Resilient Architectures in Railway Signalling

CYSIS workgroup

TECHNISCHE UNIVERSITÄT DARMSTADT

DB Mobility Networks Logistics

CYSIS Cybersecurity für sicherheitskritische Infrastrukturen

Photograph: DB AG

Introduction

Railway control and command technology (CCT) undergoes constant change. Whilst exclusive recourse was had to proprietary systems and protected communications infrastructure in the past, the use of commercial off-the-shelf (COTS) devices and public networks will take centre stage in future. Although a high level of safety has already been achieved in CCT, these new environments are already making high demands on IT security. "Resilient" infrastructure, which can maintain its essential functions despite attacks, is required, in order to meet the increasing threat from the higher sophistication and greater number of attacks on communications networks. Mere perimeter protection is no longer sufficient. On the contrary, a strategy of defence in depth is advantageous, providing multiple layers of protection combined with detection and reaction mechanisms.

The "Resilient architectures" project of the Cybersecurity for Critical Infrastructures workgroup (CYSIS) has examined resilience concepts in the field of railway CCT intensively. This white paper contains recommendations of how resilience to IT security incidents in CCT can be achieved. It is the result of intensive discussions between academia, operators and manufacturers. This document does not claim to be comprehensive, but rather describes properties which the workgroup considers important for a resilient system and which can be used to harden future CCT.

Definition of resilience

This section focuses on the definition of the concept of resilience is on technical systems and primarily on the characteristic of IT security. For this purpose, a general definition of resilience is first provided. It is largely derived from existing definitions, in order to ensure inherent consistence with other bibliographic definitions of resilience. This general definition is then refined, firstly for the purposes of railway infrastructure in the form of CCT and secondly for the purposes of IT security.

General definition of resilience within the framework of CYSIS

The following definition of resilience is provided within the framework of the CYSIS workgroup. It relies mainly on the definition by the National Institute of Standards and Technology (NIST), 2013:

The resilience of an IT system in terms of IT security is characterised by the following capabilities:

a) The system and organisation should be prepared for unfavourable conditions and/or extraordinary stresses.
b) The system should be able to react to unfavourable conditions and/or extraordinary stresses and maintain its essential functions, despite potentially restricted functionality.
c) The system should be able to return to a defined state after an acceptable time.

Specifications of *resilience* for the field of railway infrastructure (CCT)

The definition of *resilience* provided in the previous section has been deliberately kept general and will be refined for the field of railway infrastructure in this section, i.e. specifically for the field of control and command systems, within the scope of the CYSIS workgroup.

The definition of the *resilience* of a system is based upon the ability of the system to function under the influence of unfavourable conditions and/or extraordinary stress. This general statement must be restricted to safety systems, as a reduction in the functionality of a safety system is only acceptable if the functional safety of the entire system is not inhibited inadmissibly. In terms of *resilience* of safety systems, this means that the requirement for additional, self-evident safety of the entire system must also be fulfilled.

The phrase "**unfavourable conditions and/or extraordinary stress"** only covers incidents relevant to IT security, i.e. attacks within the meaning of standard IEC 62443.

"**Restricted functionality**" means that the system works on a backup level at reduced efficiency, but with the safety of the entire system guaranteed.
Classification of a function as "**essential"** should be the responsibility of the organisation, authority or industry. In general, the following functions should be classified as "*essential*":

- "*Essential functions*" within the meaning of the definition in IEC 62443-3-3: "*function or capability that is required to maintain health, safety, the environment and availability for the equipment under control*"
- All functions which are necessary to ensure the operation of an essential function within the meaning of IEC 62443-3-3, e.g. power supply, ventilation, etc.
- Functions which are mitigation functions to ensure resilience are: Identify, Protect, Detect, Respond and Recover

The definition of the **"defined state"** should be the responsibility of the organisation, authority or industry. However, in general it may be stated that even after an attack on control and command systems, the entire railway system must be in a position to fulfil the requirements of the German IT Security Act or the corresponding order.

Demands made on resilient architecture

End-to-end communications security

As large, complex networks are not usually under the full control of the operator and therefore not all their characteristics and interfaces are known, it is expedient to assume that unauthorised access can no longer be precluded.

End-to-end security of the communication path between subscribers is therefore necessary to ensure the authenticity and integrity of data. Confidentiality is not a prime objective of CCT.

Adaptability

Especially COTS systems (e.g. operating systems) are undergoing pronounced change. For this reason there will be a need for readjusting, patching and substituting processes. They are countered by certification and approval processes, which are considerably more laborious than has been usual in the IT field. Three basic principles of adaptability can be derived from this:

- Safety-critical parts should be encapsulated and longer-lasting, if possible
- Components requiring a higher frequency of modification (e.g. COTS factors and cryptographic processes) should be structured so that changes and evidence of non-intrusiveness (within the meaning of EN 50129) are possible without substantial changes to safety cases
- Only features, services or components which are necessary to provide the functionality should be used. Features, services or components which are not required should be switched off, deactivated or uninstalled

If COTS systems are used, it must be assumed that weaknesses will also be publicised by third parties with a relatively short lead time. Rectification and mitigation measures and reaction times in the railway environment must be agreed between manufacturers, operators and regulatory authorities.

Analysis capability and observation

The components and network of a railway safety installation must be observable and analysable in future. Interfaces with management systems may need to be agreed and sensors provided in the network for this purpose.

Data aggregation and reaction

In future, a critical aspect will accrue to diagnosability, observation and analysis of and the reaction to critical events. It must therefore be made possible for the available information on network status (by sensors) to be aggregated and system integrity (code and configuration) to be made available at a central point and examined for anomalies. A process for reacting to anomalies must be specified.

Dependency on diagnostic systems and situation centres must be specified.

Data filtering

Facilities for filtering data must be provided within the transmission system of the command and control installation. Data filtering facilities are ideally located at danger transition points. These represent limits of integrity areas or points of service (PoS). It is important that failure of data filtration be disclosed promptly. Filtering itself takes place under specified rules, which should ideally satisfy a white listing. Infringement of security rules must be disclosed.

System integrity run time test

Functionality in modern systems is largely determined by code and configuration, the integrity of which is crucial. It must therefore be established whether the code on the system and the configuration correspond to the state on acceptance. It must be possible to test the integrity of a component verifiably. The quality of the integrity test must also be ensured in a compromised system.
A reliable run time test may be run by using, for example, trusted boot, trusted platform modules (TPM) or similar concepts.

Attestability of integrity to third parties

It must be possible for the integrity of the system, code and configuration to be tested externally. It must be ensured that the current integrity status is attested. A process must be defined which examines the integrity of all the relevant systems regularly. The test cycles must be defined on the basis of the application and IT security level.

Logging critical events

Critical events, e.g. changes to the configuration, must be logged, to facilitate the traceability of attacks. On the basis of the application and the security level, it must be specified which events are to be regarded as critical. Subsequent amendments to the log must be prevented or at least detected.

Simple transferability of the configuration to replacement devices

In order to be able to replace a component quickly and safely it is not sufficient to replace the hardware. The configuration data must be transferred as well (e.g. by smartcard or download). Simple, rapid, secure transferability of the configuration should be ensured. Reaction and rectification times depend upon the respective device/system.

Warning of weak IT security settings

It should be possible to detect weak settings (or e.g. obsolete cryptographic algorithms). It must be possible to read out component configurations for this purpose. A suitable point for evaluating configurations and generating any warning must be specified. A suitable interval must be set for the period between two tests. The necessity of deliberate acceptance of weak configurations, e.g. to achieve necessary compatibility, must be examined.

Modular architecture to restrict a compromise

Modular system architecture is intended to facilitate the isolation of units without restricting system functionality more than is necessary. Isolation is used to restrict the effects of a compromise. Diversified infrastructure can also contribute to isolation of a compromise. It should be noted that the location of the effect of the compromise is not necessarily the point of attack and that not all the compromised components have been detected.

Detection of physical attacks

It must be possible to detect a physical attack on essential components. This should enable disclosure of unauthorised access and associated potential compromises. For example, essential installations can be protected by intruder alarms. Any interference will be evident immediately. Less essential installations can be e.g. lead-sealed. Interference is detectable later.

Cryptographic keys must be generated and stored securely

The security of a cryptographic system is wholly dependent on the secure generation and confidentiality of cryptographic keys. A secret key which can be read by an authorised party is compromised and endangers IT system security. Cryptographic keys should be stored on secure hardware and not removed from the hardware module.

Restoration of original or backup state

Ensuring that compromised state is not created immediately after successful creation of backup state represents a major challenge. An operational and/or technical response plan must be created for this purpose.

The system must be capable of making a secure mode available to the entire system or constituent systems, for which intensified monitoring is necessary. Data must be made available for analysis/forensics following a compromise.

A process for the secure replacement of cryptographic keys must be supported

A key replacement process must be supported, in order to replace secret key material securely and remotely. The process can be used, for example, for regular key replacement when upgrading to better cryptographic processes or if the system is compromised.

Fault mode achievable

It should be possible to isolate a subsystem from the entire system if the former is compromised. This provides an opportunity to carry out analyses without endangering the entire system. It should only be possible to reintegrate it after restoration of the original mode following operator intervention. Component monitoring must follow.

System margins

The system must be configured as future-proof. Sufficient margins for the highest available log level, analyses and updates must therefore be provided. This affects new software versions, new cryptographic keys and improved key processes.

Asset and configuration management

Knowledge of the mode and integrity of the entire system is absolutely necessary in order to detect and evaluate changes, estimate risks of change and diagnose faults. For this purpose, an asset and configuration management system corresponding to the current standard (ITIL V3) must be established and operated. This contains a model of the system which itself contains all their components and their target status (including the software status, version, certificate and checksum) and their interrelationships. The system model must be tested continuously and modified as necessary. Interfaces for the automatic detection of the actual status must be provided in the components to the greatest possible extent.

Annex

I. Notes on the definition of resilience

The concept of *resilience* is used in different fields of science, society and engineering, and generally describes the resistance of a system to extraordinary stresses and/or unfavourable environmental conditions. The extent of the systems under observation covers socio-ecological systems and technical systems such as command and control systems in various fields of engineering. For this reason, a variety of specific definitions of *resilience* exists, influenced by diverse specialisms. Reference is made to two documents (Petit, Phillips, Verner, & Whiteld, 2012) and (Community & Regional Resilience Institute (CARRI), 2013) as examples from the extensive bibliography on the subject, with no claim to completeness, which provide an overview of the most common definition of *resilience* in different disciplines.

Definitions from different sources have been evaluated to define *resilience*, with the following definitions of the term having emerged as a suitable basis for further work.

- Glossary for the internet platform for the protection of critical infrastructure (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016)[1]:
  Resilience
  is the ability of a system to cope with changes. Resilience means resistance to faults of any description, the ability to adapt to new conditions and a flexible reaction to change, with the objective of maintaining the system, – e.g. an operation or process.

- Publication by NIST (National Institute of Standards and Technology (NIST), 2013):
  Information System Resilience
  The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

- ANL summary (Petit, Phillips, Verner, & Whiteld, 2012):
  Resilience
  The ability of an entity — asset, organization, community, region — to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance.

In conclusion, the essential definition of *resilience* may be interpreted as meaning a system characteristic which serves the retention, defence and restoration of the working order of availability of the system under consideration in a case of extraordinary stresses and/or disadvantageous environmental conditions.

The ANL specifies this umbrella functional requirement by splitting the concept of *resilience* into the following six sub-functions: (*to anticipate, resist, absorb, respond, adapt* and *recover*), which can be attributed to the typical timeline of an incident (see Fig. 1 below).

[1] German federal offices: BSI : Federal Office for Information Security ; BBK: Federal Office of Civil Protection and Disaster Assistance

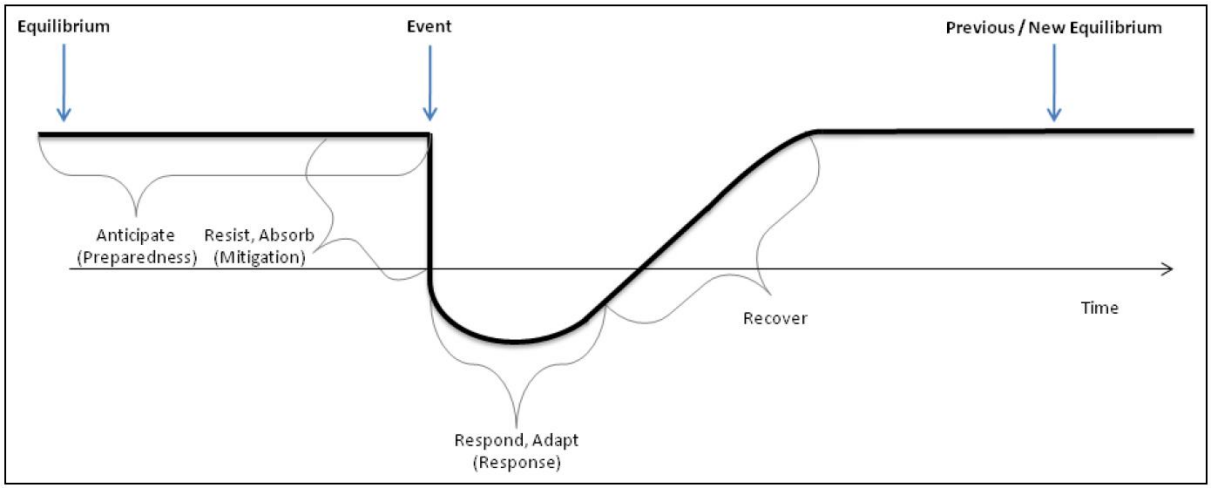

Fig. 1: Sub-functions of resilience against the background of an incident scenario (Argonne National Laboratory (ANL), 2012)

All the sub-functions are summarised in four groups of measures in the ANL document (Petit, Phillips, Verner, & Whiteld, 2012):

- ***Preparedness*** *(anticipate):* **(Preparation)**
  Activities undertaken by an entity to define the hazard environment to which it is subject
- ***Mitigation measures*** *(resist, absorb)**:*** **(Restriction of effects)**
  Activities taken prior to an event to reduce the severity or consequences of a hazard
- ***Response capabilities*** *(respond, adapt):* **(Launch counter-measures)**
  Immediate and ongoing activities, tasks, programs and systems that have been undertaken or developed to manage the adverse effects of an event
- ***Recovery mechanisms*** *(recover):* **(Return to a defined state)**
  Activities and programs designed to effectively return conditions to a level that is acceptable to the entity

The groups of measures identified in the ANL report are equivalent to the core functions for handling IT security risks defined in the NIST document (National Institute of Standards and Technology (NIST), 2013).They are:

- ***Identify*** *– Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities*
- ***Protect*** *– Develop and implement the appropriate safeguards to ensure delivery of critical infra-structure services.*
- ***Detect*** *– Develop and implement the appropriate activities to identify the occurrence of a cyber-security event.*
- ***Respond*** *– Develop and implement the appropriate activities to take action regarding a de-tected cybersecurity event.*
- ***Recover*** *– Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event*

If the ANL *mitigation measures* and *response capabilities* are formally summarised in the umbrella "*Reaction to the incident*" group of measures, the four groups of measures below emerge, which should be considered in order to establish *resilient architecture*.

I. **Preparation** for a potential or anticipated incident
This characteristic covers technical system design requirements and administrative measures, e.g. the establishment and maintenance of an IT security management system, an asset management system, the creation of a *risk tolerance policy*, the implementation of IT security risk analyses, etc.

II. **Detection** of a hazard
Detection of a compromised system and the detection of *passive attacks*, i.e. attacks intended to remain undetected, represents one of the major challenges to IT security.

III. **Reaction** to an incident:

a. **Mitigation of the effects** of a potential incident

b. **Response capabilities** as a reaction to an incident which has occurred

IV. **Recovery** to an acceptable state
Return to normal system operation in the medium- to long term represents the most crucial objective following the reaction to an incident.

The links to the above groups of measures and the corresponding NIST core functions emerge in the following table, using the general definition of resilience:

Table 1 Allocation of the measures identified and NIST core functions to the general definition of resilience

<table>
<tr><th>General definition of resilience</th><th>Group of measures</th><th>NIST core functions</th></tr>
<tr><td>1</td><td>2</td><td>3</td></tr>
<tr><td>The resilience of an IT system in terms of IT security is characterised by the following capabilities:</td><td colspan="2"></td></tr>
<tr><td rowspan="2">a) The system and organisation should be prepared for unfavourable conditions and/or extraordinary stresses.</td><td>Preparation</td><td>Identify
Protect</td></tr>
<tr><td>Detection of an event</td><td>Detect</td></tr>
<tr><td rowspan="3">b) The system should be able to react to unfavourable conditions and/or extraordinary stresses and maintain its crucial functions, despite potentially restricted functionality.</td><td>Reaction to the event:</td><td>-</td></tr>
<tr><td>Mitigation of the effects</td><td rowspan="2">Respond</td></tr>
<tr><td>Initiation of response capabilities</td></tr>
<tr><td>c) The system should be able to return to a specific state after an acceptable time.</td><td>Return to a defined state</td><td>Recover</td></tr>
</table>

The advantage of such direct compatibility of the definition of resilience with the corresponding groups of measures and NIST core functions is that direct links are also produced between the core functions in the NIST document (National Institute of Standards and Technology (NIST), 2013) and requirements from other standards, e.g. ISO/IEC 27001 and IEC 62443. This content may be used advantageously to derive later specific technical design requirements of and administrative measures for resilient architecture.

II. Detailing some requirements

Where necessary, further information is provided below on some of the requirements for resilient architecture specified in the white paper.

End-to-end communications security

Standard EN 50159 stipulates the conditions for the exchange of safety-critical data. Further protection-related objectives, such as integrity, timeliness, etc. are shown with measures in this standard.

Standard EN 50159 distinguishes between three categories of network with only the conditions for safety-critical data being stated here. Hazards are shown for each category and corresponding measures described. In the case of a category 3 network – i.e. unauthorised access cannot be precluded – cryptographic processes for data path security are prescribed. They are classified as B0 or B1 measures, i.e. cryptographic security plus an adequate safety code or use of a cryptographic safety code. This makes both tunnels and cryptographic attachments possible. Cryptographic attachments have the advantage that recording and analysis are possible at any point. If tunnels are used, this is only possible at tunnel endpoints. If cryptographic processes are used, separate safety codes or further cryptographic processes may have to be matched to each other, as errors (flipped bits) may have to be suitably disclosed.

It is assumed that the processes to be used will have to satisfy acknowledged industrial practice. Minimum requirements are set by European legislation or the regulatory authority (the Federal Railway Authority) or by administrative assistance from the Federal Office for Information Security.

Adaptability

System adaptability allows for e.g. software containing parts which are not necessary for specific use and which have therefore not been installed. In this way, software can be created for different operating conditions without having to develop and approve a system adapted to every situation.

Analysis capability and observation

These are required because the requirement for a punctual response (see the section "Data aggregation and reaction" below in the white paper) to IT security incidents is that the system be continuously monitored (see IEC 62443-3-3, Ch. 10.4 Continuous monitoring).

Data filtering

Data filtering is required in order to limit the propagation of a compromise. This is a constituent of the defence-in-depth strategy, according to IEC 62443-3-3, Ch. 9.4.2. Due to the division of the system into zones with different levels of security requirements within the meaning of IEC 62443, restriction by data filtering is necessary at the zone borders, so that a zone with high requirements is not rendered vulnerable by being connected to a zone with lower requirements.

Suitable architecture for filter solutions can be found in the bibliography and also in regulations, e.g. the basic protection catalogue of the German Federal Office for Information Security (BSI). Current solutions are e.g. the security translator system in accordance with LH 415.9104 or monitored firewalls.
Disclosure must take place to systems which are manned and monitored 24/7. In current CCT systems, this is the traffic controller's workstation or the KISA[2] security centre (KSC).

Attestability of integrity to third parties

Attestability is required in order to facilitate verifiability to third parties, e.g. the inspector or IT security officer, of the correct IT security configuration on commissioning, including recommissioning following an IT security incident, on service duration or upgrade/conversion of the system.

Warning of weak IT security settings

Following evaluation of the configuration and generation of the warning, systems or processes must be available in order to facilitate an appropriate reaction to the warning.

Restoration of original or backup state

It is necessary to distinguish between a compromisable and a compromised system state. Compromised system state means that a security vulnerability has become evident which could potentially be exploited, but has not yet been exploited in the system under consideration. The system state will change to compromised if the vulnerability is exploited. The system can only be affected if it is in a compromised state.
Cases are conceivable in which a state without security loopholes (not compromisable) cannot be achieved in an acceptable time. Such compromisable state may be suitable as a safe back-up state after an attack, if measures have been taken to monitor the extent of the compromise.

[2] Communications infrastructure for safety-critical applications

III. Allocation of the requirements to NIST core functions

The following table allocates the requirements listed in the white paper to phases of the NIST framework.

Function	Category	Subcategory	Requirement
Identify (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried ID.AM-2: Software platforms and applications within the organization are inventoried ID.AM-3: Organizational communication and data flows are mapped ID.AM-4: External information systems are catalogued ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Asset- und Configuration-Management
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated ID.BE-2: The organization's place in critical infrastructure and its industry sector are identified and communicated ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated ID.BE-4: Dependencies and critical functions for delivery of critical services are established ID.BE-5: Resilience requirements to support delivery of critical services are established	
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil	

		liberties obligations, are understood and managed ID.GV-4: Governance and risk management processes address cybersecurity risks	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk the organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources ID.RA-3: Threats, both internal and external, are identified and documented ID.RA-4: Potential business impacts and likelihoods are identified ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk ID.RA-6: Risk responses are identified and prioritized	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders ID.RM-2: Organizational risk tolerance is determined and clearly expressed ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	
PROTECT (PR)	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users PR.AC-2: Physical access to assets is managed and protected PR.AC-3: Remote access is managed PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	System integrity run time test (AC1) Data filtering (AC4, AC5)
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are	PR.AT-1: All users are informed and trained PR.AT-2: Privileged users understand roles & responsibilities	

	adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities PR.AT-4: Senior executives understand roles & responsibilities PR.AT-5: Physical and information security personnel understand roles & responsibilities	
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition PR.DS-4: Adequate capacity to ensure availability is maintained PR.DS-5: Protections against data leaks are implemented PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity PR.DS-7: The development and testing environment(s) are separate from the production environment	System integrity run time test (DS1) Attestability of integrity to third parties (DS6) End-to-end communications security (DS2) Cryptographic keys must be generated and stored securely (DS1) System margins (DS4)
	Information Protection Processes and Procedure (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained PR.IP-2: A System Development Life Cycle to manage systems is implemented PR.IP-3: Configuration change control processes are in place PR.IP-4: Backups of information are conducted, maintained, and tested periodically PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met PR.IP-6: Data is destroyed according to policy PR.IP-7: Protection processes are continuously improved PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery an Disaster Recovery) are in place and managed	Simple transferability of the configuration to replacement devices (IP4)

		PR.IP-10: Response and recovery plans are tested PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) PR.IP-12: A vulnerability management plan is developed and implemented	
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged in a timely manner, with approved and controlled tools PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy PR.PT-2: Removable media is protected and its use restricted according to policy PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality PR.PT-4: Communications and control networks are protected	Logging critical incidents (PT1) Warning of weak IT security settings (PT4) Modular architecture to restrict a compromise (PT3) A process for the secure replacement of keys must be supported (PT4)
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed DE.AE-2: Detected events are analysed to understand attack targets and methods DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors DE.AE-4: Impact of events is determined DE.AE-5: Incident alert thresholds are established	Analysis capability and observation (AE2, AE3)
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events DE.CM-2: The physical environment is monitored to detect potential cybersecurity events DE.CM-3: Personnel activity is	Analysis capability and observation (CM 1 to 7) Detection of physical attacks (CM2)

		monitored to detect potential cybersecurity events DE.CM-4: Malicious code is detected DE.CM-5: Unauthorized mobile code is detected DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed DE.CM-8: Vulnerability scans are performed	
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability DE.DP-2: Detection activities comply with all applicable requirements DE.DP-3: Detection processes are tested DE.DP-4: Event detection information is communicated to appropriate parties DE.DP-5: Detection processes are continuously improved	
RESPOND (RS)	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-1: Personnel know their roles and order of operations when a response is needed RS.CO-2: Events are reported consistent with established criteria RS.CO-3: Information is shared consistent with response plans RS.CO-4: Coordination with stakeholders occurs consistent with response plans RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery	RS.AN-1: Notifications from detection systems are investigated RS.AN-2: The impact of the incident is understood RS.AN-3: Forensics are performed RS.AN-4: Incidents are categorized consistent with response plans	
	Mitigation (RS.MI): Activities are performed to prevent expansion of	RS.MI-1: Incidents are contained RS.MI-2: Incidents are mitigated	Modular architecture to restrict a compromise (MI1. MI2)

	an event, mitigate its effects, and eradicate the incident.	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Fault mode achievable (MI2, MI2)
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned RS.IM-2: Response strategies are updated	
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events	RC.RP-1: Recovery plan is executed during or after an event	Restoration of original or backup state (RP1)
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned RC.IM-2: Recovery strategies are updated	
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centres, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed RC.CO-2: Reputation after an event is repaired RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	

IV. Handling IT security incidents in railway systems

A proposal is outlined below of how activities compliant with standards (e.g. NIST) entail activities and technology in a railway environment. The activities/technology are allocated to variants of traditional CCT v. IT technology. When introducing an IT process, the extent to which current CCT processes under guideline 892 need to be complemented by e.g. ITIL must be considered.

NIST core function	CCT variant 1 technology/activity (process analogous to current guiding principles)	CCT variant 2 technology/activity (procedure using IT processes)
IDENTIFY	Process: test and installation acceptance under directive 892 and administrative regulations governing construction, control for signalling, telecommunications and electromechanical systems (VV BAU STE) (also applicable to telecommunications systems with a safety function); plans, state of planning In future, identification of configuration items (KE) by identifier and other features (e.g. certification). Plan audit to be complemented by certificate audit. Technology: certificates will be used in addition to the pure technical identifiers (for plans). Such identity management certificates will be stored at the KSC. The certificate will also be used for access control (process, e.g. 802.1X). The inventory database is thus stored in the KSC. CCT is responsible for management. Checksums and any certificates are characteristics of configuration units. They will continue to be subject to self-testing. Certificates are audited in the KSC and may be withdrawn. Use of secure boot.	Process: the process in accordance with directive 892 and VV BAU STE is complemented by the ITIL process. An installation configuration management system is overlaid for this purpose. CCT also covers both signalmen and IT administrators. A target range is included, in addition to structural acceptance under directive 892/VV BAU STE. Load generators must be used for this purpose during acceptance. The target range is used as an input, e.g. for IDS[3]. Technology: a management system is used, in addition to the warning message on the traffic controller's workstation. The extent to which the management system is integrated into the acceptance process must be clarified. The management system also forms the inventory database and a link to the IDS. IDSs detect deviations from the target range. Operator responsibility has to be clarified. Manufacturer's responsibility for defining the target range. The original installed state can always be restored by using secure boot. The target state is also monitored afterwards. The management system can be used for patch rollouts for operating systems and firmware. Following a rollout, the desired state must be tested again. The validity of approvals and proof of non-intrusiveness must be clarified, as must the responsible disclosure time. Patch levels are also monitored by the management system.

[3] Intrusion detection system

PROTECT	Process: protection against unauthorised access under 50159 must be monitored by CCT. Deviations from the planned status are displayed on the traffic controller's workstation and documented (formerly "printed"). Technology: Connection to the CCT system is covered by certificates. Certificates are administered in the KSC. A password policy is used or a central log-in is introduced by a directory service (where the policy is stipulated). Fail-safe systems or additional suitable, accepted test partners are responsible for the integrity of the system. Networks have suitable segmentation (addresses and logical configurations). Guiding principles must be stored in regulations (e.g. 819.0705, 861.xxx). Cryptographic processes are generally used for transmission. The test processes also involve system parameters (white listing). Systems are hardened for the minimum configuration necessary.	Process: protection against unauthorised access and desired configuration management are monitored and displayed in the management system. Technology: Connection to the CCT system takes place in accordance with certificates and the desired configuration stored in the inventory management system of the management system. The password policy is monitored in the management system, possible availability of a central directory. CCT test systems only test specific applications. Application-dependent parameters/checksums/certificates may also be stored in the management system and monitored. Network segmentation is the responsibility of the IT administrators. Guiding principles are stored in the management system, which is designed as an umbrella system. Infringements are displayed here and notified to the responsible administrators. The CCT system continues to run, although in the target range. Systems are hardened, systems necessary for patch management and monitoring by the management system are live. In general, cryptographic processes are used for data transfer.
DETECT	Process: monitoring of the planned status takes place on the traffic controller's workstation and in the KSC. Faults are associated with group alarms. Additional, possibly more finely-granulated group alarms may need to be created for this purpose. Procedure in accordance with guideline 892. Technology: self-testing to monitor system integrity and mechanisms to safeguard the integrity and authenticity of messages are implemented in accordance with standards. Shutdown of parts of the system is displayed directly. Certain error messages may also be recorded. Display may take place without direct system shutdown, but with withdrawal of certificates at the KSC and thus isolation of the systems in question.	Process: monitoring takes place in the management system in accordance with CCT system self-testing in combination with the desired status and other stipulations (patch level, configuration and process monitoring). Obscure incidents are notified, although the system is in the desired state, and are sent to a situation centre for evaluation. The situation centre and the rail safety manager decide whether to continue operation and for how long. Connection relationships, attempted log ins, anomalies in data traffic, unusual ports, event logs and system parameters are also monitored. Technology: data from monitoring agents and IDS come together in the management system and are analysed and correlated. In the event of a deviation, the data are passed on to the situation centre and an alarm is generated. CCT systems must be capable of hosting monitoring agents or suitable measuring points must be stipulated for IDS. Provision must be made to obtain forensic data locally (tools for CCT administrators). Rapid restoration is possible using secure boot. Matching the frequency and process is necessary. The integrity of safety-critical messages is tested in accordance with the standard.

RESPOND	Process: operating processes run in the event of deviations from the planned status or shutdown (fault) of too many systems, as currently specified. Situation centres must be manned. Operation is continued in accordance with the process and spatial expansion. See above for more. Technology: log files and recordings of non-interfering diagnostic systems may be withdrawn and analysed. Clarification: who, period? Revocation of certificates in the KSC.	Process: isolation measures or shutdowns are implemented in the case of deviations from the desired status. Operating measures may take place following reconciliation (see above) or recovery measures be introduced if irregularities are observed in the desired status for a longer period. Technology: withdrawal of data from the management system and IDSs. Data collection log. Forensic measures on the anomalous system identified. Isolation of systems identified. Necessary network resegmentation, possible disconnection of unnecessary or dispensable connections in accordance with the contingency plan. Preparation of any necessary patch rollouts with rollout scheduling in accordance with the contingency plan (agreement with operational scheduling).
RECOVER	Process: restoration of the planned status, provided that: • The source of the error has been identified and understood • Counter-measures (and also any compensatory measures) have been introduced and rectification of any temporarily-acceptable weaknesses has been completed (following risk assessment) (risk priority number, e.g. in accordance with 0831-103). • Any necessary re-run of NTZ[4] phases (possibly abbreviated), CSM assessments or repeat availability consideration. • Reconciled observation phase Technology: intensification of diagnosis, log data analysis. Use of secure boot technology. Regeneration of certificates and possibly consideration of additional parameters. Possibly change of plan with regeneration of data and/or rapid adjustment with temporary correction. Change of relationships via KSC.	Process: redefinition of desired status or target configuration status. Any temporarily acceptable simple restoration. Patch and configuration scheduling, network resegmentation (following analysis). Analysis of changes in accordance with SLA and reflection in objectives. Loading changes via the management system following operationally-reconciled rollout scheduling. Causes must be understood, effectiveness of the measures must be verified. Agreement of additional observation measures. Any administrative measures. Technology: centralised patch management. Reissue of certificates and/or signatures. Change management via centralised management systems. Use of secure boot and central policy standards. Network management.

[4] NTZ : New German approval process for CCT

V. Bibliography

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und Bundesamt für Sicherheit in der Informationstechnik (BSI). (2016, Dezember 1). Retrieved from http://www.kritis.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/Functions/glossar.html?lv2=4968608

CENELEC. (2010). EN 50159: Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission sytems.

Community & Regional Resilience Institute (CARRI). (2013). Definitions of community resilience: An analysis.

International Electrotechnical Comission. (n.d.). IEC 62443 Industrial communication networks – Network and system security.

National Institute of Standards and Technology (NIST). (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication, 800*, p. 53.

Petit, F., Phillips, J., Verner, D., & Whiteld, R. (2012). Resilience: theory and applications. *Decision and Information Sciences Division, Argonne National Laboratory.* Retrieved from http://www.dis.anl.gov/pubs/72218.pdf

Contact

Björn Zimmer, DB Netz AG, Mainzer Landstraße 201, 60326 Frankfurt a.M.
Tel.: +49 (0) 69 265 304 16 | E-mail: Bjoern.Zimmer@deutschebahn.com

Further information

The “Cybersecurity for safety-critical infrastructures – CYSIS” workgroup was established by Deutsche Bahn AG and Technische Universität (TU) Darmstadt within the framework of the Innovation Alliance and the existing DB RailLab on 25 January 2016. The purpose of the workgroup is to make effective challenges to the cybersecurity of safety-critical infrastructure intensified by digitisation in the railway industry possible.

The Cybersecurity workgroup forms a basis for an intensive exchange of information between industry and academia in the railway sector, in order to benefit from each other's knowledge. Effective defence mechanisms and countermeasures can be researched and developed further with the assistance of partners from academia, including CYSEC, the Department of Cybersecurity at TU Darmstadt. The desired outcome is the networking of the railway industry with academic research on cybersecurity.

Website

http://www.cysis.eu