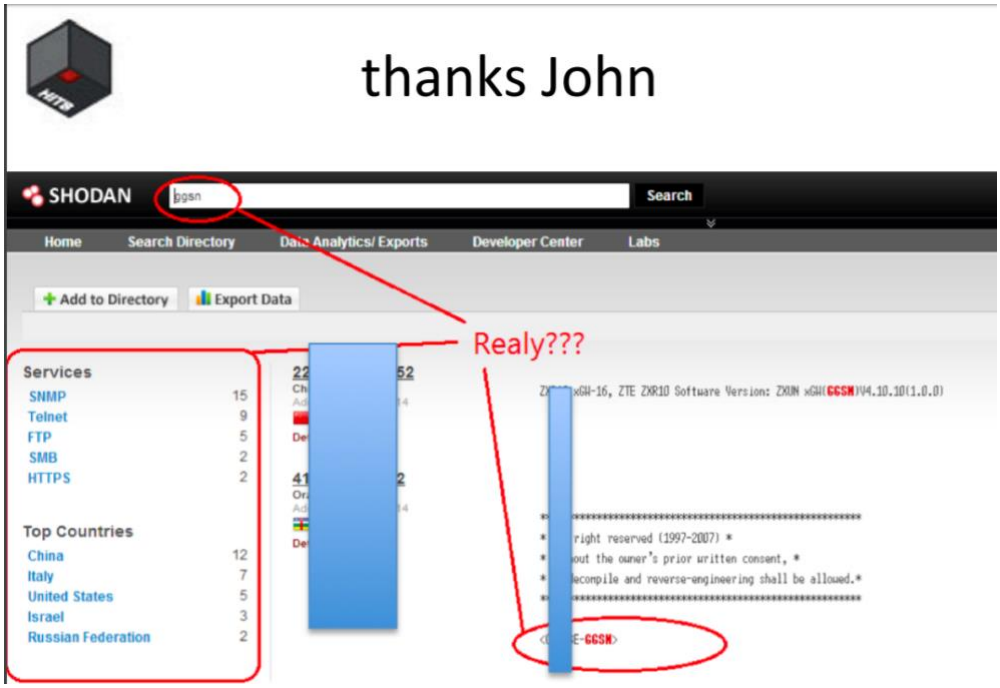


Figure 24. Identifying public interfaces for GGSN network control

Control interfaces available from the Internet often have well-known weaknesses such as weak or empty passwords, lack of updates installed, and web interface vulnerabilities. It allows an attacker to gain remote access to the system, change its settings, intercept and modify subscribers' traffic, and develop the attack further into the internal operator network.

Figure 25. GGSN control interface available from the Internet without authentication

This architecture can be also used in other systems such as remote diagnostics modules and systems for passenger flow analysis[40]. Here, a GSM modem connects to the internal locomotive Ethernet and can access the WBT used to communicate with various CBCSs. Is such a manner, an intruder can develop an attack if he/she manages to compromise the wireless connection.

A very similar architecture is used in some modern automobiles. Practical security analysis[41] showed that an attacker can use a combination of vulnerabilities to obtain remote access to the head unit of an automobile via wireless networks, modify the CAN controller firmware and then conduct a cyber-physical attack, e.g. cause an emergency braking.

40 Автоматизированная система учета и анализа пассажиропотока, http://transtelesoft.com/?page_id=133

41 Remote Exploitation of an Unaltered Passenger Vehicle, Dr. Charlie Miller, Chris Valasek, http://illmatics.com/Remote%20Car%20Hacking.pdf

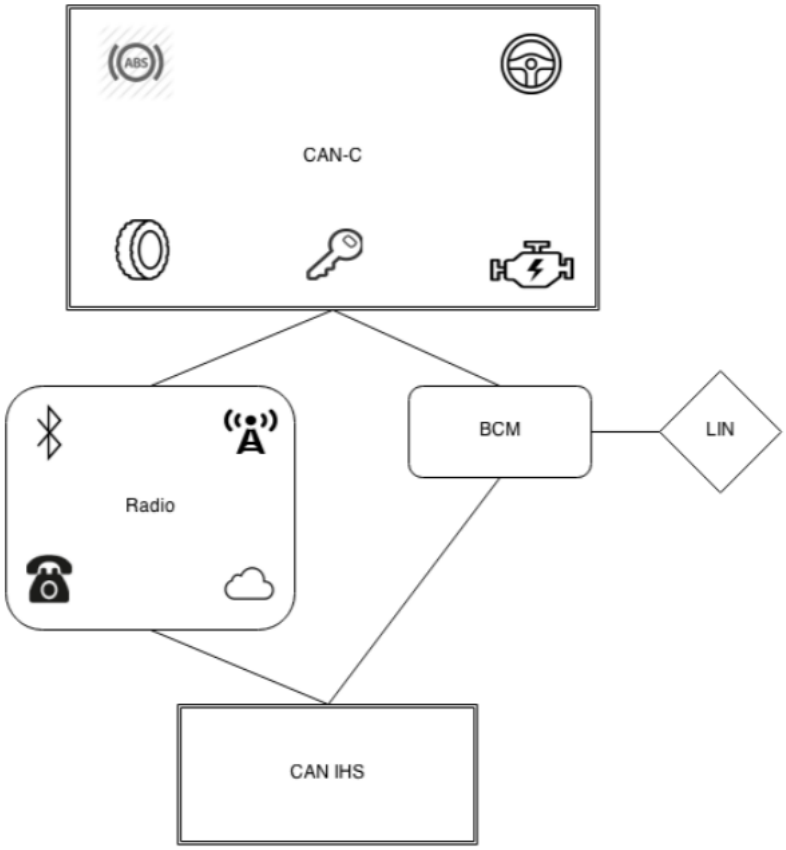


Figure 26. Block diagram of a network subsystem of the 2014 Jeep Cherokee automobile

In such a manner, if a CBCS uses public mobile communications networks, then an extended threat model should be developed. To reduce the risks, it is recommended to consider mobile communications networks as untrusted and use protection mechanisms such as virtual private networks to provide authentication, confidentiality, and integrity control for the data being transmitted, as well as identification of vulnerabilities in application systems connected to public networks.

In European Train Control System[42] (ETCS), various wireless technologies are widely used. Level 2 and level 3 imply that a radio channel is used instead of

42 European Train Control System, From Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/European_Train_Control_System

track circuits to exchange information about the train position, track occupancy, and the distance to the next train. For this purpose, GSM-R is used.

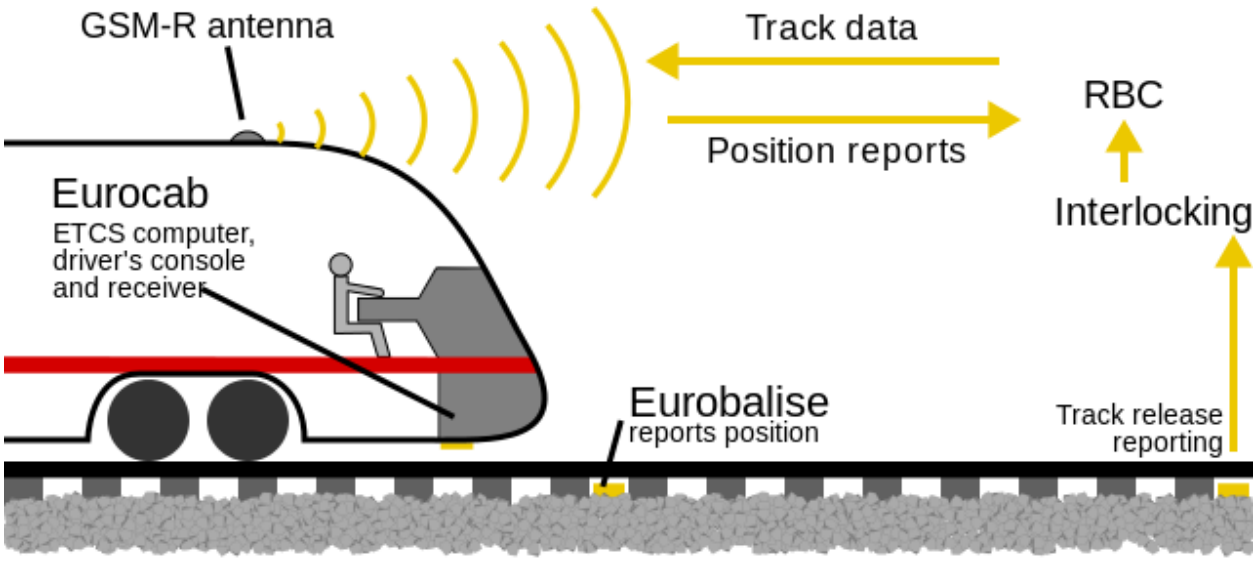


Figure 27. Application of GSM-R in ETCS Level 2

The key components are:

- Remote Data Access Train Router (RDA-RT)
- Mobile Switching Center (MSC)
- RadioBlock Center (RBC)
- Yardmaster Workstation (YWKS)
- Integration Gateway (IG) that provides communication with CBI, CTC systems, etc.

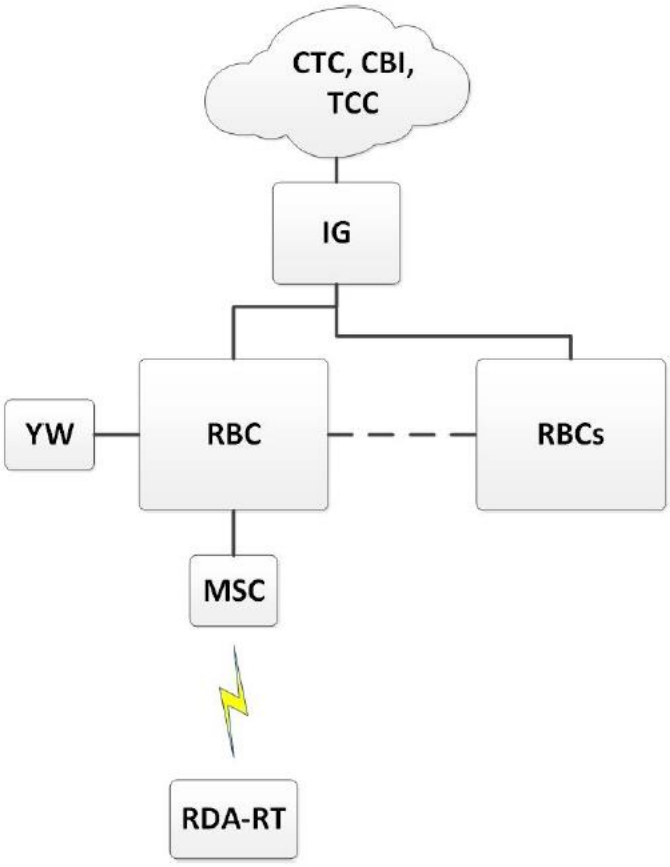


Figure 28. Interaction between CBCSs in ETCS

In this case, GSM-R becomes a critical technology that considerably influences the traffic safety. Therefore, special attention is paid to GSM-R resilience. For example, in some countries open connection between RDA-RT and RBC requires immediate train stop[43] and then moving on ready to put on brakes and stop.

43 European Train Control System, From Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/GSM-R

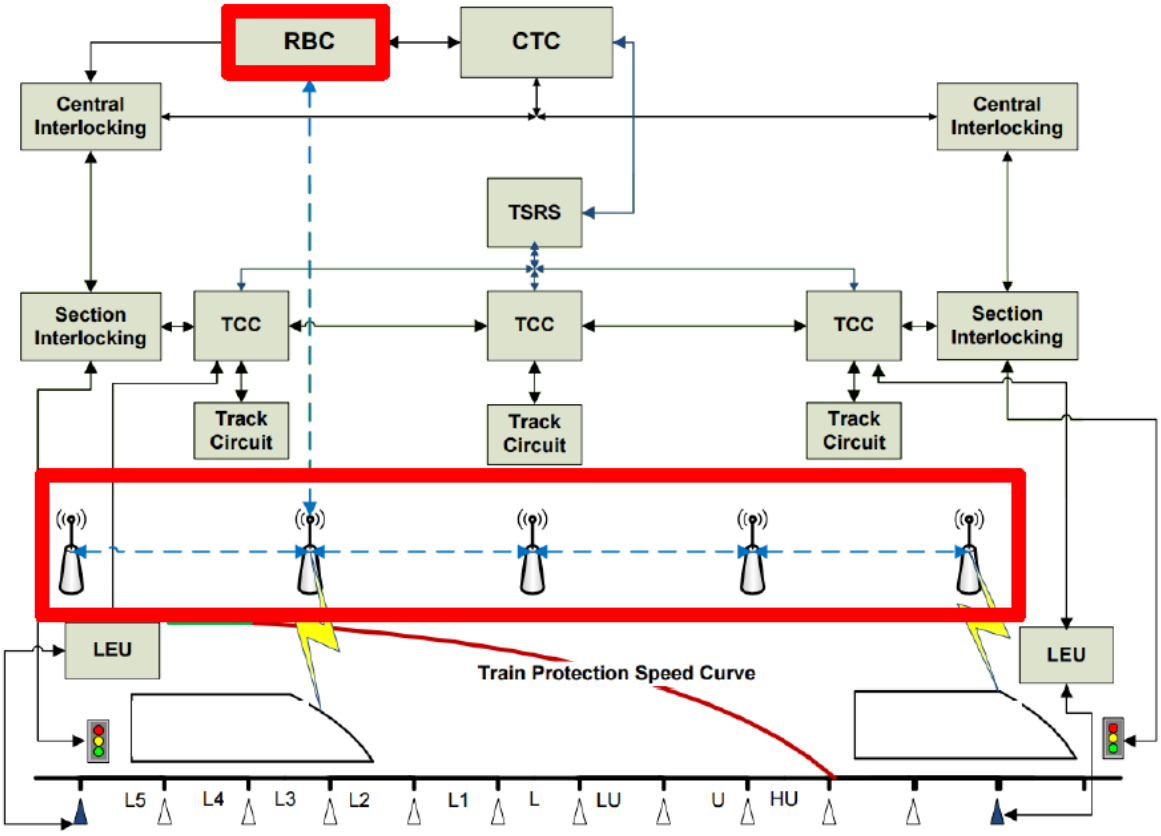


Figure 29. ETCS Radio part

In contrast to the original GSM, GSM-R implements additional layers of confidentiality and integrity control: Euroradio Safety Layer[44] (Euroradio SL) and Safety Application Interface[45] (SAI). For this purpose, Cipher Block Chaining MAC (CBC-MAC) is used involving the Triple-DES algorithm in EDE (Encryption – Decryption – Encryption) mode, which is also known as the Triple Data Encryption Algorithm (TDEA). Recently, a number of investigators reported that the real cryptographic security of the applied protocols is lower than it is in theory. Therefore, the algorithms can be prone to attacks [46] and allow a malicious person to delete messages and perform command forgery[47].

44 Subset-037: Euroradio FIS. 2005, v 2.3.0

45 FIS SAI: Safe Application Service. 2002, v 8.0, SI/TRK/UP/2

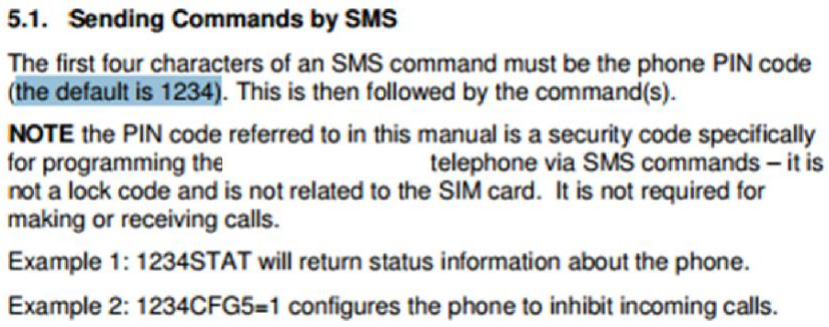
46 SAFETY ANALYSIS OF CRYPTOGRAPHY MECHANISMS USED IN GSM FOR RAILWAY, Mária FRANEKOVÁ, Karol RÁSTOČNÝ, Aleš JANOTA, Peter CHRTIANSKY

47 An Attack Against Message Authentication in the ERTMS Train to Trackside Communication Protocols

Sometimes, an additional layer of encryption using VPN is implemented to reduce these risks.

GSM-R key management possesses one of possible security issues. The specification describes only autonomous key distribution, i.e. the encryption and integrity control keys are delivered to the locomotive devices and RBC via portable media. Taking into account the great number of keys (some sources claim the UK railway services have to handle over 400 000 keys), the process of updating and revoking keys becomes sophisticated; as a result, they use only the keys generated at the device initialization[48].

Even more dangerous vulnerabilities can be found in mobile terminals such as GSM-R cell phones and locomotive access terminals. For example, many GSM-R mobile terminals implement the mechanisms of remote control using SMS. Meanwhile, rather simple passwords (often specified in documentation) are used to authenticate to the devices.



5.1. Sending Commands by SMS

The first four characters of an SMS command must be the phone PIN code (the default is 1234). This is then followed by the command(s).

NOTE the PIN code referred to in this manual is a security code specifically for programming the telephone via SMS commands – it is not a lock code and is not related to the SIM card. It is not required for making or receiving calls.

Example 1: 1234STAT will return status information about the phone.

Example 2: 1234CFG5=1 configures the phone to inhibit incoming calls.

Figure 30. Control commands for GSM-R terminal[49]

The safety assessment practice shows that default passwords and security codes are usually used; furthermore, most operators even are not aware of this control mechanism, so they do not include it into the process of IT equipment

Tom Chothia, Mihai Ordean, Joeri de Ruiter, Richard J. Thomas

48 "Can trains be hacked?", Stefan Katzenbeisser, https://media.ccc.de/v/28c3-4799-de-can_trains_be_hacked

49 Commander GSM installation and operation guide

change management. As a result, an attacker with a GSM-R terminal gains limited remote control over mobile terminals.

The specification of SIM cards for GSM-R[50] describes possible use of the SIM Application Toolkit[51] (STK). This mechanism allows one to perform various operations with a mobile terminal or a SIM card:

- display text on the mobile terminal screen;
- send SMS, initiate an outcoming call or USSD-package;
- interact with a user (via a dialog menu);
- receive data from SMS or Cell Broadcast and save them to the SIM card;
- send files from the SIM card filesystem;
- change the outcoming call numbers and deny certain calls.

For these purposes, the so-called binary SMS and Over-The-Air (OTA) mechanisms are used. These technologies provide interaction directly between the SIM card and the communications service provider and allow one to download applets and change settings without physically accessing the device. To provide safety, a standard mechanism described in ETSI GSM 03-48 (Security Mechanisms for SIM Application Toolkit) is used. It implies mutual authentication of the OTA server and the SIM card with a cryptographic digital signature using symmetric keys DES or Triple-DES written to the SIM card at its issue.

Regarding the security resilience of these mechanisms, it was shown[52] that a number of applications installed to SIM cards contain sensitive information disclosure vulnerabilities. If such application receives a request from the OTA with invalid authentication code, it will return an error notification signed with the valid code. As a result, an attacker can recover the OTA keys and send control SMS as the OTA server.

50 FFFIS for GSM-R SIM Cards, http://www.era.europa.eu/Document-Register/Documents/P38T9001%204.2%20FFFIS%20for%20GSM-R%20SIM-CARD.pdf

51 GSM SIM-ME Interface, (GSM 11.14) http://www.ttfn.net/techno/smartcards/GSM11-14V5-2-0.pdf

52 SIM card exploitation, Karsten_Nohl

Further investigations[53] showed that an OTA key can be obtained in practice, even if TripleDES is used for authentication as recommended in FFFIS for GSM-R SIM Cards. A rig consisting of 8 FPGAs (total cost about $ 2 000) allows one to find a 3DES key in 10 days.

Hardware	Speed (Mcrypt/sec)	Time for DES (days)	Time for 3DES (part of key is known, days)
Intel CPU (Core i7-2600K)	475	1755,8 (~5 years)	5267,4
Radeon GPU (R290X)	3`000	278	834
Single chip (xs6slx150-2)	7`680	108,6	325,8
ZTEX 1.15y	30`720	27,2	81,6
Our rig (8*ZTEX 1.15y)	**245`760**	**3,4**	**10,2**

+ descrypt bruteforcer - https://twitter.com/GiftsUngiven/status/492243408120213505

Figure 31. Time to guess an OTA key[54]

As a result, at attacker becomes able to read the SIM card data such as credentials (TIMSI) and encryption keys (Kc) and even download arbitrary Java applications to the card. It is also possible to block a SIM card by brute-forcing the personal identification number (PIN) or the personal unblocking code (PUK).

Most vendors follow the FFFIS recommendations for GSM-R SIM Cards and implement the OTA mechanisms in accordance with the ETSI GSM 03.48 Security Mechanisms for SIM Application Toolkit. Consequently, all the above-described attacks can be conducted, if there are errors in implementation of the APDU authentication mechanisms.

Furthermore, some devices implement additional mechanisms such as Firmware Over-The-Air (FOTA). In this case, an attacker gets extended

53 Root via SMS, Sergey Gordeychik, Alexander Zaytsev, https://pacsec.jp/psj14/PSJ2014_Sergei-Alex_SCADASL%20-%20root%20via%20sms%20last.pdf

54 Commander GSM installation and operation guide

opportunities and can exploit STK vulnerabilities to attack not only SIM cards, but the very mobile terminals represented by locomotive radio systems, GSM-R modems, desk or mobile GSM-R phones.

Figure 32. Specification of the locomotive device Traintalk GSM-R 8W CAB RADIO

To conduct an attack, a malicious person should take certain preparatory measures:

- Gain access to mobile GSM-R terminals.
- Analyze the SIM cards in use to find vulnerable APDU (for this purpose, the SIMtester[55] utility or its modifications can be used).
- Some APDUs (e.g. those accessing the file system) require SIM-card PIN codes. These values usually remain unaltered and can be achieved from documentation.
- In some cases, it is necessary to prepare a Java applet to be downloaded remotely to a vulnerable SIM card.
- Generate a modified software image to be downloaded remotely to the device. In theory, such images should be protected using strong integrity control mechanisms; in practice, this measure is rarely used.

This attack is complex but technically feasible; therefore, it should be included into the threat model for locomotive and train radio communications systems.

Sometimes, special-purpose GSM-R modems are used to provide communications with a station or a locomotive. Modern GSM-R modems connect to workstations via USB interfaces. If a modem connected to an intelligent device

55 SIMtester, https://opensource.srlabs.de/projects/simtester/wiki

has vulnerabilities, then an attacker can use this modem to attack the target system (a locomotive on-board computer, or a station system).

Figure 33. GSM-R Triorail TRM-5T modem

To conduct an attack, a malicious person can force a vulnerable USB modem to emulate another peripheral device. The simplest example is emulation of a keyboard: a modem is sending commands to the workstation as if they were keyed in by a user. There also are other attack vectors involving local vulnerabilities of printers, video cameras and keyboards. These vulnerabilities are usually considered to be not important, because local access is required to exploit them. However, a modem allows attackers to exploit these vulnerabilities remotely.

Figure 34. A Bad USB attack using a modem

The mechanism of Bad USB attack was described in more details in an article[56] by SRLabs. Its application for 3G and 4G network cellular modems was considered in an investigation[57] by the SCADA StrangeLove team.

Since wireless modems are often connected to the local CBCS data networks, the described attacks allow an intruder to gain unauthorized access to critical CBCS components such as automatic blocking systems, CBI systems, automatic train operation systems, etc. Regarding the locomotive systems, a malicious person can use a modem to attack internal buses such as WTB and ETB and develop the attack to access the control systems.

An example of intermediate systems that usually are not even considered as possible attack targets is a remote diagnostic system. As a rule, modern locomotives and high-speed trains have a mechanism to send diagnostic information about the state of various devices. Even if the CBCS uses the GSM-R standard upgraded with additional integrity control mechanisms (Euroradio or VPN), the diagnostics systems still use 2G/3G cellular networks and involve general-purpose modems and routers adapted to railway services. These systems are often connected to the MVB to call over the locomotive devices.

56 USB peripherals can turn against their users, https://srlabs.de/bites/usb-peripherals-turn/

57 Critical Vulnerabilities in 3G/4G Modems, http://blog.ptsecurity.com/2015/12/critical-vulnerabilities-in-3g4g-modems.html

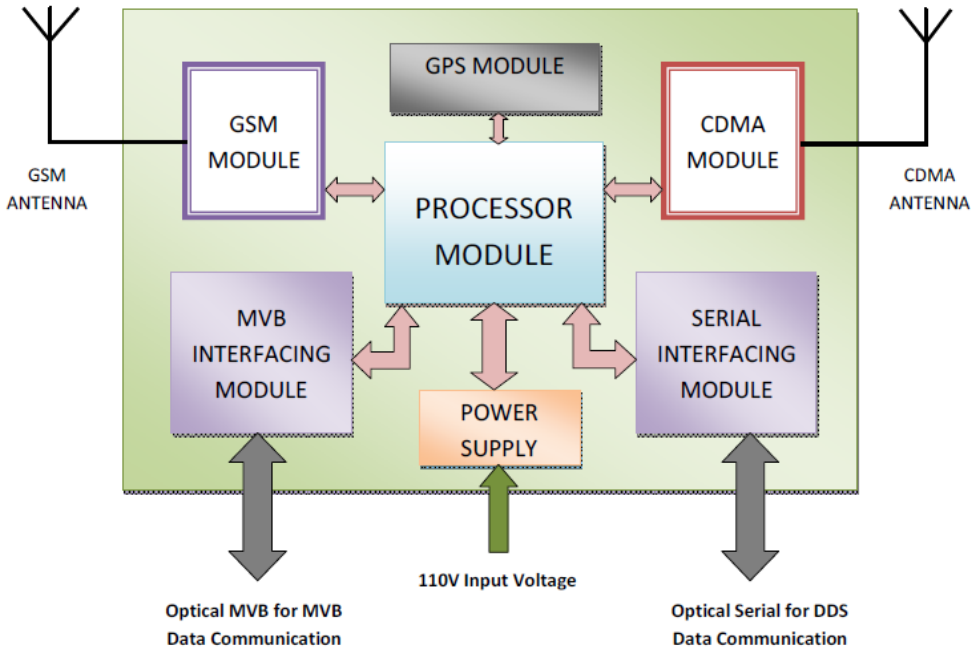


Figure 35. Block diagram of RDS, Advanced Rail Controls Pvt. Ltd

At the same time, the information sent through GSM channels is processed by servers that can have external interfaces to access the Internet and internal interfaces to access wireless networks (e.g. to send SMS notifications).

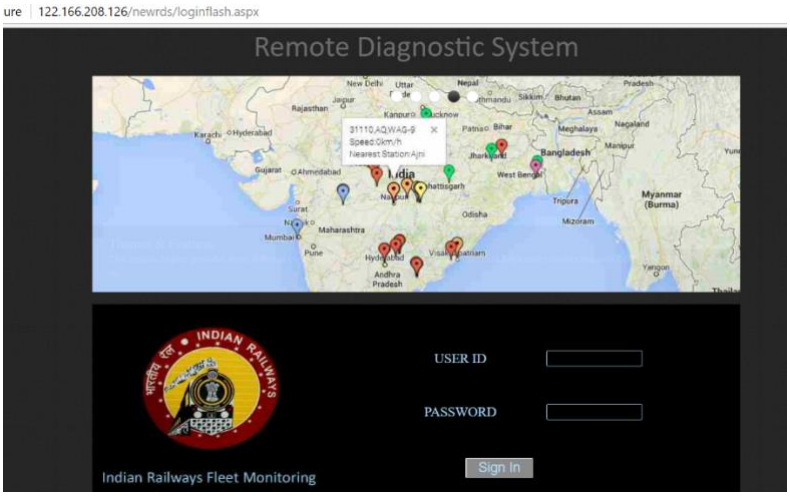


Figure 36. Accessing the web interface of the Indian Railways Fleet Monitoring system

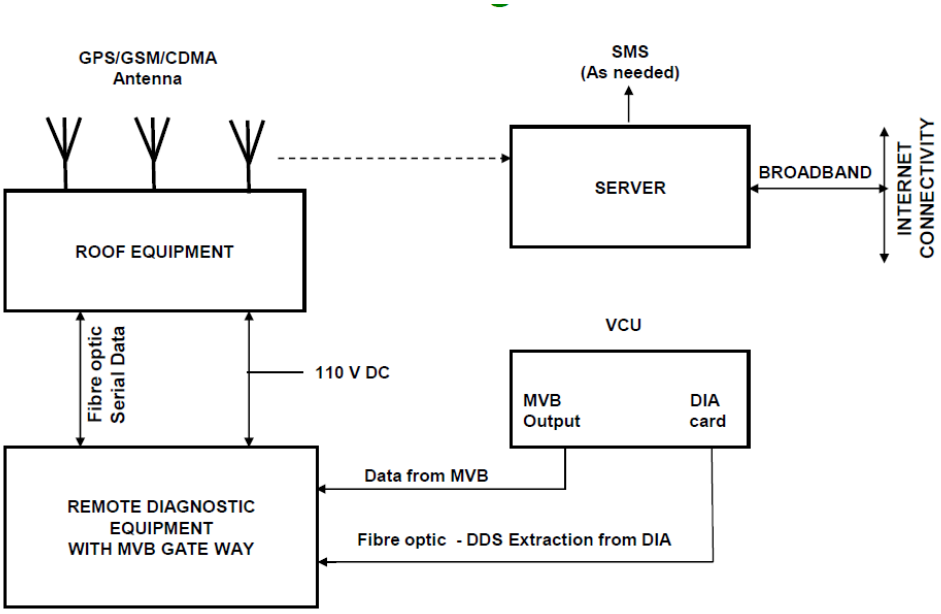


Figure 37. Attack vectors for the RDS REMAN_EL [58] system

In such a manner, connections of wireless devices (i.e. access points for Wi-Fi, modems, GSM and GSM-R train radio communication systems, etc.) should be considered as parts of the security perimeter along with connections to public networks and the Internet.

When connecting CBCS components, specialists should take measures to isolate subnetworks and control network communications. Otherwise, dependences between different IT systems will occur soon affecting the industrial safety due to possible attacks against the Internet systems.

In October 2017, DDoS attacks have brought down several IT systems employed by Sweden's transport agencies, causing train delays in some cases[59].

The first attack hit the Sweden Transport Administration (Trafikverket) on Wednesday, October 11th. According to local press, the attack brought down the IT system that manages train orders. The agency had to stop or delay trains for the time of the attack. Trafikverket's email system and website also went down,

58 Remote Diagnostic System (RDS) for 3-phase & Remote Monitoring & Analysis for Conventional Electric Locomotives (REMAN_EL), Research designs & standards organization, Government of India, Ministry of Railways

59 https://www.bleepingcomputer.com/news/security/ddos-attacks-cause-train-delays-across-sweden/

exacerbating the issue and preventing travelers from making reservations or getting updates on the delays.

Speaking to local media, Trafikverket officials said the attack was cleverly aimed at TDC and DGC, the agency's two service providers, but they were both aimed in such a way to affect the agency's services. Trafikverket was able to restore service in a few hours, but the delays affected the entire day's train operations.

The next day, October 12th a similar DDoS attack hit the website of another government agency, the Sweden Transport Agency (Transportstyrelsen), and public transport operator Västtrafik, who provides train, bus, ferry, and tram transport for parts of Western Sweden.

Application Level

This section describes typical technical vulnerabilities of CBCSs at the level of OS, data, and applications.

An early edition of Ten Immutable Laws of Security[60] postulates a low reading as "If a bad guy has unrestricted physical access to your computer, it's not your computer anymore." Though the idea is rather obvious, it is highly important and serves as the basis for a separate IT security subdiscipline – physical safety, which is a mandatory element of most security programs. Indeed, an attacker who has physical access to the system can apply various methods such as digital forensics practices, boot sequence alteration, cold reboot attacks, etc. to bypass most protection mechanisms.

It should be mentioned, that every rule has its exceptions. There are special-purpose systems aimed to provide safety in case of unauthorized physical access. However, these systems are usually designed for military applications to meet

[60]Ten Immutable Laws Of Security (Version 2.0), Microsoft, https://technet.microsoft.com/en-us/library/hh278941.aspx

specialized needs, e.g. formulated in FIPS 140-2[61]. The purpose of these protection mechanisms is not to provide operability, but to prevent disclosure of critical data (e.g. the encryption keys).

People traditionally considered the railway services to provide high level of physical safety. However, the author's experience shows that it is not true; in most security assessment projects, the experts managed to gain unauthorized physical access to the CBCS components. There are several reasons for such insecurity:

- Spatial distribution. CBCS components are presented in the entire area of railway networks. Stations, passenger depots, trackside equipment, ticketing offices, passenger information desks have very different environment in the terms of physical safety.
- Developing network connectivity. Integration of systems leads to the situation when successful attacks against a remotely administered CBI system and a backbone node will cause comparable damages.
- Working with moving objects. Locomotives and cars are distributed through the railway networks. They may be moving, staying in storage yards, being classified, etc. Each situation provides an attacker with different opportunities. If teenagers can graffiti cars and locomotives, then motivated malicious people will surely manage to access them.

Below are given the results of several audit checks concerning the privileges an attacker managed to gain.

- Access server (relay) rooms containing CBI components including the CPU and object controller racks.
- Connect devices (USB keyboard emulators, external memory) to the yardmaster WKS or signal technician WKS.
- Connect devices (wireless access points) to the switches and routers at the stations.
- Access locomotive MVB and WTB devices.
- Switch CBCS devices to the maintenance mode to access advanced features.

61 Cryptographic Module Validation Program, NIST, https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards

Let us consider some potential consequences of unauthorized physical access.

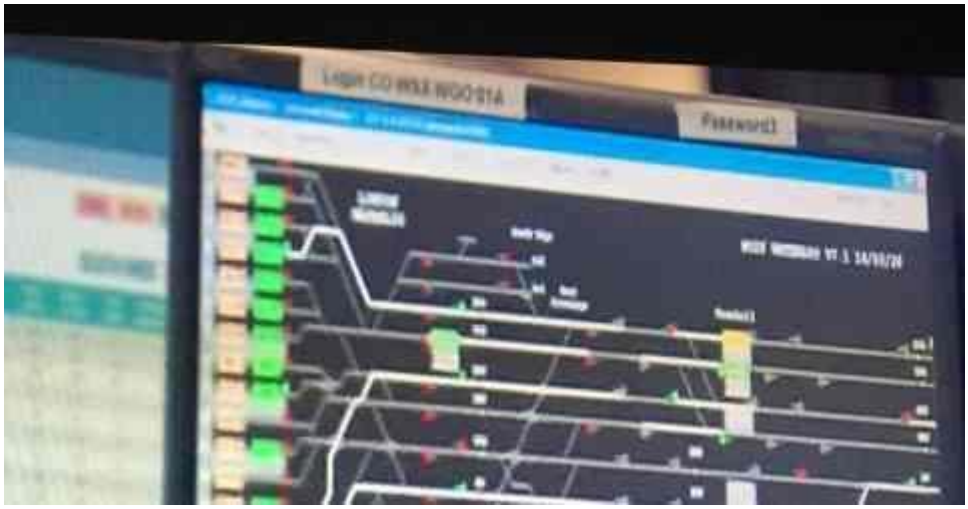
In the course of security audit projects, experts often examine how the employees store their passwords. These checks usually reveal multiple violations.

Password Format	Location Found	Percent
Sequential, Place names, sport teams, Colors, dates	Under the Mouse pad	10%
"	Under the Keyboard	10%
"	On the monitor	5%
Default passwords, and combinations (dates+names+sequentials, etc)	On desk, bookshelf, unlocked drawer	25%
Default passwords, and combinations (dates+names+sequentials, etc)	Spreadsheets, and MS Access Databases	50%

Table 6: Password format and storage location

Figure 38. Typical ways to store passwords[62]

In industrial enterprises, such practice is common. Passwords are usually stored in public places, e.g. on monitors. Here is a remarkable example: passwords to control systems of the London Waterloo station were disclosed in a BBC documentary[63]. It is a typical situation for RTA CBCSs and ICSs on the whole.



62 User Authentication Principles, Theory and Practice, Yaacov Apelbaum

63 Major London rail station reveals system passwords during TV documentary, John Leyden, The Register, https://www.theregister.co.uk/2015/05/01/london_rail_station_exposes_signal_system_passwords/

Figure 39. Passwords to Waterloo station systems disclosed in the BBC film “Nick and Margaret: The Trouble With our Trains”

The reason is that an operator must access the system promptly in case of emergency. In such situation, complex passwords can cause extra delays. In fact, the IT network password policy being applied to industrial systems increases the access time and reduces the control operational efficiency.

However, development of network connectivity along with distribution of modern OSs that implement the principles of single sign-on and single password cause a new issue. Now, single user credentials can serve both for physical-access authentication and for network authentication to workstations, servers, and applications available to the user.

The workstations of CBCS operators often work in so-called Kiosk mode. In this mode, the OS-user interaction features are limited and include only several applications; other applications cannot be launched, the command prompt is unavailable.

However, these restrictions are poorly implemented and can be removed not only by an experienced attacker, but even by an ordinary employee. A number of investigators claim that operators were bypassing the Kiosk mode without exploiting OS vulnerabilities in over then 50%[64] of industrial HMIs. The operators justified safety rules violation with the necessity to use additional applications not included into the white-list to perform their production tasks. To do so, they used various hot keys (e.g. F1 for Help) and the mode of accessing application files (e.g. driver selection in Print mode).[65]

To improve the controllability, workstations are often replaced with terminals running Microsoft Terminal Server, Citrix XenApp, etc. If the

64 SCADA STRANGELOVE or: How I Learned to Start Worrying and Love Nuclear Plants, Sergey Gordeychik, Denis Baranov, Gleb Gritsai, https://www.slideshare.net/qqlan/scada-strangelove-29c3

65 TrustedSec, Kiosk/POS Breakout Keys in Windows, https://www.trustedsec.com/2015/04/kioskpos-breakout-keys-in-windows/

restrictions of software environment are set improperly[66], then an attacker can exit the Kiosk mode to compromise all users working with the server. The experience shows that many cloud-based HMIs[67] suffer from this problem.

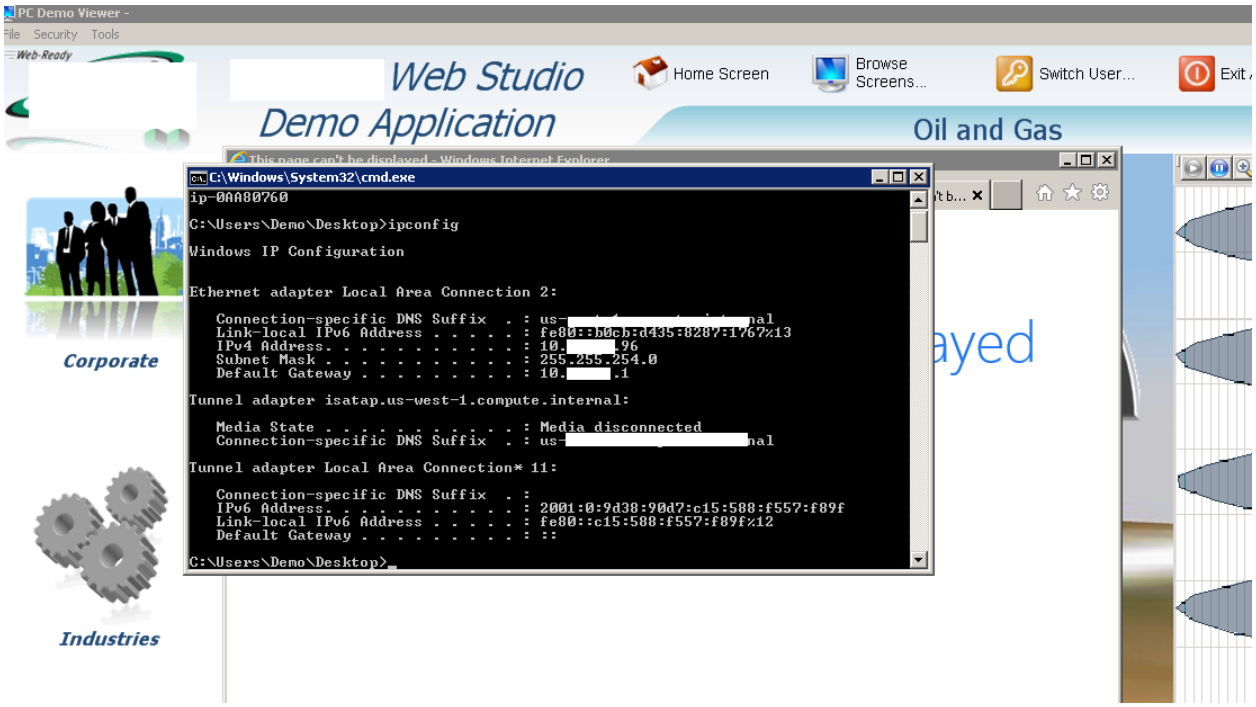


Figure 40. Exiting the Kiosk mode in a cloud HMI

When exiting the Kiosk mode or directly accessing the file system, one can obtain the password hashes used by applications to access databases and application systems. These passwords are often stored not in a secure OS storage, but in configuration files readable by any OS user.

Furthermore, USB ports are often left enabled on servers and workstations. It is caused by the necessity to maintain the system, copy files, download updates, and connect standard peripheral hardware (keyboards, mouse, cameras). In this case, an attacker also can use USB to connect malicious devices and copy files,

66 Breaking Out! of Applications Deployed via Terminal Services, Citrix, and Kiosks, Scott Sutherland, https://blog.netspi.com/breaking-out-of-applications-deployed-via-terminal-services-citrix-and-kiosks

67 SCADA StrangeLove 2: We already know, Gleb Gritsai, Sergey Gordeychik, http://scadastrangelove.blogspot.com/2014/01/30c3-releases-all-in-one.html

access external networks or conduct a Bad USB attack. To address this threat, one can use host-level protection tools such as DLP and anti-viruses that provide selective USB blocking.

Many CBCS components such as network switches and CPUs have special-purpose ports and modes meant for local control and maintenance. The maintenance mode disables the integrity control mechanisms, mounts the file system in the write mode, and allows one to modify the system objects and parameters. In such a manner, if attackers have physical access to the system, they can switch it to the maintenance mode and change its settings (e.g. add remote-access accounts or install malicious software) to further use them for attack development.

If an attacker gains physical access to CBCS devices or connects to the LAN, he/she will be able to interact with local (USB, UART) or network (SNMP, FTP, Telnet, HTTP) supervisory and remote control protocols. In industrial systems, diagnostic ports are usually protected with default passwords or even not protected with passwords at all. Default passwords can be achieved from documentation, configuration files or CBCS firmware description.

Figure 41. Default credentials disclosed in system documentation[68]

[68] Ebilock 950, http://scbiinfrastruktura.ru/wp-content/uploads/%D0%A0%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5

There are various databases of standard passwords for industrial systems, e.g. SCADAPASS[69]. An entry usually contains the system type, the remote access protocol, and the credentials. These databases can be easily integrated with vulnerability scanners to automate safety auditing.

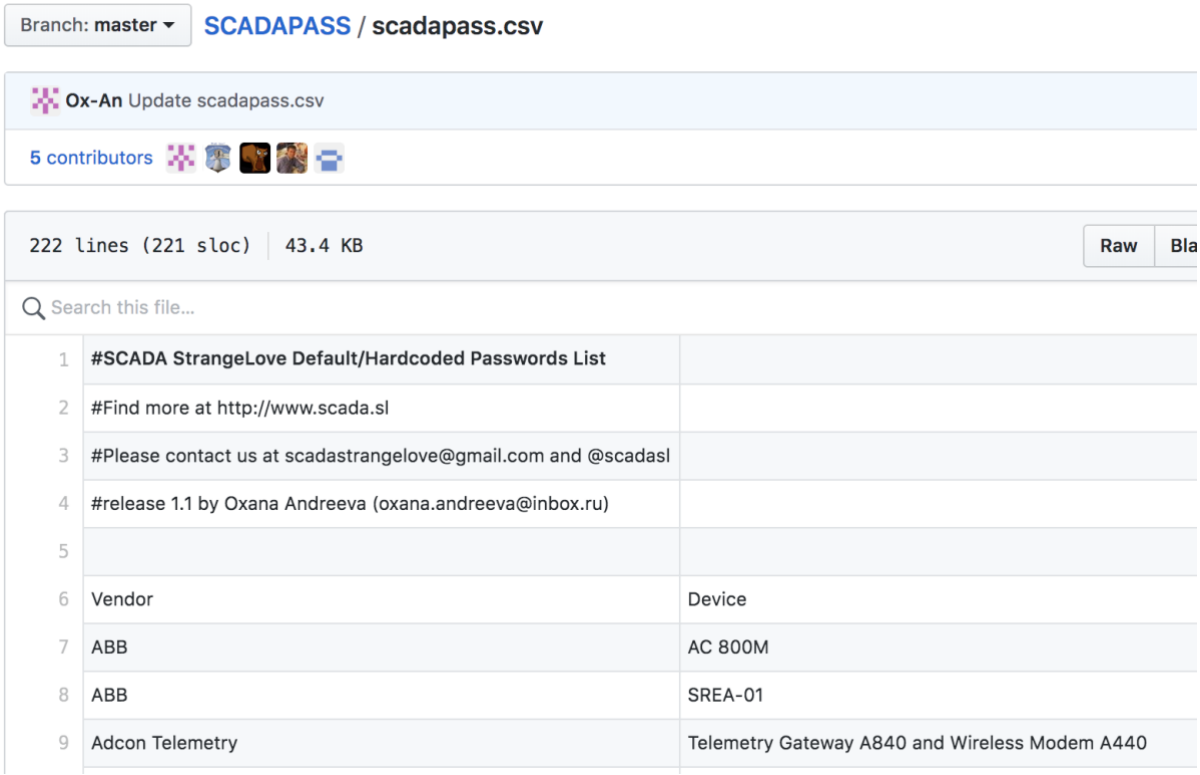


Figure 42. SCADASOS repository of standard passwords for industrial systems

It should be mentioned that simple, default, and "engineering" passwords allow attackers not only to obtain local physical access to the system. Intruders

%D0%BD%D0%B4%D0%B0%D1%86%D0%B8%D0%B8-%D0%BF%D0%BE-%D0%9C%D0%9F%D0%A6-EBILock950.pdf

69 SCADAPASS #32C3 Release, http://scadastrangelove.blogspot.com/search/label/scadapass

can also exploit vulnerabilities in baseline, global, and wireless networks (if any) to obtain network access to the LAN and then connect to the CBCS via remote control protocols.

3. Railway Cyber Resilience

In this chapter, we consider the basic areas in providing RTA cyber resilience, describe a security analysis technique, suggest applying the mission-centric approach to define a cyber threat model, and state technical requirements to the system of attack and security incident detection.

Let us consider the following independent but interconnected directions in providing RTA cyber security:

1. Control of MPS trust level.
2. Control of cybersecurity level of railway information systems involved in traffic management.
3. Control of cyber protection tools efficiency.
4. Detection of and investigation into cyber attacks and incidents, system recovery.

CBCS Trust Management

The task of CBCS trust management basically refers to organizing consistent relationships with system developers. Furthermore, implementation of corresponding measures makes the developer responsible for a part of cyber resilience tasks, which reduces the total cost of cyber security (according to a number of researchers, error correction is incomparably cheaper at the stage of design and development compared to that at the stage of operation[70]).

One of the key solutions in this area is creation of a repository to store CBCS software, related software components and documentation, and to build test benches. This repository allows one to solve the following problems:

[70] K. JayaSriDevi, P. Mohan, A. Udaya Shankar. Quality Flaws: Issues and Challenges in Software Development // [IISTE International Knowledge Sharing Platform] URL: http://www.iiste.org/Journals/index.php/CEIS/article/viewFile/3533/3581

1. Ensuring CBCS availability if legal entities representing CBCS and software IPR holders dissolve.

2. Ensuring CBCS cyber resilience by detecting and eliminating weaknesses, vulnerabilities and undocumented features that affect CBCS security.

3. Coordinating system modifications with vendors; co-development of software for CBCS enhancement; introducing modifications to improve CBCS functional and IT safety.

Taking into account the tasks in hand, the repository must have tools to assemble software from the source code. The modern systems are very complex and it is impossible to make modifications and ensure software operability just having the source code available without reliable technique and hardware to compile and integrate software components.

Since that, the process of saving software to repository should include control assembly that provides ready-to-use CBCS software components. These elements are compared with analogous files and components used in test benches.

The described solution allows for:

1. Integrity control of CBCS components, which is not only a necessary requirement for IT and cyber security, but also an important stage of measurement assurance.

2. Ensuring non-repudiation for CBCS software components.

3. Sufficiency control of the components being saved to the repository with respect for CBCS operability assurance.

Most software solutions contain third-party components. This situation has an effect on cyber security and other sides of system operation and maintenance. If third-side software (OSs, DBMSs, compilers, etc.) are used, then the reference copies of these products (supported by vendors in the context of compatibility) should be also stored in the repository and be included into control assembly and safety tests.

As an example of third-party software affecting the main system cyber resilience, let us consider vulnerabilities OpenSSL HeartBleed (CVE-2014-0160) and Shellshock. These vulnerabilities were revealed in OpenSSL and Bash Shell components, which are widely used in various products including SCADA/ICS such as Siemens programmable controllers S7-range and Siemens SCADA WinCC-range. The weakness was found in software not directly related to the system functions, but its exploitation allows an attacker to bypass security mechanisms, to obtain unauthorized access to user passwords, and to execute arbitrary code in the system.

Another common situation is when vendors cease to support their products. An average operating cycle of ICS components including CBCSs is fifteen years, which is much longer than the standard support period in IT. For example, Windows 2000 and Windows XP OSs were discontinued in 2010 and 2014 respectively (after almost 10 and 13 years of operation). As a result, there are no current security updated for these widely-used systems. For example, the vulnerability in Windows 2000 and Windows XP Service Pack 2 used by Stuxnet worm to attack Iranian nuclear facilities in 2010 has not been and will never be eliminated. Patch for vulnerability MS-17-010 (EthernalBlue) revealed in Windows XP was published with long delay.

In summary, up-to-date list of software components (including third-party components) used in the system allows one to reveal vulnerabilities in due time and forecast the influence of software life-cycle on the system's cyber resilience. Furthermore, this list can be used to control software clean licensing and to identify risks related to software components published under GNU GPL, which implies the source code to be open.

Analysis of RTA CBCS Cyber Resilience

Detection of CBCS Vulnerabilities and Threats

As mentioned above, vulnerabilities of information systems are often a key to successful cyber-attacks. Consequently, the existing security assessment techniques should be supplemented with activities for early vulnerability detection and elimination of possibilities for cyber-attacks against the CBCS. At that, the relevance principle should be applied, which means that a threat to CBCS resistance is considered to be relevant if it meets all of the following conditions:

- one or several CBCS components contain one or several vulnerabilities that allow an attacker to implement the threat;
- an attacker has opportunities to exploit these vulnerabilities and thus implement the threat;
- the threat if implemented will lead to inacceptable results for the CBCS.

In the course of cyber security assessment, the investigator should assume that intruders have maximal capabilities and act intentionally.

To accomplish the goal, the intruder conducts an attack or a series of attacks against the CBCS using various vulnerabilities. The intruder's capabilities to conduct a successful attack depend on the following conditions:

- the intruder's skills are enough to implement the threat using given vulnerabilities;
- hardware necessary to exploit the vulnerabilities is available;
- there are initial opportunities to exploit the weaknesses.

The principle of maximal capabilities means that the intruder is assumed to act under the best conditions listed above.

In cyber security, intruders usually cannot achieve their goals by one single action involving one single vulnerability. On the contrary, the intruder would

conduct a series of attacks, each of which exploits a certain vulnerability to increase the attacker's capabilities and improve conditions for achieving the goal. Consequently, cyber security assessment should include analysis of interrelation between vulnerabilities and corresponding attacks. For this purpose, the principle of vulnerability primacy is applied, which means that a CBCS threat is included into the scope only if it can be implemented using revealed vulnerabilities.

This approach to vulnerability and threat assessment defines the following work sequence:

1. Weaknesses of CBCS software and hardware are revealed.
2. The revealed weaknesses are analyzed to identify vulnerabilities and estimate attacks that can be conducted by their exploitation.
3. Possible attack series are analyzed; threats that can be implemented by these attack series are identified.

To reveal weaknesses and vulnerabilities, the following methods are used:

- documentation analysis;
- audit data analysis;
- analysis of configuration settings;
- analysis of network protocols;
- CBCS components scanning;
- analysis of authentication mechanisms;
- source-code analysis;
- analysis of access interfaces to CBCS components.

It is recommended to use Common Vulnerability Scoring System version 3 (CVSS v3.0) as the basis for vulnerability assessment. In this system, three metric groups are used: Base Score, Temporal Score, and Environmental Score. Vulnerability scoring makes it easier to associate weaknesses with relevant attack vectors and shows most urgent vulnerabilities to be eliminated first. This approach is beneficial for developers and reduces vulnerability elimination efforts.

Ideally, updating data on vulnerabilities and threats allows one to obtain qualitative estimation of cyber, functional, and traffic safety.

CBCS Vulnerability and Threat Assessment Methodology and Management

Vulnerability analysis has four stages:

- preparing CBCS for assessment;
- CBCS pre-examination;
- CBCS vulnerability detection;
- analysis of results.

Security assessment can be carried out both on a test bench containing the main CBCS components or in productive systems. In the latter case, investigation may cause a denial of service and disturb industrial processes. On the other hand, an isolated laboratory study can give erroneous results, because test-bench conditions may differ from real-life conditions (i.e. configuration and operating procedures). It can lead to:

- overestimation of intruder capabilities, when malicious actions demonstrated in the course of laboratory investigation cannot be performed under actual CBCS operating conditions due to protection measures applied;
- overestimation of security features, when implementation of a reliable-in-theory protection mechanism has weaknesses and can be bypassed by a real-life intruder.

It is reasonable to combine these two approaches. In a test bench, they try to reproduce real-life configurations of hardware and software as faithfully as possible and to include all CBCS software components in the same versions as those used in productive systems. On the other hand, results of laboratory tests should be additionally verified in productive systems.

If it is impossible to build an equivalent CBCS test bench, then all or separate assessment procedures are conducted in the productive system. In this case, the CBCS operator should at first receive the list of analysis methods to be

used and possible issues related to these methods. It is operator who decides whether an action is an admissible or not.

At preparation stage, the CBCS operator:

- defines the list of measures aimed at early detection, mitigation and elimination of negative effects caused by vulnerability assessment procedures;
- together with the testing laboratory group, defines periods to perform assessment works (start and end dates, allowed hours during and outside working time and on holidays);
- informs the CBCS maintenance personnel about the scheduled works and measures taken;
- assigns a work coordinator responsible for cooperation between the testing laboratory group and maintenance personnel; this person also makes decisions on laying-off, resumption and termination of works (the entire investigation or separate actions).

CBCS pre-examination stage includes:

- analysis of CBCS documentation;
- examination of main functions and industrial processes;
- preparation of security checklists based on state, industry and international standards, recommendations and best practices;
- inventory of CBCS software and hardware components and network services;
- checksum test against reference values (received from vendors or stored in repository);
- verification of operation configurations;
- identification of the main points for an intruder to access the system, including CBCS software Graphical User Interface (GUI), programming interfaces of CBCS components, remote access interfaces, interworking interfaces for adjacent systems, physical access to CBCS components, and access to data communication channels;

- generation of a preliminary list of threats and potential ways to conduct an attack;
- attacker model refinement;
- updating the list of vulnerability detection methods to be used in the course of assessment.

When planning activities and choosing appropriate methods, one should remember that the CBCS must be tested in all operating modes:

- normal operating mode;
- various emergency operating modes according to the CBCS design documentation;
- maintenance conditions of the CBCS and its components.

It is a common mistake to think that an intruder who has no information about the system will fail to detect vulnerabilities in it. In contrast to the testing laboratory group, attackers are almost not limited in time. The information the testing laboratory group receives during pre-examination can be obtained by an attacker through trial-and-error. Pre-examination provides completeness of security assessment and merely saves time.

At vulnerability detection stage, penetration testing is performed using the following methods:

- scanning of CBCS components;
- mining of user accounts;
- analysis of CBCS access interfaces;
- analysis of network interfaces used by CBCS components;
- analysis of CBCS configurations.

Penetration testing can be internal or external depending on access points used by investigators. For external penetration testing, the following access points are used:

- remote-access user interfaces to CBCS components available outside the network perimeter;

- remote-access administrator interfaces to CBCS components available outside the network perimeter;
- CBCS interfaces to interact with adjacent information systems;
- wireless access protocols.

For internal penetration testing, the following access points are used:

- special-purpose workstations deployed for investigators and connected to internal CBCS LAN segments;
- user workstations with CBCS software installed;
- programming access interfaces to CBCS components;
- remote-access user, administrator and interworking interfaces available only from CBCS LAN;
- local interfaces of CBCS components (including management consoles and physical interfaces to connect management facilities) that require physical access;
- access features obtained by exploitation of earlier-detected vulnerabilities.

In the beginning of both external and internal penetration testing, investigators apply methods of vulnerability detection that are available to intruders with minimal capabilities:

- analysis of available network protocols;
- brute-force of accounts to access available protocols;
- black-box scanning of available CBCS components.

As new vulnerabilities are revealed, additional investigation methods involving their exploitation can be applied:

– white-box scanning of CBCS components using obtained accounts;
– configuration analysis of CBCS components that were accessed via vulnerability exploitation;
– gaining control over CBCS components and using them as additional access points.

Vulnerability detection stage is considered to be finished when all applicable methods have been applied.

Based on the investigation results, a report is drawn. It contains a workflow description, a list of revealed vulnerabilities and facts of CBCS defence features blocking the investigators' activity. The weaknesses and vulnerabilities revealed in the course of assesment are described in the report as follows:

- weakness name;
- weakness description;
- recommendations on weakness elimination (solution);
- additional information.

The weakness name sums up the weakness type and software/hardware components affected. The description provides insight into the weakness along with exploitation methods and potential attack impact; it also should provide qualitative (critical, high, moderate, low) and quantitative estimation of the risk level.

The solution describes measures suggested to eliminate the weakness or, if it is not possible, to prevent its exploitation or mitigate the damage. The additional information can contain links to public weakness descriptions that help eliminate the weakness or analyze the results of its exploitation.

To perform threat analysis, it is suggested to use a partial model of CBCS threats. In this model, the following components are used:

- a CBCS model describing network and system interconnections between the components, as well as the existing functional and IT security mechanisms;
- a detailed threat model adapted to the certain CBCS with regard to the actual attack vectors and intruder model;
- a list of vulnerabilities revealed in the course of security assessment.

CBCS Model and CBCS Threat Model

For CBCS vulnerability and threat analysis, it is necessary to build a partial threat model based on typical traffic safety, economic efficiency and reliability breaches. A system model is constructed to identify attack vectors. It is very important to describe all possible operating modes, because different modes (normal, emergency, maintenance, etc.) can have different attack surface.

A CBCS model allows one to analyze conduction of attacks exploiting various vectors and vulnerabilities, as well as to consider possible security implications of successful attacks. The model is based on the system block diagram coupled with the description of internal and external interaction channels.

Usually, basic models of one-class CBCSs (e.g., Power Interlocking Systems, PISs) can be standardized. To adapt the standard model for a certain system, it is necessary to consider the following features:

- network protocols that are used;
- built-in functional protection tool;
- built-in or typical IT security tools;
- integration capabilities and interfaces for interaction with external systems.

In cybersecurity, a CBCS functional module is considered to be important, if it:

- has (or can have) internal security mechanisms, which means that it serves as a security boundary separating areas with different security levels and is an issue for an attacker;
- can be subject to an attack.

Let us consider an example and build a CBIS model. Typical CBIS components are described in below.

Component	Description
Signaling, centralization and blocking (SCB): trackside devices Switch motors and signals	An intruder can try to capture control over the trackside equipment, but usually the attack is not targeted against the devices themselves, since their interfaces are not advanced enough. However, if a radio-control system is used to manage switch motors and signals (i.e. object controllers send codes to the radio channel rather then apply voltage to the assets), then such systems can be subject to an attack and therefore should be decomposed and included into the model.
Central Processing Unit (CPU) or Central Station Unit (CSU)	These units receive instructions from workstations and other systems along with status information about trackside devices; they then use interlocking rules to decide whether a command is allowable in the current traffic situation. CPU/CSU is usually implemented as special-purpose software on the basis of a general-purpose OS (Unix, Linux, QNX). These units provide the basic mechanisms for functional safety and failure reliability (duplication of computational nodes, troubleshooting, interlocking control). They interact with object controllers and workstations. CPU/CSU is a high-priority target for attackers, because it controls power interlocking and implements functional safety features.
Interlocking Processing Unit (IPU)	The unit performs the main tasks related to controlling signal interlocking and switches and enables compliance with traffic safety requirements. IPU can be implemented as an additional duplicated CPU/CSU module.
Object controllers (OC)	Object controllers receive instructions from the CPU and convert them into control signals meant for trackside devices; OCs send information on the state of the controlled objects back to the CPU/CSU. Object controllers can perform certain functional safety and interlocking functions. Depending on implementation, these components can be high-priority targets for attackers, because they allow one to carry out administrative actions bypassing the interlocking system.
Workstations	Workstations serve as Human Machine Interfaces (HMIs) and allow operators (centralized dispatching operators, signal or communication technicians,

	yardmasters and others) to monitor the traffic situation, the state of signaling, centralization and blocking assets, and send commands to the PIS. Workstations are usually implemented as special-purpose software on the basis of personal computers running a general-purpose OS (Windows). They provide a graphic user interface for operators to interact with the control system, to send instructions and to analyze the received diagnostic data. Workstations can have internal protection features. These components have a large attack surface, because they have multiple network and hardware interfaces (e.g. USB) and interact extensively with other power interlocking components and employees, which enables social engineering methods.
Network equipment: switches, routers, converters, modems, SIM cards, wireless access points, etc.	These are devices that provide interaction between the components. They can support both common protocols (Ethernet, IP, 802.11, 802.15, GSM, etc.) and special-purpose/legacy protocols (IEC 61158, Profinet, HDLC, etc.). Network communication is a usual attack vector. Network equipment can be a target for attackers, because it provides considerable computational capabilities, remote administration tools, etc.
Network protocols	Network protocols provide interaction between CBI components. A cyber threat model should account not only for transportation protocols (Ethernet, TCP/IP, HDLC, GSM, etc.) and protocols implementing the CBI logic, but also for service protocols implementing diagnostics, remote control, OS/DBMS interaction, etc. Features and vulnerabilities of network protocols sufficiently influence the possibility to conduct various attacks.
Communication channels	In CBIs, different communication channels can be used: Current Loop for CPU/OC interaction, wireless or backbone links for integration with other systems, etc. Communication channels represent one of the most popular attack vectors.
Signalling integration junctions and gateways: centralized traffic	These components enable diagnostics information, information on SCB device status and train position, as well as control instructions to be exchanged with adjacent systems.

and dispatch control systems, automatic block systems, and other CBI systems	Integration junctions and gateways expand the attack surface, because they make the CBI a part of a distributed system, which provides more opportunities for remote attacks. Usually, security requirements to centralized traffic control systems are lower than those for computer-based interlocking systems, which should be taken into account in case of their integration.
Employees	Operators (yardmasters, SCB technicians), system administrators, vendor support employees.

The described decomposition is sufficient to solve most practical problems. However, if you need to perform a detailed analysis (e.g. for attack simulation), do not forget that the above-described components are not monolithic. For example, a CPU/CSU consists of several logic blocks that use different hardware devices and OS instances. These blocks usually provide reliability mechanisms, result comparison with majority circuits, functionality testing, and implement control and interlocking algorithms. One can see that a CPU/CSU are multi-component systems with explicit security boundaries; this fact should be translated into the CBCS model.

To build a consistent threat model, one should consider all attack vectors, i.e. access points and targets of potential intruders in all attack phases. In below a CBI model is given with possible attack vectors shown as red arrows.

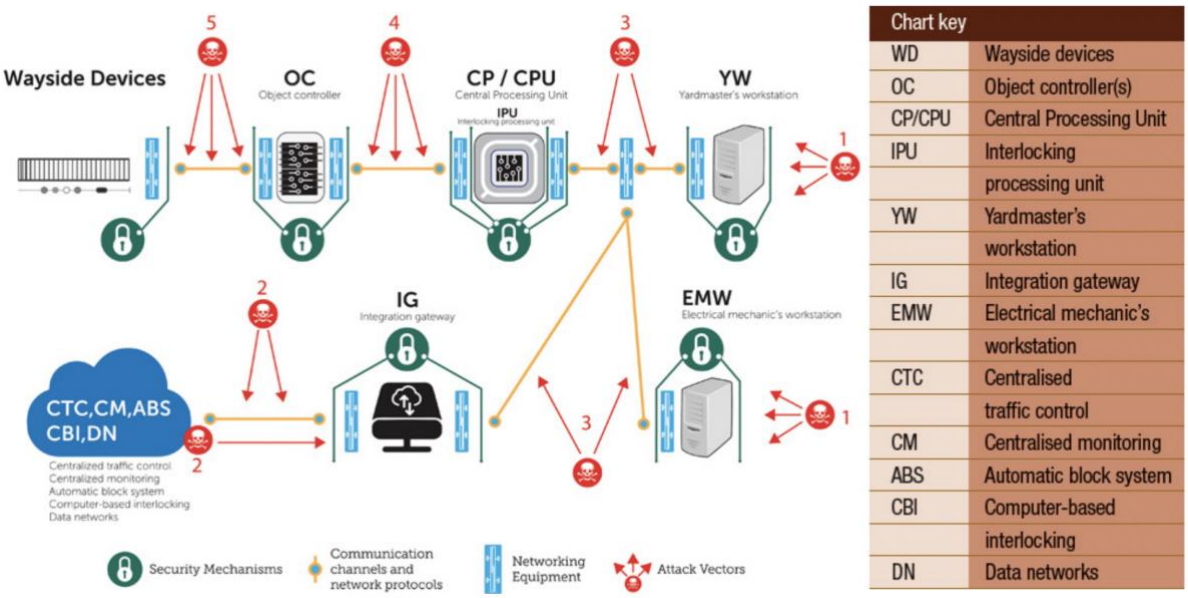


Figure 43. CBI model and attack vectors

An attack is usually possible where an external interface allows an intruder to influence the target.

Attacks can be either local or remote. Opportunities for remote attacks often depend on the technical implementation of interfaces. For example, attack vector #5 is usually considered to be local, because an intruder can power a signal light or a switch motor by accessing the cable between an object controller and a trackside device. However, remote attacks become possible if trackside devices are radio controlled.

Attack vectors

Vector	Interface	Target	Type	Examples
1 and 1’	Workstation software and hardware interfaces	Technician workstations Yardmaster workstations	Local	Social engineering, connecting peripheral equipment (USB Flash, modems)

Vector	Interface	Target	Type	Examples
2 and 2’	Integration communication channels, centralized traffic and dispatch control networks, DCNs	Signalling integration junctions and gateways Network equipment Network protocols	Remote	Connecting communication channels, compromising centralized traffic and dispatch control systems, compromising DCN equipment, compromising network equipment
3	CBI LAN	Technician workstations Yardmaster workstations Signalling integration junctions and gateways CPU/CSU Network equipment Network protocols	Local Remote	Physically connecting to LAN Connecting to wireless channels Compromising workstations, signalling integration junctions and gateways, and network equipment
4	Links to object controllers	CPU/CSU Object controllers Network equipment Network protocols	Local Remote	Physically connecting to link channels Connecting to wireless channels Compromising object controllers, compromising centralized traffic and dispatch control systems, compromising CSU, compromising network equipment

Vector	Interface	Target	Type	Examples
5	Links to trackside devices	Object controllers Trackside devices	Local Remote	Physically connecting to wired and wireless connecting channels Compromising object controllers and network equipment

Building a partial model allows one to implicitly take into account possible undocumented features. A component containing undeclared features is marked as compromised and is considered to be an interface for attacks. However, if discovering undocumented features is one of the main modeling purposes, then these interfaces should be shown explicitly.

To analyze CBI threats, let us use three-level mission-centric classification[71] based on railway operating rules and other principal requirements:

1. Traffic safety breaches.
2. Reduced transportation efficiency.
3. Other breaches of functional safety and reliability.

Threats resulting in functional safety breaches are usually the most difficult to implement and require the greatest efforts by intruders. To be successful, an attacker must bypass the CBI functional safety mechanisms. If object controllers are not available for direct impact (e.g. via radio-channel vulnerabilities), then an attacker needs to modify the operating logic of the main CBI modules implementing switch and signal interlocking, which is a sophisticated task. However, if successful, an attacker will be able to:

1.1 Change a signal aspect to green for a route with occupied tracks (false track vacancy).

[71] Sergey Gordeychik, Denis Baranov, Gleb Gritsai. Cyber threat model for Computer Based Interlocking

1.2 Set a signal to less restrictive aspect (e.g. green aspect at diverging switch).

1.3 Operate a switch with a train passing over it.

1.4 Handle a train over a trailed point.

1.5 Set conflicting routes.

Threats aimed at reduction in transportation efficiency do not usually require an attacker to be high-skilled and can be implemented using standard malware. It makes these threats more likely to be put into practice, because it does not require development of special-purpose tools. Here are examples of such threats:

2.1 Putting CBI out of operation.

2.2 Blocking control for a long time.

2.3 Displaying false traffic information in the yardmaster workstation.

2.4 False occupancy.

Putting non-redundant components such as CPU/CSU out of operation will cause CBI denial of service and force the stuff to change-over to manual control. It will reduce the efficiency of transportation management. Spoofing and blocking network interaction between the yardmaster workstation and CPU/CSU or continuously rebooting these components can result in long-term system's unability to send commands. It will require a switch to manual operation and sufficiently reduce the transportation management efficiency. Spoofed interactions between the yardmaster workstation and CPU/CSU can be used to indicate false occupancy of a track circuit or display incorrect train positions in the yardmaster workstation, which will require additional control from the yardmaster.

The following threats reduce the overall system reliability:

3.1 Temporary putting the CBI out of operation.

3.2 Putting service equipment out of operation.

3.3 Displaying false diagnostics information in the station technician workstation.

Temporary putting the CBI out of operation by rebooting CPU/CSU or yardmaster workstation shortens the run-to-failure time (which is defined for software products as the time until completely restarting a program or rebooting an OS). This can be achieved through a variety of attacks, including attacks aimed at exhaustion of network and computational resources (Denial of Service, DoS) and attacks against network equipment that modify configuration, TCP/IP or Ethernet parameters and remove/replace firmware.

To conduct an attack, intruders exploit vulnerabilities and weaknesses of CBI components. It is usually necessary to conduct a series of attacks to implement a threat. Let us consider some possible attack chains that allow one to implement certain threats shown above.

The threat *3.1 Temporary putting the CBI out of operation* can be put into practice via attack vectors 1, 1', 2, 2', and 3. To do so, an attacker can exploit vulnerabilities in workstation OS (e.g. if security updates were not installed or an obsolete operating system like Windows 2000/XP is used), vulnerabilities in CBI software, weak OS passwords, etc. Another chance to implement the threat 3.1 is to attack communication channels and network protocols: to flood communication channels, to introduce false routes (e.g. via ARP Spoofing), etc. Most of the mentioned attacks can be conducted using general-purpose malware aimed at infecting Windows OSs. To attack the system via vectors 1 and 1', a malicious person can use social engineering methods. For example, an attacker can trick a yardmaster into inserting a USB flash containing malware or performing actions that will cause a denial of service. To attack the system via vectors 2 and 2', it is necessary to bypass security mechanisms of the integration gateway first (in case this component is present in the system and has its own protection features).

The threat *2.3 Displaying false traffic information in the yardmaster workstation* can iplemented via attack vector 3'. To do so, an attacker can manipulate network traffic between the yardmaster workstation and CPU/CSU, if the corresponding protocol is vulnerable. Other vectors for this threat require multi-stage attacks to be conducted, e.g. obtaining unauthorized access to a workstation via attack vector 1 or to signalling integration junctions and gateways via attack vectors 2 and 2'.

The easiest way to implement *Traffic safety br*eaches is to use attack vectors 1, 1', 2, 2' and 3. An intruder needs to successively bypass the protection mechanisms of signalling integration junctions and gateways, CPU/CSU, IPU and object controllers, which will require a high level of skills. On one hand, CPU/CSU and IPU implement integrity control features and protect the interlocking logic from unauthorized modification, which diminishes attacker's chances. On other hand, if attacks via vector 5 are possible (by data manipulation or man-in-the-middle attacks against communication channels between trackside devices, object controllers and CPU/CSU), then attack complexity is significantly reduced.

It should be mentioned that threat models can have different levels of detail: from a simple list to a symbolic model. The suggested approach to threat simulation based on CBCS model allows one to identify the most probable attack vectors, the corresponding protection mechanisms and system cyber security weaknesses.

This approach can be easily adapted for other CBCS types. For example, a computer-based classification system model should include both the basic CBI elements and additional threats related to gravity classification.

Threat model extension for a computer-based classification system

Main threats	**Description**

Classification safety violations: − switching points when a track is occupied with a cut of cars; − side collision of rolling-down cuts; − collision of a train and an overspeeding cut carrying dangerous goods; − derailing a cut due to overbraking by retarders.	Threats of this type are related to violation of safety rules defined in railway operating rules, railroad signaling regulation, rail traffic safety instructions, and other ruling documents. Threats to traffic safety are most critical, because they can lead to death of people and destruction of trains and station equipment.
Reduced classification efficiency: − issuing wrong and poor commands to trackside equipment; − sending false data to adjacent systems (Automated Control Systems and Hardware and Software Complexes for Supervisory Control); − displaying wrong classification information in the yardmaster workstation; − putting certain components out of operation.	Threats of this type are related to the fact that system's components directly participate in control and optimization of railway cars separation on a hump. Violation of the system's normal operation influences (implicitly or explicitly) the operating mode, selection of routes, etc., which in turn affects the classification efficiency.
Threats that do not affect classification but result in operational and financial losses: − physical denial of service of separate system's components	Threats of this type can be used to reduce performance of the whole system or its separate components, as well as to shorten time-to-failure for the whole system or its components. Successful attacks lead to operational and financial losses, since it is necessary to recover the damaged components. Meanwhile, only the components' operability suffers; control functions are not affected.

Mission-centric approach to CBCS threat analysis allows one to ditch rather abstract concepts of integrity, availability and confidentiality violation in favour of building a threat model based on the requirements to traffic safety, economic efficiency, and functional safety.

Graph synthesis and analysis are common methods in IT security, but it is difficult to use them in practice. For example, investigators failed to calculate the complete graph of attacks for a UNIX host filesystem containing only thirteen vulnerabilities. However, relative simplicity of CBCSs allows experts to apply this methods if certain assumptions are admitted.

Mathematical and simulation modelling significantly enrich the threat model and allow one to optimize security and cyber safety assessment, as well as to choose and rationalize the set of protection features.

Identifying Weaknesses and Vulnerabilities

To identify CBCS weaknesses and vulnerabilities, lab and/or field research should be carried out using a methodology based on the threat model in order to find as many vulnerabilities and weaknesses as possible. A variety of methods are used, such as:

- Analysis of the physical security of a facility, the CBCS and its components.
- Detection of known vulnerabilities via vulnerability scanners.
- Manual and automated examination of configurations of the components (network equipment, OS, DBMS, etc.) for compliance with vendor recommendations and best practices.
- Analysis of authentication and access control mechanisms, examination of password policy, identification of standard and fixed passwords and encryption keys.
- Survey of the work of operators aimed to identify any violation of security requirements in their established practices (bypassing the limitations of graphical interfaces, connecting external devices, etc.). It is recommended to carry out this investigation in actual workplaces.
- Analysis of network communications, including those carried out over wireless connections.
- Analysis of system maintenance procedures and tools, including those using remote management features.
- Identification of security mechanisms and test of their efficiency.
- Examination for compliance with technical requirements.

Let us elaborate the stages of source code and network communication analysis.

The source code is analyzed according to the OWASP Code Review Guide, which combines two areas of investigation:

– searching for typical programming errors;

– searching for typical errors in implementation of certain security features.

Searching for typical programming errors implies searching code for fragments that contain programming errors that cause vulnerabilities. The search is targeted and use criteria designed to identify certain classes of programming errors. Generally, the following errors are searched for:

– buffer overflows;

– injection of control expressions (OS commands, SQL statements, operators in coding languages, etc.);

– errors in synchronization of parallel computing processes;

– errors in handling runtime failures and exceptions;

– specific web application errors (cross-site scripting, session identification errors, etc.).

Searching for typical errors is performed using both automated source-code analysis tools and manual analysis. Searching for typical errors in implementation of security features combines automated and expert analysis methods. This includes:

– identification of the source code fragments implementing the main security functions;

– static analysis of the algorithms implementing security functions;

– dynamic analysis of algorithm execution by emulating source code execution or debugging using test data, including the use of standard methods of vulnerability exploitation.

When defining the scope of work and evaluating the investigations carried out to analyze the source code, one should keep in mind that this method of vulnerability detection has the following application restrictions:

– analysis can be only performed for a certain set of programming languages restricted by the tools used and the existing analysis procedures;

– analysis is aimed at identification of certain classes of vulnerabilities and standard errors in security implementation;

– analysis is performed locally at the level of separate software functions and modules, and thus can fail to identify architectural vulnerabilities and IT-level vulnerabilities and security implementation errors.

The investigators should make independent decisions on the set of security features to be analyzed in the course of security assessment. Here, they will refer to the programming language used, the architecture of computer equipment used to execute the source code, availability of applicable analysis methods and tools, etc. Usually, implementation of the following security features is assessed:

– identification and authentication;

– access control;

– session management;

– input data validation;

– handling runtime errors and exceptions;

– generation and storage of audit data;

– cryptographic functions and encryption-key management.

Analysis of network communication is used as an auxiliary method of passive vulnerability analysis to solve the following problems:

– passive inventory of CBCS components, including identification of nomenclature and versions of OSs and other software products;

– identification of information flows that reveal the CBCS topology;

– detection of forbidden types of interaction and information flows that indicate malware activity;

– detection of confident and sensitive information (including login credentials) being communicated insecurely (i.e. as plain text).

In addition, it is reasonable to include analysis of communication hardware such as network modems, (U)SIM cards, GSM-R and SDR stations. Such devices represent rather sophisticated computer systems in which vulnerabilities have been previously revealed. These vulnerabilities allow a malicious person to attack the entire CBCS infrastructure.

As a result of this investigation, a list of CBCS weaknesses will be generated. Some of these weaknesses can prove to be vulnerabilities. At the next stage, the weaknesses are assessed and identified as vulnerabilities. This can be done in one or several ways:

- to show in practice how a vulnerability can be exploited to pose a real threat to cyber security;
- to describe in theory how a vulnerability can be exploited to pose a real threat to cyber security (the description should raise no objections from CBCS specialists);
- for known source-code vulnerabilities: to find the description of a vulnerability in one or several vulnerability scanner data bases or in a vendor security bulletin related to update eliminating this vulnerability;
- for unknown or unpublished vulnerabilities: to obtain a message from the vendor that confirms the weakness to be a vulnerability;
- for obsolete and unsupported software products: to find a press release or another statement that confirms termination of software support;
- for configuration errors: to find a release by vendor or other authorities that recognizes the given configuration to have negative impact onto the cyber security of the entire CBCS or its separate components.

The severity of confirmed vulnerabilities can then be estimated and recommendations can be formulated to address them.

If a previously unknown vulnerability is revealed in the course of security assessment, then the testing laboratory team should inform the CBCS developer by sending a vulnerability notification.

The collected data are then used to analyze cyber security threats. This involves construction of attack sequences (the attack graph) that meet the following conditions:

- for each attack, there is a vulnerability in CBCS that allows one to conduct it;
- by the beginning of a certain attack, the intruder has all necessary capabilities to conduct it (the capabilities can be initial or obtained as a result of previous attacks);
- the final attack implements one of the objective threats.

To construct a directed graph of attacks, one should take the final attacker's target as the initial graph node. At the first stage of analysis, investigators determine vulnerable CBCS components that allow an attacker to implement one or several objective threats. Here, the capabilities required to conduct attacks against these components are determined. Next, vulnerable CBCS components are determined for every attacker's capability; these are the components that, if compromised, will give an attacker the requires access level. The process is then repeated until either there are no more CBCS vulnerabilities to consider or the vulnerabilities already included into the graph are necessary and sufficient to conduct all the attacks in question (taking into account that an attacker successively obtains new capabilities with every new attack conducted).

The next stage of security assessment involves examination for compliance with state, industry and international standards, recommendations and best practices. At this stage, the goal is to find requirements that the CBCS doesn't meet or meets badly. For these works, it is useful to have a correlation table for

the requirements given in different standards. For example, one can find such table for Order #31 by FSTEC of Russia, NERC-CIP (REV5 – DRAFT), IEC-62443-2-1 (ISA99.02.01), and NIST – SP800-82, NIST – SP800-53 in the document *Correlation of Requirements Given in Order #31 by FSTEC of Russia with International Standards*.

Results of Assessment

The results of cyber security assessment are listed below. They can be represented in the form of various documents.

- Description of vulnerability analysis workflow (including the the facts of system's counteraction).
- A list and description of detected vulnerabilities along with their severity levels.
- Solution (how to eliminate the vulnerabilities).
- A graph of attacks in the form of a chart or a free-form textual description.
- A list and description of cyber security threats that can be implemented for the current CBCS security level.
- A summary table that shows compliance with separate CBCS security requirements.
- Description of weaknesses in implementation of CBCS security requirements and recommendations how to improve.

If automated tools (such as security control tools, source-code analysis tools, configuration control tools, etc.) have detected multiple vulnerabilities and generated vulnerability descriptions, then these descriptions can be included into the report.

The obtained data can be further used to solve various problems. Examples are given below.

- Elimination of revealed vulnerabilities in cooperation with the RTA CBCS vendor.
- Examination for compliance with regulatory requirements.
- Development of particular methods to analyze and improve the security level of the given CBCS class.
- Development of a standard project for improving cyber security resilience of objects that use CBCSs.