UITP
ADVANCING PUBLIC TRANSPORT

REPORT

PRACTICAL GUIDANCE ON CYBERSECURITY

REQUIREMENTS IN TENDERING

JANUARY | 2023

Thank you to our sponsors!

International Association of Public Transport (UITP)
Rue Sainte-Marie, 6 | B-1080 Brussels | Belgium

Tel: +32 2 673 61 00
info@uitp.org
www.uitp.org

TABLE OF CONTENT

INTRODUCTION

Cybersecurity protection in public transport and railways is a new but growing concern. Nowadays, almost any product incorporates firmware or software and - because computing tools usage has become universal, from the maintenance staff to the railway President - it is one of the few cross-functional subject matters that public transport operators (PTOs) must face. Unfortunately, few employees have the relevant proficiency to deal with such complicated issues, particularly when it comes to cybersecurity for automation of physical operations, such as rail system communications, signalling and processing. Hence, the dilemma facing PTOs: should IT/OT specialists be spearheading all functional processes (for example, marketing or procurement) that involve automation product definition or not? Role definition, particularly in this area, is a complex matter and is one that we will tackle later, describing the specific contributions that IT, OT and other cybersecurity specialists can bring to the protection of railways. That said, we strongly suggest that whenever necessary, IT/OT specialists should support their functional colleagues in creating appropriate processes and intervening on the very technical topics. It also means over and above the usual training that all employees should have, these functional managers should rely on guidelines to help them address the cybersecurity issues in their process.

MISALIGNMENT BETWEEN PTOS AND VENDORS

It is no wonder, even today, why cybersecurity can be seen as a remote and complex challenge, one which may frighten procurement managers who know little of the subject. At the discharge of procurement managers, the fact that IT specialists are rarely allocated to support them, and worse still, few IT specialists have experience or expertise in applying cybersecurity principles to the systems used in physical automation, may explain their fear. The emergence of OT specialists who are also cyber experts, who know the operational environment of railways, shall in the future bring additional support for buyers. Nevertheless, very few operators currently have such support or can easily access consultable guidelines for these functional processes. It goes a long way to explaining why so often there is a profound misalignment between the PTOs' cybersecurity expectations and the vendors' cybersecurity deliverables.

© Stnazkul_fotolia

In fact, the rule in many public transport and Railway environments is still that vendors do not supply PTOs with secure solutions. At the same time, many vendors complain that the PTO's requirements are so vague that any cybersecurity is good enough, even a cheap firewall solution that offers no real valuable protection. It's only wishful thinking to believe that procurement and vendors can be aligned without establishing a procurement path that includes clear security deliverables, supported by the right level of cyber expertise and funded by an adequate cybersecurity budget. Furthermore, security requirements should be included in all procurement contracts, irrespective of the System under Consideration (SuC), to ensure that both parties have clearly defined responsibilities, supported by contractual arrangements. This remains true even when the cybersecurity solution applied to the SuC is part of another procurement process.

CYBERSECURITY PROACTIVE INITIATIVES

These contractual arrangements should apply throughout the SuC's lifecycle and be based on standardised security clauses, relevant standard specifications and selected risk reduction measures. The Procurement department should be proactive, and prepare the ground with the entire supply chain prior through effective dialogue about their security needs. By adopting the secure development processes described in IEC 62443 and TS 50701, including security functions in systems and products and - where appropriate - teaming up with existing security product vendors to identify and clarify risks, procurement will ensure that cybersecurity threats are well understood by all stakeholders and taken seriously by the vendor's proposal.

CLEAR CYBERSECURITY CONTRACTUAL REQUIREMENTS

This white paper addresses the main requirements that railway and public transport operators should consider in their RFP (Request for Proposal) to help vendors understand their current and future security posture, and how it will affect the procurement process for their SuCs. Although not all procurement process (for example, buying a simple user interface) requires following the entire cybersecurity assessment, a PTO acquiring a complex SuC, particularly when interfacing with other subsystems, should provide the vendors with an initial risk assessment and a requirement to comply with the appropriate standards. This will ensure that the supply chain takes into consideration dedicated cybersecurity measures adapted to its product or system type, including not only the technology but also those relating to data handling.

The security requirements provided during procurement should be used to rank the vendor's solution and be part of the tender evaluation process. This ensures that vendors compete not only on the SuC's functionality requirements but also on the security aspects. By clearly specifying security design requirements, the procurement avoids unfairly treating a vendor who priced the adequate cyber-protection solution. Ensuring a level playing field is in the interest of the PTO, who will avoid costly design modifications that always involve litigation measures. The concept of trusted vendors can also be used to build security into the procurement process by creating a list of trusted suppliers that, for example, have:

- *gone through a cybersecurity certification process.*
- *include test and development tools, facilities and processes.*
- *follow a secure development life cycle.*
- *ensure security integrity through delivery, installation and commissioning phases.*

Without being overly prescriptive, the contract should clearly state which cybersecurity requirements are mandatory and which are optional. This document will give the Procurement Managers guidance on what should be the minimum mandatory requirements.

OBJECTIVES AND SCOPE

This document establishes the minimum requirements for protection against cybersecurity attacks on a PTO's network. Often regrouped under the terminology 'Enterprise Security Systems' (ESSs) these solutions should be implemented with the objective of preventing unacceptable physical, business and other consequences of cyberattacks for the PTO.

IT/OT DIVIDE

When it comes to cybersecurity, it is important to acknowledge the differences between Information Technology (IT) and Operational Technology (OT) environments. IT software systems are those for which the worst-case consequences of cyber compromise are business consequences, such as lost revenues, brief service interruptions, privacy breaches and lawsuits. Common examples of IT systems are websites, databases, payroll systems and other 'office' computers.

OT systems are those for which the worst-case impact of compromise are physical consequences, such as sustained service outages, material damage to rolling stock and other equipment, environmental disasters, public safety threats as well as worker or public casualties. Common examples of OT systems are networks supporting automation for physical access controls, rolling stock, electrical power distribution and signalling systems. It is always the case that cybersecurity priorities, programmes and management systems differ materially between the two domains.

In this document, we often refer to IT networks and some automated functionalities, as 'business critical' and OT networks as 'safety critical', 'reliability critical' or sometimes more generally 'control critical' automation.

Cybersecurity is important for both types of automated processes. In many cases, somewhat similar risk assessments and risk mitigation measures can be applied. However, material differences between the two domains exist:

A concrete example of the differences between security programmes in these two domains is the treatment of information. IT security programmes generally seek to protect information, in particular Personally Identifiable Information (PII). OT security programmes observe that all cyber-sabotage attacks ***are*** information. Thus, the top priority for most OT security programmes is not to protect the information, but rather to ***protect*** physical operations ***from*** information. More specifically, to protect them from cyber-sabotage attacks that may be encoded in information that enters OT networks ***from*** external sources.

Thankfully, very few examples of derailments originating from cyberattacks can be found, with none having led to any fatalities. However, many examples of OT cyberattacks on grid infrastructure exist to remind us that equipment can be put out of order and cause genuine operational headaches for weeks.

CLASSIFYING IT VS. OT SYSTEMS

One factor in the classification is the ability of cyberattackers to use compromised systems to attack other computers. A common attack pattern, for example, is the Remote Access Trojan (RAT). A RAT is a malware component that connects or 'beacons' directly or indirectly out to an internet-based malware Command and Control Centre (C2). Once a RAT is established on a computer, the attacker logs into the C2 and operates the RAT by remote control via the C2. The attacker uses the RAT to attack other targets reachable from the hosting computer. RATs are then planted in turn on the newly compromised computers. In this way, attackers are said to 'pivot' their attack from one computer to another. The lesson here is that, because of the possibility of pivoting attacks, all computers able to exchange information bidirectionally through TCP (Transmission Control Protocol) or equivalent connections should be considered to be at the same level of security. An attacker who takes control of any one of these computers has a real chance of taking control of them all.

Figure 1: IT vs. OT focus

	IT	OT
Worst-case consequences:	Business consequences	Physical consequences
Security Priorities:	Privacy, confidentiality, integrity and availability of information.	Safe and reliable physical operations.
Rate of Change:	Prompt security updates, AV updates and other changes to stay ahead of pervasive threats.	Strictly controlled changes, particularly for the most safety-critical and reliability-critical components.
Cybersecurity history	Concern dealt with for many years	Generally, a recent concern.
Network connectivity	High	Low (but increasing)

This is one of the many reasons that business-critical IT computers should be deployed on separate networks from control-critical OT computers. If we deploy a safety-critical computer, for example, on an internet-exposed IT network, then we risk a cyberattack pivoting from any compromised IT assets into the safety computer. It is vital to our security programme, therefore, that we classify computer systems correctly and host them on networks of similar criticality. For example, let's consider a network of video cameras:

- Monitoring sections of track in tunnels that are accessible to the public to some degree, but whose geometry are such that in-person supervision of the tunnels is not safe. Rail system operators use the cameras to verify that the tunnels are clear before authorising trains to proceed. The cameras are safety-critical OT assets.
- Installed on commercial displays in stations that use the images in order to profile passengers walking in the area. Those cameras are privacy sensitive, because they collect personal data. The unavailability of those cameras has no impact on operation, then they should be deployed on an IT network.
- Monitoring tracks in stations where an engineering study has determined that the worst-case consequences of compromise of these cameras is the destruction of the cameras, for example by overwriting their firmware and rendering the devices unbootable. In this event, human supervisors with radios can be dispatched to affected stations to visually verify that members of the public are not present on tracks and thus can authorise trains to proceed. Here, the worst-case impact of compromise is either business- or operation-related. Some PTOs will simply allocate people to monitor the tracks until the cameras can be replaced, while others will choose to remove those people from their usual job, and decide that other services are impacted. These cameras may be deployed on general purpose OT or IT networks and managed as IT or OT assets, depending on the risk assessment of the PTO.

In short, it is important to classify OT and IT assets correctly, but system designers should be aware that there are times when simple engineering changes or manual fallback procedures can change the outcomes of worst-case compromises and so reclassify OT assets as IT assets (or vice versa). Classifying it as IT asset is generally a desirable outcome security-wise, because they demand far less thorough protection than safety-critical or reliability-critical OT assets.

SCOPE

Two mandatory principles should be applied whenever designing the RFP document. The first is linked to this difference in logic between IT and OT, which should be extended to safety-critical and third-party networks. Hence, any procurement of an SuC should consider - as a minimum - cybersecurity measures that physically and logically create segmented networks, including:

- Safety-critical systems with a high level of safety such as SIL 2 to SIL 4, for example, signalling communication network, onboard networks.
- Reliability-critical OT systems, for example, operational communication network - fixed and wireless, smoke and fire detection network, SCADA network for traction substations and stations.
- IT systems, for example, Administrative Communication Network / ERP, traffic control, payment systems.
- Others / third-party systems, for example, traffic light management for non-segregated lanes, CCTV police station.

As we mentioned, for certain systems it is ambiguous as to whether those systems should be considered reliability-critical or business-critical. For example, ticketing systems crippled by a cyberattack could result in service outages, which are a physical consequence. On the other hand, ticketing systems generally need to interact strongly with payment systems and even with websites, all of which are very much IT systems. The treatment of these ambiguous systems depends on the design of the PTO's automation and security systems as well as on the organisation's tolerance for risk.

For example, a risk assessment for a ticketing system and its cyber defences may conclude that a worst-case service outage of three days every two years is a reasonable expectation. The PTO may compare this risk to other risks the organisation accepts, such as multiday outages due to inclement weather events on average every couple of years. This organisation may, therefore, conclude that the cyber risk to the ticketing system constitutes an acceptable business risk, and may proceed to model the ticketing system as an IT asset.

A word of caution: the largest and most societally important PTOs may wish to review their risk assessments with government authorities. The risks that PTOs decide to accept should agree in the main with societal expectations for safe and reliable operations. If there is a material mismatch of expectations, and there is ever a serious cyber incident, then the PTOs should not be surprised when government authorities react by imposing strict new cybersecurity regulations.

The second principle to be considered when designing RFPs is the 'Defence-in-Depth' (DID) concept. Multiple layers of security controls (defence) must be placed throughout the PTO's network. The intent of this concept is to provide redundancy in the event that a security control fails or a vulnerability is exploited. Cybersecurity programmes should be able to absorb at least a single point of compromise without exposing the organisation to unacceptable business or physical risks. This principle shall apply to all layers of the OSI stack, considering the following element: data, application, host, network, perimeter. This principle must be integrated into the RFP, bearing in mind that it must apply to personnel, procedural, technical and physical security for the entire duration of the SuC's life cycle.

Finally, this document is focused primarily on OT cybersecurity requirements, such as those explained in IEC 62443 and TS50701. Information protection requirements for the procurement of IT systems are already well understood by IT practitioners. Teams responsible for buying IT systems or components in a mixed IT and OT procurement process are encouraged to consult and take guidance from their IT teams.

The focus of this document is primarily the procurement of OT systems. Procurement teams must be aware that IT security practices cannot be applied directly to OT purchases and must realise that OT security and procurement practices are much less mature than IT security and procurement practices. Hence the guidance in this document.

GENERAL REQUIREMENTS AND SECURITY GUIDELINES

On top of applying these two main principles, the RFP should consider a minimum set of general requirements. As an introductory guideline, the following are recommendations that will be addressed later in more detail.

1 • The RFP shall always be supported by the laws of the country that apply for the procured SuC. Three different types of legal constraints apply to any tendering process:

a. The national tender regulations. We will give an overview based on EU regulation.

b. The national cybersecurity authority (for example, ANNSI in France and CISA in the USA), which may intervene in the deployment of the SuC.

c. Any specific national regulations applying to cybersecurity. We will develop this section using mainly IEC 62443 and TS 50701.

2 • The RFP shall always be technically supported by the relevant standards. Many different types of standards may be applied in a tendering process, but these can be regrouped under the following:

a. Specific standards applied to the SuC

b. General public transport standards

c. General operating standards

d. Specific cybersecurity standards.

3 • Work should be performed by qualified personnel.

a. For cybersecurity concerns, some of the work may have to be performed by authorised and approved personnel (by the client/government authority).

4 • The PT operations should drive the ISS solutions, not the opposite.

5 • The vendor's proposed solution should be scalable.

6 • The PTO should provide an existing risk and vulnerability assessment for the SuC, or establish a preliminary version.

a. The SuC/solution supplier should consider this assessment and adapt it to its technology.

7 • The vendor's solution should be integrated within a detailed ISS that offers the possibility to track, record and monitor interactions within all of the IT/OT infrastructure:

a. We will discuss this point according to the standards TS 50701/IEC 62443.

8 • The Vendor's solution should consider cryptographic data exchange mechanisms and technologies where required:

a. For example, encryption, key management, access control, authentication and data integrity

9 • To address GDPR obligations, the SuC should incorporate a strong data leak prevention policy with the appropriate technologies.

10 • The vendor should provide a security operational plan, an information security policy and procedures adapted for the proposed SuC.

For those who wish a quick overview of the necessary topics to consider in a RFP, they can consult the 'Quick Reference Guide For Cybersecurity Procurement' on page 49, which may prove useful.

TARGET AUDIENCE

This document provides guidelines that should help PTO procurement personnel without a cybersecurity background to understand the challenges linked to cybersecurity. It will provide the minimum cybersecurity requirements to be considered for most subsystems that include firmware and software, which nowadays is more the norm than the exception. For additional information on some topics, we will make a reference to the suite of White Papers that the UITP cybersecurity committee has already published and that may be consulted by buyers.

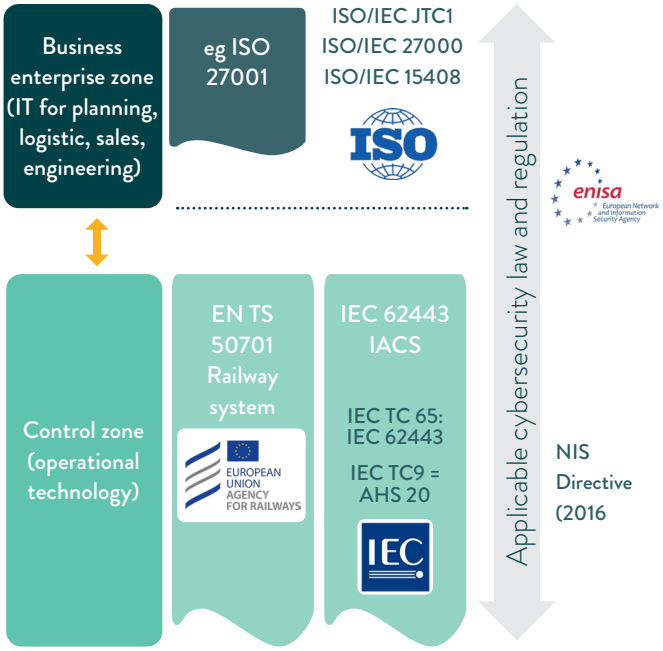
METHODOLOGY

This White Paper is based on the experience of PTO and cybersecurity experts from the industry. The topics were developed taking into consideration surveys and interviews performed with PTO members of the UITP association.

REGULATION AND LEGAL FRAMEWORK

All procurement processes are integrated within a legal and technical background specific to the SuC and to the country in which this SuC will be procured. The following diagram gives an overview of the different regulations, standards and government entities that should be taken into account for cybersecurity.

Figure 2 regulatory context – from TS 50701



We will describe this environment using the European legal framework for cybersecurity and procurement process. PTOs outside of the EU should consider national regulations.

PROCUREMENT REGULATION

Since most public transport and railway operators offer services essential to the population, their procurement process is usually governed by specific regulation. Hence, in most cases, contractual private law does not apply, while national public procurement laws must be considered. The procurement laws in Europe are the result of a succession of negotiations between the EU Member States, which evolved over time and were passed into different Directives. These Directives were then transposed into national laws.

One of the main European Directives for procurement impacting the transportation sector was established in 2004. This created a separation between utilities and the rest of the public sector. While the procurement of the former remained governed by a new Utilities Directive, Directive 2004/17 coordinated the procurement procedures of entities operating in the water, energy, transport and postal services sectors. The three original Directives were amalgamated into a single Public Sector Directive - Directive 2004/18 – the objective of which was to coordinate the procedures for the award of public works contracts, public supply contracts and public service contracts. At time of writing, Directive 2004/18 still governs procurement by public authorities other than that for utilities. The Directives, apart from simplifying and clarifying the existing law, introduced a new procurement procedure, the competitive dialogue and allowed the procurement of framework agreements.

The last Directives on public procurement, utilities procurement and concessions were adopted by the European Council on 24 February 2014. Member States were allowed until 18 April 2016 to transpose this fifth generation of Directives into their national laws. The 2014 Public Procurement Directive introduced an obligation to take into account accessibility criteria for disabled persons in the specification for any works, goods or services intended for use by the general public.

Directive 2009/81/EC: In Europe, Directive 2009/81/EC of 2009 coordinates and applies a procedure for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security. It was amended by Directives 2004/17/EC and 2004/18/EC and may have consequences for cybersecurity contracts.

SPECIAL FORM OF PROCUREMENT

Public contracting authorities have the possibility of entering different forms of procurement, which are often used in railway procurement processes.

- **Framework agreements:** PTOs may enter into framework agreements with one or more businesses. These prescribe the terms and conditions that would apply to any subsequent contract and make provision for selection and appointment of a contractor by reference directly to the agreed terms and conditions or by holding a competition, inviting only the partners to the framework agreement to submit specific commercial proposals.
- **Dynamic purchasing systems:** PTOs may adopt such processes operated as a completely electronic procedure for the purchase of commonly used items, generally available on the market. Such dynamic systems are applicable across a range of goods, works and services, divided into appropriate and objectively defined categories.
- **Competitive procedure with negotiation:** Such a procedure is possible whenever the contracting authority cannot find a readily available solution on the market and - provided it gives a description of its needs - the characteristics of the goods, works or services to be procured and the award criteria. Companies are invited, through a prior indicative notice, to express an interest in being invited to tender, and selected companies are then invited to submit their offer. Negotiations may take place between the contracting authority and each business to improve the content of each tender before invitations are issued to submit a final tender. Final tenders are then evaluated against the previously published award criteria and a contract awarded.
- **Negotiated procedure without publication:** This allows contracts to be awarded without publication of an OJEU contract notice "in the most urgent cases", but the circumstances allowing for the use of this process are restricted.
- **Public-Private Partnerships:** They are not subject to special rules in EU procurement law, but must follow the rules and principles resulting from the European Treaties, including those embodied in secondary legislation.
- **Other forms of procurement process also exist.**

ARE CYBER SECURITY PROCUREMENTS DIFFERENT?

Given recent procurement reforms in the EU, including the 2009 reform on defence procurement, a white paper[1] described the public cyber security procurement in Europe. More specifically, it examined two specific questions:

1. Whether cybersecurity procurement differs from public procurement in general.
2. Whether there were any noteworthy signs of Europeanisation in terms of cybersecurity procurement.

According to the empirical results of the study, cybersecurity procurement seemed to differ from the general public procurement. In particular, competition obstacles were highlighted in terms of bids for cybersecurity procurement tenders in all industries. Furthermore, it seems there was a visible lack of Europeanisation, although the same observation could apply generally to EU public procurement.

NIS AND INTERNATIONAL REGULATION

The Network and Information Security Directive (NISD) 2016/1148/EU came into force in May 2018, with the goal of improving the level of cybersecurity among EU Member States.

It ensures:

- Member States must have a CSIRT (Computer Security Incident Response Team) and a national NIS authority.
- Cooperation between Members States, sharing information about risks and incidents.
- Security across sectors vital for economy and society and relying heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.
- Member States should identify business as operators of essential services and should ensure that they take appropriate measures to prevent and minimise the impact of incidents.
- Operators of essential services should take appropriate and proportionate technical and organisational measures to manage cybersecurity risks affecting operations.
- Operators of essential services should notify the authority of any incident having significant impact on the continuity of the service.

PTOs are identified in some case as operators of essential services. Therefore, these organisations will have to take into account the Directive and the respective national law. PTOs that aren't, are recommended to do so and should still consider applying the NIS recommendations. PTOs in non-EU countries should check if their operations are considered as a critical infrastructure and to verify whether general directives also apply.

1 An Acid Test for Europeanisation: Public Cyber Security Procurement in the European Union,

GENERAL DATA PROTECTION REGULATION

The **General Data Protection Regulation (GDPR)** is a European Regulation on privacy and data protection. It also addresses the transfer of personal data outside the EU. Its primary aim is to enhance individuals' control and rights over their PII and to simplify the regulatory environment for international business and supersedes the 95/46/EC, Data Protection Directive. It applies to any company - regardless of its location and the data subjects' citizenship or residence - that processes the personal information of individuals inside the EU. It was adopted in 2016 and became enforceable in 2018. Since the GDPR is a Regulation and not a Directive, it is binding and applicable and does not provide any flexibility to individual Member States.

GDPR Main principles

A data subject must provide their informed consent to data processing before the company can process the personal data. The GDPR provides rights, which can be summarised as: transparency and modalities; information and access; rectification and erasure; right to object and automated decisions. No personal data may be processed unless this is done under one of the six lawful bases specified by the Regulation (consent, contract, public task, vital interest, legitimate interest, or legal requirement). When the processing is based on consent, the data subject has the right to revoke it at any time.

To be able to demonstrate compliance with the GDPR, the data controller must implement measures that meet these principles of data protection by design and by default. It enforces pseudonymisation, which is a required process for stored data; this transforms personal data in such a way that the resulting data cannot be attributed to a specific individual without the use of additional information. Additionally, records of processing activities must be maintained by companies according to a list of established criteria.

Maintaining the security of the data is a legal obligation of the data controller. Any breach of data confidentiality is an offence punishable by fines of up to 2-4% of sales turnover, depending on the offence. Thus all PTOs should ensure full conformity with the GDPR.

Note that GDPR considerations apply much more routinely to the purchase of IT systems than to those of OT systems. However, close to the IT/OT boundary, GDPR considerations may also be found to apply to a small subset of OT systems.

NATIONAL CYBERSECURITY AGENCIES

As we initially mentioned, as well as for regulation, PTOs in most countries can call upon cybersecurity agencies for assistance. These agencies play a consulting role and can support the railway procurement process. In some countries, the agencies can be active, reviewing the railway cybersecurity architecture, checking the cybersecurity operational plan and the procedures applied to the SuC. In some cases, we have even seen these agencies conducting pre-screening and authorising employees to execute an important cybersecurity role. Procurement personnel should check whether or not this clearance mission will be required and integrate this constraint within the RFQ documents.

ENISA, the European Network and Information Security Agency, is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these stakeholders to develop advice and recommendations on good practice in information security. Its mission is to achieve a high common level of cybersecurity across the EU in cooperation with the wider community.

ENISA aims to deliver proactive advice and support to all relevant EU-level actors. It brings in the cybersecurity area policies targeted at the product development lifecycle, through viable and targeted technical guidelines. It seeks to put cybersecurity risk management frameworks in place across all sectors that are followed throughout the cybersecurity policy lifecycle.

CISA, the Cybersecurity and Infrastructure Security Agency, is the US equivalent of ENISA. It is a standalone US federal agency, with oversight from the Department of Homeland Security. Its activities are a continuation of the National Protection and Programs Directorate.

In Europe, there are several national entities that play an active role in cybersecurity protection of critical infrastructure. For example, the French National Cybersecurity Agency (ANSSI) (www.ssi.gouv.fr) is committed to ensuring that French public administrations, public services and businesses can take full advantage of secure and trustworthy digitalisation. Its role is to foster a coordinated, ambitious, proactive response to cybersecurity issues in that country, to drive awareness raising and to spread the French vision and expertise and European values abroad. Its German equivalent is the BSI, the Federal Cyber Security Authority, (www.bsi.bund.de), which also aims to shape information security in digitalisation through prevention, detection and response for government, businesses and society.

Here is the list of other European countries at time writing:

- Austria: (www.digitales.oesterreich.gv.at)
- Denmark: FCS – Centre for Cyber Security (www.cfcs.dk)
- Spain: OCSTI (www.ccn.cni.es)
- Estonia: RIA – Riigi Infosüsteemi Amet (www.ria.ee/en/)
- Finland: FICORA (www.ficora.fi)
- Italy: OCSI (www.ocsi.isticom.it)
- Luxembourg, (www.anssi.lu)
- Norway: SERTIT (www.sertit.no)
- Netherlands: NLNCSA (www.tuv-nederland.nl)
- Poland: NASK (www.nask.pl)
- Sweden: FMV/CSEC (www.csec.se).

In the UK, the organisation is the NCSC, the National Cyber Security Centre (www.ncsc.gov.uk).

INFORMATION SYSTEM APPROVAL PROCESS

Some of these agencies (for example ANSSI) recommend going through the information system approval process, which is a prerequisite for building confidence in business or physical automation systems and their operation. The objective of this process is to find a balance between acceptable risks and security costs, then to have this balance formally arbitrated by a manager with the relevant authority. Security certification allows a manager - based on the advice of experts - to obtain information and certify to the users of an automation system that the risks that weigh on them, on the information that they handle and on the services rendered, are understood and mastered. An approval authority emits the approval certificate of the automation system before it is put into operational service. Approval makes it possible to identify, achieve and then maintain an acceptable level of security risk for the information system in question.

Those responsible for procurement should check if their SuC should seek approval from one of these agencies.

STANDARDS AND TECHNICAL FRAMEWORK

Public Transport and Railway Operators are standards driven, and rightly so. Indeed, standards offer the benefits of integrating the knowledge of subject experts who are usually part of a dedicated committee, and applying it universally to a topic. For a procurement manager, who cannot be expected to be a technical expert on all issues, requiring that a vendor meets the specific requirements of a standard ensures that important aspects of those issues have been accounted for.

It should be kept in mind that, although standards fulfil an important function, they have their limitations. Software and cyber threats are constantly evolving, making it difficult to solve cybersecurity through standards alone. The goal should not be total compliance with standards, it should be correct levels of cybersecurity for all SuCs. For critical systems, this can be addressed through best-value procurement, where compliance to relevant standards is used as a base requirement for participation, with project specific cybersecurity requirements as value selection criteria.

Railway procurement personnel can easily be overwhelmed by the sheer number of standards to be considered. Ideally, only the relevant standards should be specified. This is why it is recommended that a technical expert from within the PTO, or a consultant supporting the procurement team, goes over the list to check that no important standard is missing. Obviously, most SuCs have their own standard. Furthermore, Railway and Public Transport Operators have very specific operating environments, which require applying generic requirements that are usually treated by standards. EMC (Electromagnetic Compatibility) is a good example of an issue that affects most electronic products, which is treated in the standard IEC 61.000. EN 5012X are similar standards that apply across multiple SuCs. These are extremely important in railways, because they apply to safety, one of the main industry differentiators. In fact, they are so important that the railway industry has decided to write a dedicated Technical Specification - TS 50701 - to show how to apply the ICS cybersecurity standard IEC 62443 in the specific railway environment.

RISK ASSESSMENTS

Risk assessments and risk requirements drive the selection of minimal cybersecurity provisions, whether those requirements be specified in an RFP or in a standards document. Whether carrying out in-house assessments, or specifying requirements for outsourced assessments, particularly in OT domains, there are a number of factors that must be considered by assessment teams.

Cyber risk has two components. The risk of inadvertent cyber errors and omissions can be modelled statistically. In this domain, ***risk = consequence x likelihood.*** People and teams, particularly in large numbers, make mistakes at rates that can be predicted by factors such as previous error statistics, the introduction of new and unfamiliar technologies, the addition of new personnel to existing teams and so on. However, the risk of deliberate cyber-attacks cannot be modelled this way. Such attacks are more akin to deliberate physical and terrorist attacks, modelled as:

Risk =
f(consequence, intent, capability, opportunity)

Where:

- **'Consequence'** is each risk outcome that we seek to avoid, generally measured quantitatively as a monetary figure or qualitatively as a small integer corresponding to outcomes ranging from 'low impact' to 'completely unacceptable'.
- **'Intent'** is a number between zero and 1 that indicates the likelihood of each threat actor attempting to bring about the consequence.
- **'Capability'** is an assessment of the tools, techniques, personnel and other resources available to each threat actor.
- **'Opportunity'** is an assessment of all residual attack paths in a defensive posture that may lead to the consequence.

Some notes on the above: First, as a rule, just as nothing can ever be completely safe, nothing can be completely secure. This means that there is always some residual opportunity for attacks to create undesirable consequences. The goal of cybersecurity programmes and of risk assessment is not to eliminate all attack opportunities, but rather to understand those risks that are acceptable and thus how to specify how secure an SuC must be to achieve that level of risk tolerance.

Second, it is generally unwise to rely on intent in risk assessments. Ransomware groups are quickly adopting nation-state attack tools and techniques, and these groups target anyone with money. More generally, threat actors' intent can change much more quickly than their capabilities or attack opportunities. Most PTO's model intent as a 1 on a scale of 0-1, with rare exceptions. For example, for specific nation-state threat actors, a PTO's national intelligence agency may be able to provide regular and reasonably accurate briefings on that threat actor's intent and targeting decisions.

Given the financial rewards of ransomware or the geopolitical gains generated by attacks, it is fair to assume that sooner or later, the consequences of an anticipated risk are likely to impact the SuC. This risk usually materialises when the threat actor's capabilities exceed the level of expertise and/or resources required to exploit identified vulnerabilities. Thus, the key to specifying security capabilities for procurement is to require that residual attack opportunities for delivered systems the SuC demand capabilities that are greater than or equal to those attributed to the threat actors of concern. In addition, when undertaking such risk assessments, it is not enough to evaluate current capabilities; SuCs must generally work securely and correctly until the next major change window, often occurring every three to five years. To be effective, risk assessments must therefore project the attack capabilities that will be throughout the entire time between the deployment of the system and the next change window's opportunity to upgrade the SuC's security.

© Kwan Fung

Here are some simple examples of risk tolerance statements:

1. IT domain: No IT system compromise should be able to cause any physical consequence more serious than a service outage. All IT systems able to cause or contribute to service outages should be recoverable from backups and/or transaction logs within two calendar days of the outage.
2. OT domain: All opportunities for material equipment damage, public safety threats and public or worker casualties should ideally be mitigated by analogue, unhackable protections[2] such as analogue signalling and track circuits.
3. OT domain: When analogue protection such as (2) above proves impractical, safety-critical and reliability-critical networks should be connected to less-critical networks only through hardware-enforced unidirectional gateway[3] technology, thus preventing the remote exploitation of residual cyber risks. In addition, the proposed solution should include safeguards against offline attack information movement that are strong enough to ensure that the only residual risk to critical systems is deliberately cooperating, compromised insiders at the PTO or its service providers[4].

EN 50126, EN 50128 AND EN 50129

In Public Transport, managing the safety risks is a critical issue for both manufacturers and operators. Specific rail hardware and software systems are complex and interconnected, rail components are sourced from multiple suppliers and rail development lifecycles are becoming shorter with increasing international competitive pressure. This is why the tendering process, particularly when applied to an SuC for an OT system, should consider railway standards EN 50126, EN 50128 and EN 50129. These have been developed by CENELEC (European Committee for Electro-technical Standardisation), and apply to heavy rail systems, light rail and urban mass transportation.

More specifically, each of these technical railway standards cover the following functional safety requirements:

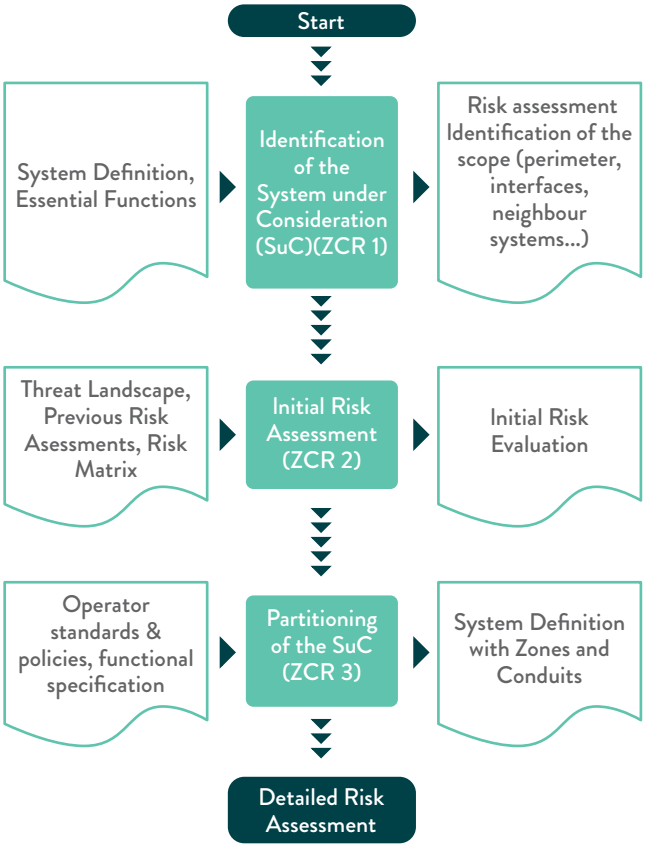
- EN 50126 (IEC 62278) – reliability, availability, maintainability and safety (RAMS)
- EN 50128 (IEC 62279) – software
- EN 50129 (IEC 62425) – system safety

EN 50126: This is used to specify and demonstrate RAMS. It describes the life cycle process for safety-relevant railway systems, through a systematic process for specifying requirements for RAMS and demonstrating that these have been achieved.

EN 50128: This defines additional conditions for the software included in programmable electronics whenever they are integrated in safety-related systems. It specifies procedures and technical requirements for developing programmable electronic systems used in railway control and protection applications of any safety implications. The standard is intended for software development and the interaction between software and the system of which it is part.

EN 50129: This defines requirements for the acceptance and approval of safety-related electronic systems such as signalling, including hardware and software aspects. Both must be considered within their whole system life cycle. It deals with the evidence to be presented for the system's safety case acceptance. It specifies the life cycle activities to be completed before the acceptance stage and additional planned activities to be carried out afterwards.

Figure 3
From TS 50701 - Initial Risk assessment flowchart



2 See Security PHA Review, by Edward Marzal and Jim McGlone, ISA, 2020, ISBN 1643311174.
3 A unidirectional gateway is a combination of hardware and software. The hardware is physically able to send information only one way. The software makes copies of servers and emulates devices. NIST Glossary - https://csrc.nist.gov/glossary/term/unidirectional_gateway
4 See Secure Operations Technology, by Andrew Ginter, Abterra Technologies Inc., 2018, ISBN 978-0-9952984-2-2.

TS 50701

This technical specification is intended to provide requirements and guidance on cybersecurity for railway technologies, taking into consideration both safety and security. It proposes dividing the SuC into zones and conduits, in line with the IEC 62443, and defines how to differentiate between the security levels to be applied for each zone.

It introduces the concept of SecRAC (SECurity-Related Application Conditions), inherited from SRAC (Safety-Related Application Condition) described in EN50126.

Railway procurement personnel should use the TS 50701 as their main source of guidance to write the RFQ. Annexes 1 and 2, which offers examples on how to deploy the technical specification, is extremely useful and instructive.

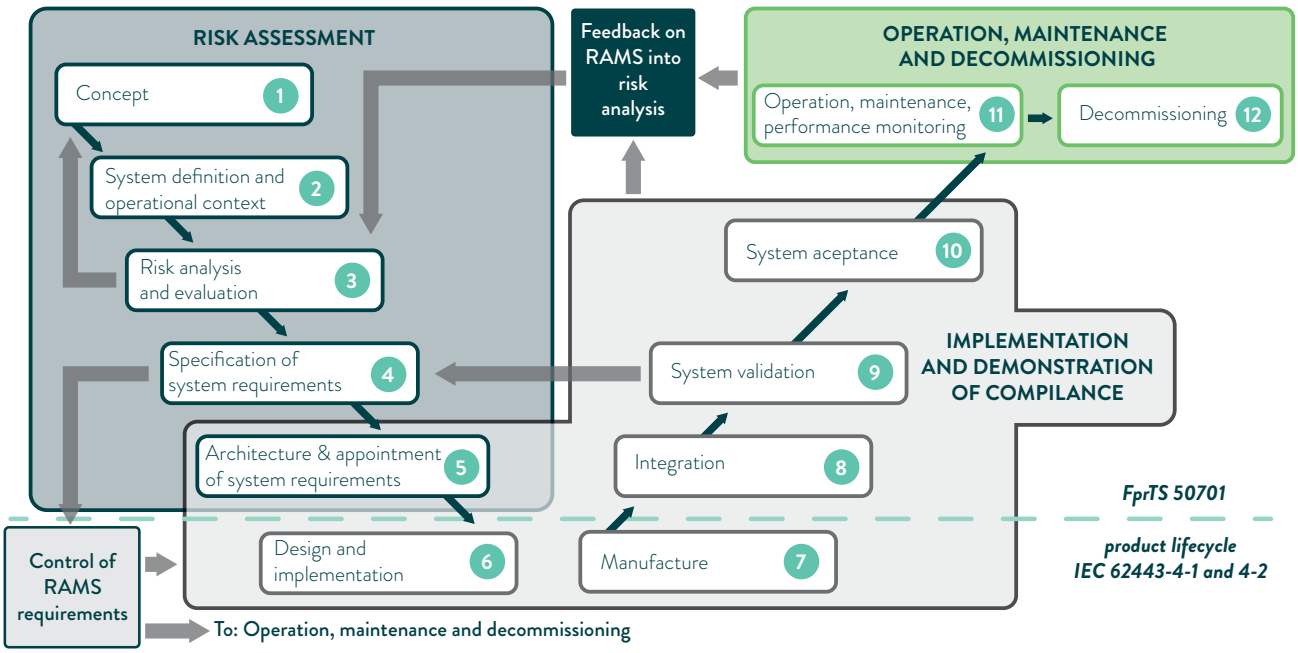
IEC 62443

The IEC 62443 is currently considered the worldwide standard for cybersecurity, particularly in the OT world, and is applicable to all Industrial Control Systems (ICS), including railway and PT Operations. Addressing four main topics - generalities, policies, system and component – it provides valuable insights for railways on how to evaluate potential threats and vulnerabilities and on how to help apply the necessary mitigation measures. Furthermore, this standard is consistent with the application of security management requirements based on ISO 27001 and ISO 27002. As already mentioned, the railway TS 50701 is based on IEC 62443, which supplements it by integrating specific railway concerns.

IEC 62443 is divided into different sections, and describes both technical and process-related aspects of industrial cybersecurity. It divides the industry into different roles: the operator, the service providers for integration and maintenance and the manufacturers. Each different role follows a risk-based approach to preventing and managing security risks within their activities. It is divided according to the following sections:

- Part 1-1: Terminology, concepts and models.
- Part 2-1: Aimed at operators of automation solutions, it defines requirements for considering security during the operation of plants.
- Part 2-3: Patch management in the IACS environment.
- Part 2-4: Defines requirements ('capabilities') for integrators. These requirements are divided into 12 twelve topics, which are described hereafter in IEC 62442-2-4.:
- Part 3-1: Security technologies for industrial automation and control systems.
- Part 3-2: Security risk assessment for system design.
- Part 3-3: System security requirements and security levels.
- Part 4-1: This defines how a secure product development process should look. It is divided into eight areas ('practices'), which are described hereafter in IEC 62441-4-1.
- Part 4-2: This defines the technical requirements for products or components 12 subject areas It also defines Common Component Security Constraints (CCSC).

Figure 4- V-cycle representation and the role of IEC 62443 in regard to TS 50701



PRODUCT CYBERSECURITY CERTIFICATION

There are four key components of the IEC 62443 standard used for certification. Two of these define processes and the other two define product and system requirements.

- Process specifications:
  - IEC 62443-4-1 defines a Secure Development Lifecycle (SDL) for developing and maintaining secure products.
  - IEC 62443-2-4 specifies requirements for entities that integrate individual offers into a system.
- Product and system requirements specifications:
  - IEC 62443-3-3 provides detailed technical requirements for a control system.
  - IEC 62443-4-2: Component certification.

IEC 62443-4-1: The certification process specifies the development process requirements for products. It includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, release, defect management, patch management and product end-of-life.

A key element of the certification is the use of secure development life cycle during the product's development. The focus must be on designing the underlying software to avoid creating a product riddled with vulnerabilities that can be easily compromised. The certification also proves that the vendor has the infrastructure in place to address a vulnerability, which should be a key consideration to railway asset owners. IEC 62443-4-1 uses maturity levels rather than security levels. Hence, a vendor's development process can be certified to one of four maturity levels: initial, managed, defined and quantitatively managed.

Buyers should assess the importance of the SuC within their railway network. If is a key element, then the procurement process should identify whether all vendors authorised to participate in the bid need be able to demonstrate a certain level of maturity in their development process, according to IEC 62443-4-1.

IEC 62443-4-2 specification provides detailed technical control requirements (CRs) for products. Component requirements are grouped into seven foundational requirements:

1. Identification and authentication control: control access to devices.
2. Use control: Mapping to roles and authorisation enforcement.
3. System integrity: Ensuring the integrity of data to protect against unauthorised changes.
4. Data confidentiality: Ensuring the confidentiality of data through encryption.
5. Restricted data flow: Restricting the flow of data to protect against publication of information to unauthorised sources. Using network segmentation.
6. Timely response to events: Responding to security violations by notifying the relevant authority, reporting forensic evidence and automatically taking timely corrective action.
7. Resource availability: Ensuring the availability of all network resources to protect against denial-of-service attacks.

Since IEC 62443-4-2 includes the concept of security assurance levels, a series of requirements designed to bring system security to one of four defined levels: SL-1 to SL-4.

Buyers should assess the importance of the SuC within their railway network. If this is a key element, then the procurement process should assess whether all vendors authorised to participate in the bid should be homologated and demonstrate a certain security level, to be defined according to the criticality of the SuC.

Figure 5: Example of authentication and identification control;
Adapted from IEC 642443-4-2 by Serge Van Themsche

Feature: Product should enable/support	SL-1	SL-2	SL-3	SL-4
Human user identification and authentication	x	x	x	x
Accounts management	x	x	x	x
Identifier management	x	x	x	x
Authenticator management	x	x	x	x
Password based authentication with defined password strength	x	x	x	x
Obscure authentication feedback during authentication	x	x	x	x
Look account after unsuccessful login attempts	x	x	x	x
Message warning when users log in	x	x	x	x
Users uniquely identified and authenticated		x	x	x
Software / device identified and authenticated		x	x	x
PKI infrastructure enables (when PKI is used)		x	x	x
Certificate validation (when PKI is used)		x	x	x
Symmetric key based authentication		x	x	x
Unique software / device identified and authenticated			x	x
Authentication protection by hardware mechanisms			x	x
Password reuse prevention configuration for Human users			x	x
Public Key protection via hardware			x	x
Symmetric key data protection via hardware			x	x
Systematic Multifactor authentication				x
Password reuse prevention configuration for Software/device				x
Others				

IEC 62443-3-3: This is a set of requirements for designing systems rather than components / products, and provides detailed technical control system requirements. It uses the same foundational requirement categories and the same security level concept as part 4-2, but specifies the requirements from a system perspective rather than from individual product, as it is the case in 4-2.

Buyers should assess the importance of the SuC within their railway network. They should then assign a Security Level (SL) to the SuC and demand that system integrators deliver a system that is compliant with 3-3 requirements and best practices for that SL. Buyers are cautioned that IEC 62443 is a cross-industry standard. For example, a minimally compliant SL-1 implementation might be appropriate for a rail station video surveillance system. Such an implementation is not appropriate for a signalling system. This is one of the goals of TS50701; to guide application of the 62443 standard to rails applications.

Nevertheless, we have recently seen metro operators specify that all wayside and onboard SuCs should meet a certain SL. Because of the numerous ransomware attacks orchestrated by criminal organisations (often protected or even sponsored by state actors), the trend is to ask for SL-3 for the product and system integration.

Figure 6: Security levels according to sophistication of attacks and perpetrators; Source Serge Van Themsche

Security Levels	Protection against:	Type of actors
SL-1	Casual or coincidental attacks	Students or internal resources
SL-2	Intentional attacks with simple means	Script kiddie
SL-3	Intentional attacks with sophisticated means	Criminal organisations
SL-4	Intentional attacks with extended resources	State Actors

IEC 62443-2-4: This is a system integration and deployment process certification, which specifies a set of requirements for the system providers responsible for integrating and maintaining the railway / industrial control systems. It leverages the maturity level concept, as in the example of part 4-1. Requirements originate in twelve functional areas:

1. Solution staffing
2. Assurance
3. Architecture
4. Wireless
5. Safety Instrumented System
6. Configuration management
7. Remote access
8. Event management
9. Account management
10. Malware protection
11. Patch management
12. Backup/Restore

For public transport and railway operators, having a product or a system certified before implementing it in its environment provides robust assurance that these solutions for the SuC have been designed and built according to specified security requirements. Depending on the importance of the SuC, requiring such certification or not should be evaluated seriously. Furthermore, Public transport and railway operators should decide on the required certification Maturity and Security Levels, based on the SuC's criticality in the rail environment.

ISO/IEC 27000 AND IEC 27001

ISO 27000 is a family of standards for Information Security Management Systems (ISMS), which can be used by organisations to protect information assets against the loss of availability, confidentiality and integrity. An ISMS provides guidelines, policies and procedures to identify and manage risk, and to achieve information security through controls that can be selected to protect information assets.

ISO 27001 specifies requirements for designing, implementing and maintaining an ISMS tailored to a specific organisation. The standard includes a variety of controls, such as information security policies, human resource security, asset management, access control, operations security, supplier relationships and incident management. The selection of controls for a specific organisation must take into account context-specific elements such as organisational objectives and operational constraints. This also means that controls that can best be implemented for one part of an organisation - such as IT in offices - may not be fully applicable for another part of the organisation, such as OT for rolling stock.

PTO procurement personnel should ensure that for critical SuCs, the vendors invited to participate in the RFP process are certified according to ISO 27000 and/or ISO 27001.

PROCUREMENT PROCESS AND SPECIFICATION FRAMEWORK

THE PROCUREMENT PHASES

Most operators have clearly identified their procurement process and - as described in section special form of procurement - usually adapt their plan in function of the specificities of the SuC to be bought. To help provide a framework for this White Paper, we can break these specific processes into three or four main timeframes, in which several public transport and railway departments play different roles. For example, the procurement phases can be summarised as: pre-tender, tender and project implementation, which can then be further broken down to the right level of granularity. Figure 7 focuses on one of the tendering phases, describing how it is applied within the context of a European public procurement process.

Another useful way of detailing the procurement process is to implement a functional framework. Figure 8 breaks down the procurement process into four phases (need assessment and definition, buying process design, proposal evaluation and contract implementation) and further refines these stages.

We won't go further in our description of these phases, as the objective of this White Paper is not to describe all the different procurement steps - which are already well known by the Procurement team - but rather to describe what are the key cybersecurity issues that this team should address during these phases.

Figure 7: EU public procurement process[5]

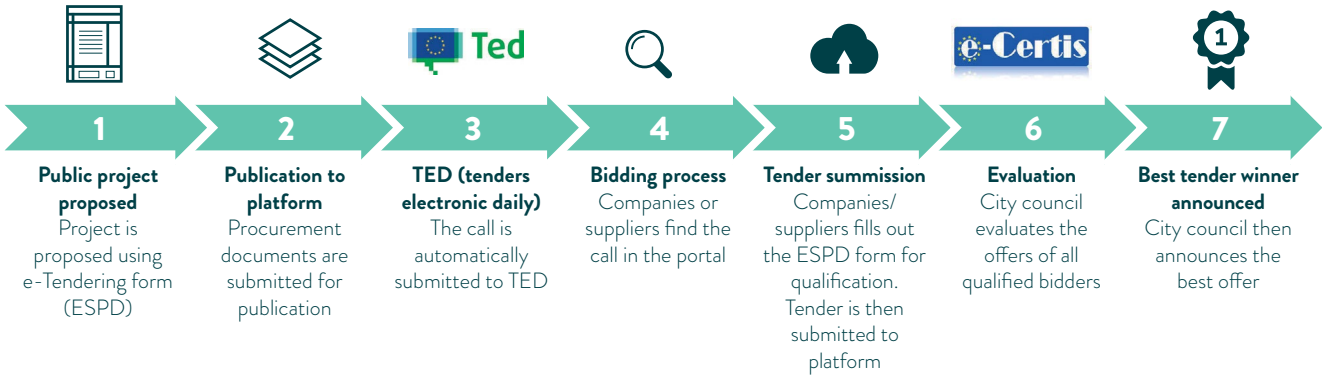
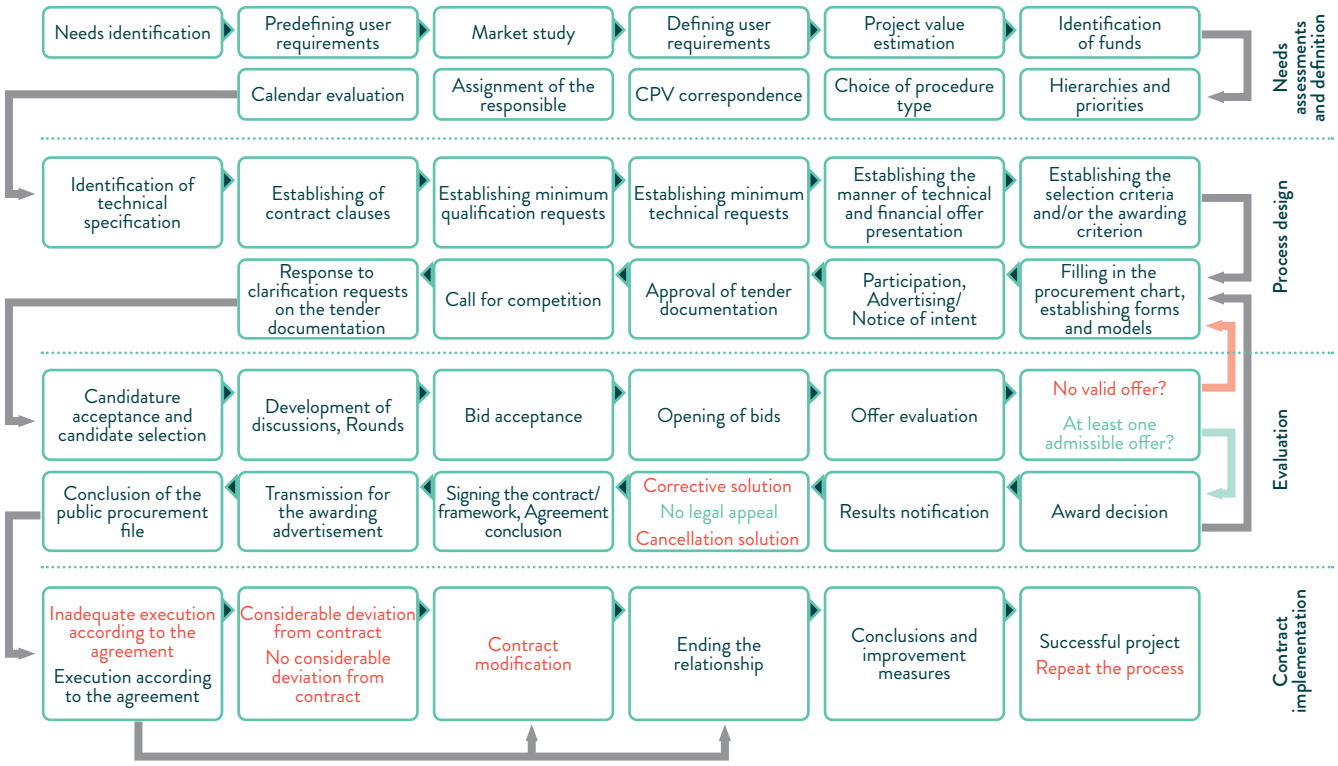


Figure 8: Example of a Process of Awarding Public Procurement Contracts[6]



5 https://ec.europa.eu/espd

6 Patraș, Mirela; Banacu, Cristian-Silviu; 2016/07/31; Critical Phases in the Process of Awarding Public Procurement Contracts: A Romania Case Study

RESPONSIBILITIES DURING THE SUC'S PROCUREMENT PROCESS

In the procurement process, functional managers or subject-matter experts can play different roles (for example decision maker, validator, or consultant). These roles can evolve over time in function of the subject to be decided upon. Hence, and in function of the procurement process' complexity, it might be advisable to establish a matrix with on one side the involved managers and on the other the subject matter, describing in this table the role played in the process.

Depending on the type of SuC to be procured, a PTO procurement process can involve various personnel from different functional departments, or even external consulting companies. Below is a list of the main departments that should be involved:

Procurement Department

This is the department that owns the entire procurement process. After equalising the technical offer (i.e., making sure that all vendors have quoted the same requirements and identifying possible gaps between the offers) with the support of the various technical departments (for example, engineering, IT, Cybersecurity), it manages the commercial discussions with the support of the legal department).

User Department

This is the functional department that will ultimately use the equipment being procured. It should be involved from the outset in the SuC's need definition. These needs must be transposed into technical specifications. It can be a department with no technical cybersecurity background (for example marketing, finance, quality, procurement) or not (for example operations and IT).

Operations Department

This oversees the operation and maintenance of the operational technologies of the transport system, responding for the required regularity of the service and the safety of the passengers. It defines the OT system requirements and the technical specifications for tenders. It is responsible for the OT system acceptance.

IT Department

This oversees the operation and maintenance of IT systems and enterprise networks. It should support the OT department (where one exists) during system specification, design and implementation phase on subject matters relating to IT/OT hardware and software capabilities and specifications. Depending on the PTO structure, it can also oversee cybersecurity matters.

Security Department

This is responsible for the physical protection of company assets and for the security of passengers. It may be consulted for defining access control to the IT/OT equipment.

Cybersecurity department

Headed by a CISO, this organisation defines the railway security policy. It drafts the information security system policies and procedures, ensuring that they are respected during the procurement process of all SuCs involving software or firmware.

IT competence for Operation Technology

The increasing usage of IT components in OT environments has created a knowledge gap in operation departments that need to be properly addressed. In some cases, the easiest way to address this issue is to let the IT department bridge that gap.

However, the IT department is focused more on privacy than on availability, and it is used to working within an Information Security Management System context, which cannot be applied in the same way as it is in OT.

Public Transport Operator managers, evaluating their organisation, should decide to:

- Ask IT department to support the OT department to define cybersecurity requirements.
- Provide competent IT staff to the OT department to define cybersecurity requirements.
- Hire external IT consultancy to the OT department to define cybersecurity requirements.

PRE - TENDER PHASE

The pre-tending phase can last from a few days to several years, depending on the criticality of SuC to be procured. During that phase, the railway department that has identified the need will define its user requirements to determine a budget, which will be approved internally or potentially allocated by public authorities. Depending on the SuC, experts from within the railway or consultants may be asked to support the initiative, helping improve the definitions of these user requirements and the budgetary envelope. During this pre-tendering stage, the role of the procurement team is more one of support to the department seeking the SuC.

The procurement team should become involved as early as possible to ensure that the right process is pre-identified and that there is already a dialogue with the main vendors. For critical SuCs, this dialogue should be done directly, or through a RFI (Request For Information) process.

Here are a few guidelines that the procurement team should contemplate at this early stage relating to cyber-security requirements. For this White Paper, we will only consider SuCs that show a certain level of criticality.

TYPE OF GOODS/SERVICES TO BE SPECIFIED

In terms of cybersecurity, the first question is if the good or service to be procured includes software or firmware. If not (for example for rail tracks, dormant sleepers or accounting audit), then no cybersecurity issues should be contemplated. If it includes software, then the next question should be whether the procured good will be considered part of an IT or OT network. Indeed, we've already indicated that cybersecurity requirements for IT and OT systems are fundamentally different (see section IT/OT divide). Since safety-critical systems expose passengers to potential physical harms, they must also be treated differently from less-critical OT systems from a cybersecurity perspective. Non-trusted systems, either because they are open (for example to the internet) or because they depend on a third party over which the PTO might have no control, must also be positioned carefully in the acquisition; the role such systems play in high-criticality SuC's must be strictly curtailed.

Hence, any procurement process of an SuC should first contemplate where it fits in the overall public transport and railway network architecture. Depending on the SuC's location, the procurement process should specify the appropriate corresponding cybersecurity solutions, processes and measures. Obviously, the challenge resides within SuCs that interface with at least one of the other three network types, as recapitulated hereafter.

These four environments, with their main security issues, are:

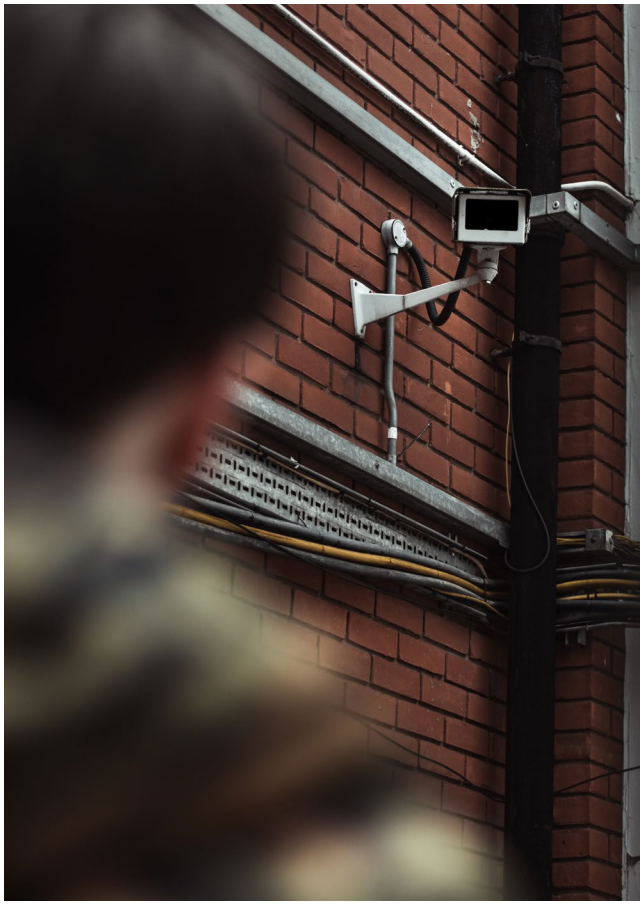
IT networks: IT security is most commonly concerned primarily with protecting data from falling into the wrong hands and being used for criminal or industrial espionage purposes. IT is also increasingly concerned with database systems or other systems being impaired by malware and potentially erased or otherwise rendered unusable unless a ransom is paid to a criminal organisation. For IT networks, the procurement team's cyber focus should be on features such as prompt detection of compromised systems, data encryption, reducing device and system vulnerabilities, prompt incident response, high-assurance backups and prompt recovery strategies for compromised components.

OT networks: OT security is mostly concerned with preventing cyber sabotage of operations components that result in physical consequences, ranging from service shutdowns to equipment damage and threats to public safety. Since all cyber-sabotage attacks are information, the focus of OT security is not protecting information, but rather protecting safe, reliable and efficient physical operations from information, most particularly from cyberattacks that may be embedded in incoming information.

Safety-critical networks: Safety-critical systems include another layer of complexity, which is the management of safety throughout the SuC lifecycle. Hence, the procurement team should ensure that safety and security requirements are well aligned via the strict observance of TS 50701.

Untrusted Network: Such networks should be insulated from the organisation. Physical segmentation is strongly recommended. This could be provided by unidirectional gateway technology, or potentially through demilitarised zones on separate physical switches rather than shared switches and VLANs.

The tendering of the SuC must be integrated within a specific tendering and legal framework and integrate dedicated Standards and technical specifications. We already described the various regulations and standards to be considered.



The procurement team should seek assistance from the PTO's legal department in establishing the appropriate framework.

It should also be assisted by personnel from within the department that defined the needs and initiated the procurement process. For highly technical matters, the appropriate engineering department for the railway can also be involved to validate the selection of the standards to be specified. Subject experts under the CISO's responsibility can also assist for those matters relating specifically to cybersecurity.

OT ASSET LIFE CYCLE AND OBSOLESCENCE MANAGEMENT

The expected long-life span of rolling stock and other railway assets – 15 to 40 years - conflicts with the much shorter life cycle of COTS hardware. The use of commercial firmware and operational systems within the railways' OT environment and the related hard-to-manage software obsolescence problem, only adds to this issue.

PTO procurement team are recommended to consult UITP's guideline on obsolescence.[7] The main topics that the team should address are:

- legal protection against obsolescence
- ensuring coherence with the obsolescence management policy of the railway
- defining which type of obsolescence risk should be addressed for the SuC
- minimising obsolescence during the SuC design
- ensuring that existing cyber tools (for example, Continuous Monitoring System) can identify obsolete assets of the SuC.

Procurement teams should also be alerted to the fact that unpatched software vulnerabilities in out-of-support products is not the most important consequence of premature product obsolescence. The global cybersecurity threat environment continues to degrade rapidly. Arguably, the most important consequence of obsolescence is that older hardware and software - whether or not they are out of support - may not incorporate security protections against modern threats. Indeed, such protections may be unavailable as add-ons to old products and - even if such protections were available - new protections often consume more computing resources than are available in older products. Therefore it is important to assure that those products maintain any required performance reserve capabilities.

Procurement teams may therefore wish to specify strong physical attack information-flow control measures, such as hardware-enforced unidirectional gateways and strict controls over removable media, laptops and other removable devices. This is in addition to built-in security and patch programmes. As all cyber-sabotage attacks are information, then physical and hardware-enforced measures that strictly control the flow of potential attack information tend to maintain their protective capabilities even as products age.

SPECIFICATION OF CYBER LONG-TERM SUPPORT

As we have seen, there is often a mismatch between the life cycles of various railway assets. It is certainly the case for the use of cybersecurity hardware components that rely on IT COTS product, which must be replaced every five to ten years. Hence the tender specifications should define the long-term responsibility of the SuC's selected vendor, who must also provide cybersecurity protections. For practicality reasons, a period of five years is an appropriate term for the availability of the cybersecurity solution.

Indeed - and contrary to solutions that can be proposed for the complete lifecycle of for their term - cybersecurity solutions that provide protection against threats evolving constantly should always specify the use of updates for a reasonable period. Such updates should be released following identification of new high-risk malware or at least every six months. Continuous monitoring systems, firewalls and IDS are good example of products that should promptly integrate new virus and malware protection.

A description of the PTO's patch management policy in the specification should help the vendor address issues concerning updates and help the railway minimise operational discontinuity on its network. If the PTO doesn't have the available resources to or does not want to take over the cyber-security responsibility of the SuC protection, the tender might specify Service Level Agreements (SLAs), which will describe in greater details how incident response and recovery management are done.

PRELIMINARY RISK ASSESSMENT

The procurement process should rely on an initial risk analysis of the SuC, which should act as a reference and as a conceptual approach. It should be conducted for the SuC and each of its subsystems and interfaces for the following issues: safety, business continuity, operations and maintainability, disaster recovery and degraded modes of operation.

7 Obsolescence on operational environment and cybersecurity.

The SuC's risk analysis should be based on the functional mapping of the required subsystems and devices running on its network. Supplying a table summarising the SuC's connections to other railway systems and network types (ACN, OCN, SCN and untrusted networks) is recommended, as well as their physical location (for example in the OCC, on the wayside and in the train).

Cybersecurity solutions (for example continuous monitoring solutions, firewalls, unidirectional gateways and NTP servers) already existing on the other systems and networks should be indicated. Preliminary cybersecurity solutions for the SuC should be identified and proposed, usually assuming that the SuC's environment includes a Network Management System (NMS). These solutions should take into account the internal users' network connection requirements as well as the connections to external environments (for example, connections by WAN via phone service providers). Any forbidden connection to an untrusted network should be highlighted, taking into account the fact that high-quality unidirectional gateways can be used in the event that vital information still needs to be transmitted.

Ideally, the specification should include - as a reference - a diagram summarising the initial conceptual security architecture that illustrates the SuC's network and devices, with the proposed cybersecurity solutions to provide protection against the security risks. The 'do's and don'ts' connections should be highlighted.

For clarity reasons, it might be appropriate to provide a table in the specifications showing:

- The communication flow (none, unidirectional, bidirectional) between the SuC's network and the other networks.
- The security level of these communication flow according to certain criteria (for example availability, monitoring, detection, authentication, hardening, support).
- The mandatory cybersecurity solutions, if identified (for example continuous monitoring system, firewalls, unidirectional gateways).

It is fundamental that the RFP documents highlights the fact that a full evaluation and risk analysis will be conducted as part of the preliminary and detail designs and will be approved by the railway or public transport operator, according to these specifications. A brief description of what this risk analysis should look like is recommended to level the playing field, and to ensure that every vendor integrates such a study into their costs.

CLOSING THE PRE-TENDING PHASE

The SuC pre-tendering phase is closed when a financial envelope has been identified, presented to, and approved by, the various railway stakeholders and the budget has been allocated. The budget should include the necessary resources to perform the procurement activities during the tender and project implementation phases. At this stage, all technical specifications with useful documentation in annex must be completed. A copy of the future contracts with its term and conditions should also be added to the RFP documents.

TENDER PHASE

The special forms of procurement described will obviously influence the tendering phases and shape its outline. In its simplest form, called the open tender, the RFP is issued together with the RFQ. Qualification and evaluation criteria are published together with the copy of the future contract in the same package of documents. A frequent variation to this simpler tender process is a two-stage tender, requiring pre-qualification. This is where the pass/fail test of qualifications is conducted at an earlier stage; the RFP is issued, or candidates are invited to send proposals only after the qualification process is finished.

Bidding processes that include various interactions or dialogue between the vendor and procurement teams are also possible. The most likely stages are:

- Tender advertising and issuance of the documents.
  - Often, the PTO will require a site visit to the environment where the SuC will be implemented.
- Bid preparation by the vendors.
  - During this period, the process allows for a time where the vendors may ask questions formally, known as the RFI (Request For Information) process. There may even be discussions to define the contract solution during the dialogue stage (for example a competitive dialogue in the EU).
- Bid submission by a certain deadline.
  - Often, the PTO will require a bid bond insurance to ensure that the vendors are serious.
- Evaluation of qualifications and proposals.
  - During this phase, the procurement team will equalise the offers (i.e., make sure that all requirements are costed by all the vendors) to ensure a fair level playing field.
- Signed contract award.
  - Financial collaterals, such as performance and warranty bonds, will be required.
- Financial close, in more complex bid structure where the vendors are usually part of a concession in a PPP-structured finance project, a process by which the banks must close all financial concerns to bring the financing.

CONTRACT IMPLEMENTATION (POST TENDER)

Contract implementation can take from a number of months to several years, depending on the complexity and workload of the SuC being procured. Several good project management practices are necessary, but these go far beyond the objective of this White Paper. We will now briefly describe how to address cybersecurity during the SuC's integration within the overall IT or OT environment.

DETAILED RISK ASSESSMENT

As indicated in on preliminary risk assessment, the selected vendor should, during the contract implementation phase, ensure that all relevant risks to the SuC's

environment are clearly identified and integrated within a risk analysis. This must be approved by the PTO and potentially by national authorities before the SuC's implementation. This should assess the potential worst-case physical consequences when there is an attack by outsiders or insiders on the SuC, mis-operating the system's CPUs and other components.

The level of confidentiality associated with the SuC's integrity and availability should be mapped, identifying the data required for the attack. Furthermore, confidentiality issues on important business and industrial espionage - more generally as part of the PTO's policy on data loss prevention - should be identified and implemented according to the SuC's functional requirements and architecture. This should also detect devices with high vulnerability and establish the security solutions that will mitigate the risk.

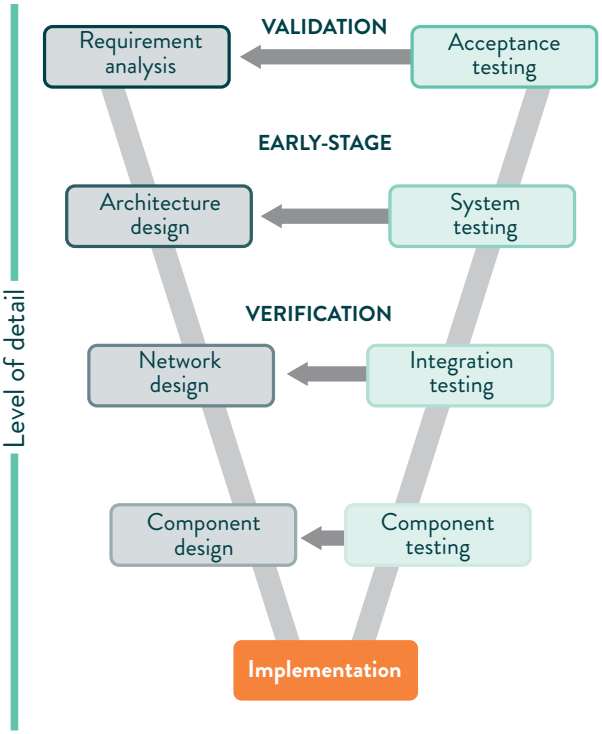
Moreover, the risk analysis should integrate an assessment of the potential worst-case physical consequences resulting from an attack on the SuC's functionality. For each main functionality of the SuC, the realisation of risks should describe the physical impact that mis-operated devices, database, programme coding, networks and other features may have. This analysis should be conducted according to the various potential threats.

Finally, cybersecurity, like safety, is on a spectrum, not a pair of discrete 'yes' or 'no' states. As no SuC can ever be completely 'secure', there always remains a way to compromise the SuC with a cyber-attack. Furthermore, business decision makers usually understand specific attack scenarios and consequences far better than they do abstract risk metrics. The final detailed risk assessment should therefore always include a section describing - in layman's terms - at least three or four of the simplest cyberattacks capable of causing serious physical consequences. The procurement team and other stakeholders should review those attacks to ensure that they represent what the team regards as acceptable risks. The risk assessment should also include indications of which of these attacks are likely to become more likely or widespread as the threat environment evolves over the life of the SuC.

DEVELOPMENT CYCLE IN V

The V-model summarises the main activities to be performed and the results that must be produced during the SuC development. This is mainly used for systems composed of equipment where there may be some firmware. As cybersecurity is mainly concerned by software, the software industry has developed different models with varying pros and cons.

Figure 9: Stages of the V-model



SOFTWARE DEVELOPMENT LIFE CYCLE

Software development may have a huge impact on resilience of the cybersecurity posture of the SuC to be delivered. To describe good practices in this area, we can use a simple linear model, SDLC (Software Development Life Cycle). At the initial stage of the SuC project implementation, the SDLC process is initiated to create documentation of the initial design concept. The project is refined, developed, tested, deployed for the PTO to use, and ultimately retired at the SuC's end-of-life. It is a logical progression, with each completed development phase being replaced by the next. While there are several variants of this model, they all usually describe seven discrete phases:

- **Planning:** During this step, the breadth and scope of the project implementation is delineated.
- **System Analysis:** At this stage, the RFQ's technical requirements are adapted to create functional requirement documents, which will drive the specific software design for programmes. Its output should result in screen prototypes, preliminary data and process flow documents as well as all other diagrams that will support the system design phase.
- **System Design:** At this stage, the software development team should provide high-level design specifications. Such specifications should include documentation (for example, context diagram, data flow diagrams, flow charts, data modelling) that support

the overall system design.

- **Development:** This is typically the longest phase of the process. It starts when functional requirements are transitioned into coding. The SuC analysts segment the functions into modules, which are usually distributed to the development team for coding.
- **Testing:** This involves several types of testing: string testing, where a series of programmes/modules are tested for interaction; system testing, where the entire system is tested for functionality; and user testing, where users confirm that the project meets their desired expectations.
- **Implementation:** The SuC modules and programmes are transferred from the test bench to the railway environment. During this rollout, a final verification and validation of the code and system performance is conducted to confirm that the system meets the RFQ's requirements.
- **Maintenance:** At this stage, the project implementation stops and is replaced by the operational phase. However, software must be updated and patched, particularly those cybersecurity solutions that must detect ever-evolving malwares.

Nowadays, many software developers are more familiar with variants of the SDLC, which drive deliverables to meet the RFQ requirements. These various approaches include agile software development, rapid application development, feature-driven development, dynamic systems development, LEAN development and SCRUM development.

SECURITY BY DESIGN

Railway and public transport operators must think about cybersecurity from the outset. Security by design means that the vendor's team has designed the SuC software, has reduced the likelihood of flaws that may compromise a company's signalling and other industrial control systems. Every component added to a product, or product to a system, can present inherent vulnerabilities. Knowing when it happens and whether it affects the final product requires an in-depth understanding of the components making up the product or the code constituting the software. Therefore, it is recommended to maintain a programme for monitoring any incorporated components/products for new vulnerabilities and investigating the impact of any that are discovered. This is particularly important, as software vendors often create products by assembling open source and commercial software components.

As maintaining such a comprehensive record manually can be time consuming, best practice is to use a companion artifact to a Software Bill Of Material (SBOM). This allows manufacturers to communicate the exploitability of a vulnerability discovered in one of its software components listed in an SBOM. It also enables the system integrator to trace and understand if the vulnerability identified is likely to impact the system's security.

As we mentioned earlier (product cybersecurity certification), it is recommended for critical SuCs that PTOs assess if the pre-qualified vendors should or not demonstrate the right level of maturity in their product development process, by being homologated according to IEC 62443-4-1. Likewise, they should decide if the vendor must show security assurance levels, bringing their solution to the required security level by being homologated according to IEC 62443-4-2. Moreover, they should decide whether system integrators must have their system and enterprise homologated according to IEC 62443-3-3 and IEC 62443-2-4 respectively.

SOFTWARE DEVELOPMENT SECURITY TESTING

Good software development practices require penetration testing for the application, system component or system platform. The attack performance reviews should be periodic and obviously intentional. Consulting companies

specialised in penetration testing can find coding flaws that are likely to be used by malevolent actors to penetrate the SuC. Thus the essence of security testing is for the development team to understand the weakness in the application software or operating system.

Penetration testing should be used to determine the overall fitness of a development process. Simply patching or remediating specific vulnerabilities or attack paths discovered by a penetration tester is the wrong way to use the test results. In practice, every path of compromise discovered by a penetration tester represents a failure of the secure software development process. Penetration testing should therefore be used to assess the strength of the process, not the strength of a particular product or SuC.

For software development, the attack surface includes:

- An understanding of the value of data used in the software and how it is protected by the developed code.
- The sum of all paths taken by data and commands, originating from the SuC.
- Checking that the code protects these identified data and command paths, including the resource where the programme connects.
- Thorough inspection of the functionalities providing authentication and authorisation to the execution of the system code.
- Data stream validation of suitable encoding, decoding and encryption/decryption.

To perform a software security test first requires establishing a baseline, so that any future changes can be measured and confirmed to the baseline. This requires the development of an attack surface map. This denotes several potential attack vectors, including points of entry to the software, user display forms or run-time usage, as all will present attack vectors that can be leveraged. Vulnerability scanning tools noted on the OWASP website can support the coding developer in mitigating security issues. After mapping the attack surface, higher risk areas need to be identified and prioritised. In summary, developing secure code requires implementing a configuration management process, establishing a baseline, mapping the attack surface and identifying the highest-risk areas.

Again, as all cyber-sabotage attacks consist of information, an inventory of information flows entering an SuC is important to understanding the attack surface. A complete inventory of incoming information flows also represents a complete inventory of incoming cyber-sabotage attack vectors. Every one of those incoming vectors must be controlled as thoroughly as is practical.

RAISE CYBERSECURITY AWARENESS AMONG STAFF

During the contract implementation (and also afterward), the PTO should raise awareness among its employees, agents and representatives - as well as its vendors - of cybersecurity in general and the risks relevant to the performance of their specific roles and duties.

INFORMATION SECURITY SYSTEM SPECIFICATION

GENERAL PRACTICE

We cannot repeat enough that cybersecurity is a cross-functional issue. Hence, it must be applied to all contemplated purchase SuCs of software or firmware. To ensure coherence between the various procurement processes, a specific document called an Information Security System (ISS) should be created, in which the main railway cybersecurity principles and requirements are detailed. Parts of, or the entirety of, the ISS document should be included in all tender documents of relevant SuCs.

ROLES AND RESPONSIBILITY

The CISO organisation should be responsible for editing, updating and informing on how to use the ISS throughout the railway or PTO organisation. The ISS should address IT and OT environments. OT cybersecurity principles in the ISS must reflect the sensitivity and Security Levels of protected systems.

Below is a high-level organisational chart, where the Chief Information Security Officer (CISO) is positioned alongside their fellow officers. The following organisational chart positions the CISO within the overall cybersecurity risk management attribution.

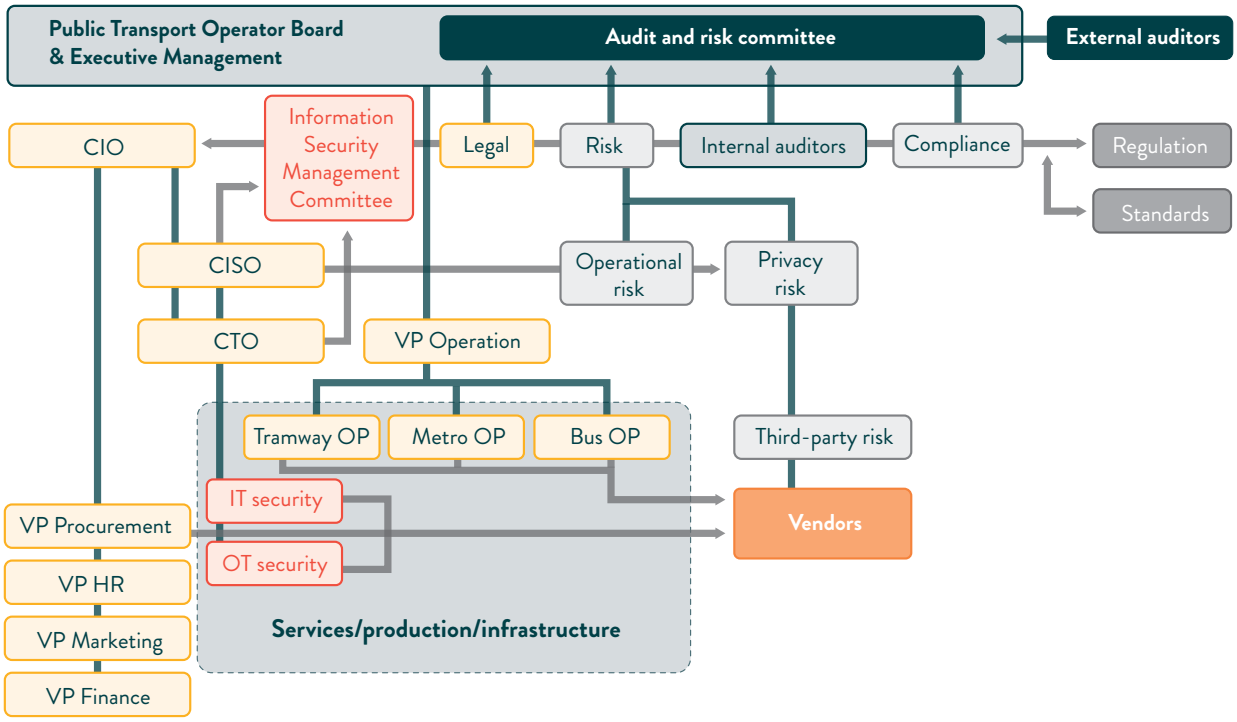
THE CISO ORGANISATION INVOLVEMENT IN PROCUREMENT PROCESS

If no OT specialists are available, someone from the CISO organisation should be assigned to support the procurement team acquiring an SuC critical to the operational environments. The assignment period should be sufficient to provide the guidance throughout the drafting of the RFP and during the project implementation. Different employees might be allocated throughout the procurement phases, depending on the skills required. For small PTO organisations, someone from the IT department with cybersecurity background, or a trusted consultant, can be allocated to support the procurement team.

ISS PRELIMINARY RISK, THREAT AND VULNERABILITY ASSESSMENT

The ISS should define a high-profile risk, threats and vulnerability assessment for the entire railway, which should be the basis of the preliminary risk and vulnerability assessment of the SuC to be procured. It should be based on TS 50701/IEC 62443. Information, such as a high-level cybersecurity architecture, should be included and shared with suppliers of the trusted vendors list. In the event that the railway already went through the process of developing its corporate risk and vulnerability assessment, some or all of this document may be shared (or not) in line with the PTO's confidentiality policy.

Figure 10 - Organisation chart; example based on risk management responsibility; source Serge Van Themsche



SECURITY POLICY AND PROCEDURES

The ISS should define the overall security policies and procedures for the IT and OT environments for the entire PTO organisation. Each selected supplier should issue and submit for approval its recommended policy and procedures for the SuC, which would complete the operator's overall ISS security policy. Hence the ISS is most likely going to need updates following the acquisition of a significant SuC.

The security policy should include a classification and designation guide according to the data's importance, integrity, availability and value, explaining how to deal with IT/OT information and assets. To the greatest extent possible, the policy should ensure that responsibilities are separated, so that no individual has complete control over related critical IT/OT operations. The following duties should be separated: operations, system administration, network administration, database administration, application programming / development testing and security management.

The policy should also contemplate obsolescence management and how software updates and patching should be addressed. Given the real threat that obsolescence can generate, it is recommended that the ISS refers to the international standard IEC 62402:2019, which contains requirements and guidance for obsolescence management applicable to any organisation. The railway and public transport operator should obviously adapt such a standard to its specific environment and to the SuC life cycle.

ENHANCE SECURITY CONTROLS FOR WIRELESS COMMUNICATION

The ISS should propose overall policies on specific controls of wireless communication, as these offer high level of vulnerability. Policies on public wi-fi access in onboard environments and in stations in particular should be clearly defined in the ISS. The following actions are also recommended to minimise the security risks:

- The wi-fi network should be separated from all OT networks and from non-relevant IT network segments.
- Access should be restricted from the wi-fi segment to the internet.
- Remote management access of wi-fi routers should be disabled.
- Wi-fi Access encryption (for example, WPA2) with appropriate password protection should be used.
- Logs and monitoring of the wi-fi network should be implemented.

CYBER SECURITY TESTBED AND MODELLING POLICIES

Nowadays, an increasing number of operators are modelling their operational environment. A station or train digital twin is a digital version of the physical entity that replicates the network environment, with all its connected subsystems. These models are not used merely for integration and debugging purposes; they also provide an environment for testing the interface between other subsystems and the SuC, to ensure that the resulting system is not prone to cybersecurity vulnerabilities. The ISS should describe such testbed environment and modelling policies. The SuC procurement team should ensure that the supplier designs, installs and maintains its digital twin as part of its deliverables for supporting testing and commissioning during the delivery phase and subsequent maintenance, considering all necessary interfaces. The cyber-security tests on the modelled environment should be undertaken before the system's approval.

The objectives of these tests are to:

- Validate the cybersecurity measures, including data availability, integrity and confidentiality.
- Test and approve new, updated components before adding them to the production environment.
- Learn pattern of actions, to simplify forensic activities after a cybersecurity event.

The test should ideally be conducted on the operator's testbed model, but if this doesn't exist, then the RFQ can suggest conducting it on the supplier's own testbed model. In this event, the testbed and its components

should ideally be transferred to the operator following completion of the tests. Such a testbed is an important component for emerging mitigations for sophisticated supply chain threats.

ESTABLISH BUSINESS CONTINUITY PLANS

Contingency plans should be developed, documented in the ISS, and maintained to ensure that essential level of service can be delivered following any loss of processing capability or destruction of IT/OT Systems. All SuCs to be procured should describe their Disaster Recovery (DR) capabilities. The SuC's implementation of contingency plans should not compromise data sensitivity or integrity requirements. Critical security controls should be resilient and easily accessible. The ISS contingency plans should be updated following the SuC's acquisition.

SUC DATA BACKUP

The backup measures should maintain the same security policy (confidentiality, integrity and availability) on the backed-up data as on the operational environment. Backups of sensitive data should have strong encryption and solid key management technology. The system should have the capability of backing up and restoring all security-relevant data. Processes for secure handling of backup media should be developed and implemented, and each critical environment should be individually backed up.

Back-up mechanisms should rotate the media used or have some other mechanism of ensuring that at least some back-up copies of each component in an SuC are offline or otherwise physically inaccessible at any given moment in time. Modern ransomware and other cyber-sabotage malware increasingly have the ability to encrypt or erase online backups as well as primary running copies of software systems and data.

ACCOUNTING FOR INTEROPERABILITY ISSUES

The operator should develop a functional mapping of all sub-systems and networks, which will support the system's risk analysis. The operator should write, in its ISS, a table that summarises a list of these components and their interoperability, split on one side according to the network types (for example SCN, OCN, ACN or others) and per implemented or to be purchased SuC (for example SCADA, CBTC or PIS) on the other side.

ALLOW AUDITING AND LOGGING

A continuous monitoring process for identifying, authenticating, authorisation and controlling the access to, and administration of, information infrastructure security should be developed for OT and IT environments. This will determine whether proper security has been established and maintained. All security events should be managed at a SOC level, which can be installed and operated within the OCC or remotely through cloud-based solutions.

The railway's information security system should be capable of generating audit information for the following security-related events, at minimum:

- Job or process status
- File and database access, where applicable
- Device connection, disconnection and reconfiguration
- Network status messages
- User log-on and log-off attempts
- System operator commands and responses
- Any actions performed under administrative privileges
- System status messages or requests for configuration changes
- Changes to system logging facility status, access control information and to lists of authorised users
- Detected security incidents
- Unauthorised network scanning, such as port scans.

The recorded audit shall be retained for a minimum of one year, to provide support for incident forensic investigations and to meet regulatory or organisational required information. The information security system should be capable of generating the following logging data:

- Nature of incident, with exact time stamp, according to a NTP server
- User and device (for example, IP/MAC address, host name) identification
- Job or process identification
- Identification of resources accessed and through which means
- Configuration details
- Details of the activity performed.

Security event logs shall be kept for each important device and system for a minimal period of one year, protected from unauthorised access, modification and deletion. They shall be sent to the Security Information and Event Management (SIEM) for further analysis, correlation and evaluation, in order to identify and respond to suspicious activities.

ENCRYPT SENSITIVE PERSONAL DATA AT REST AND IN TRANSIT

The ISS should emphasise that accessing the confidential information environment must require authentication and be restricted to legitimate business needs. User privileges should be allocated using 'need to know' and 'least privilege' business principles. The operator should implement strong privileged user accounts (for example, administrator) to the minimum number of personnel required. The use of these accounts should be audited and monitored. A unique user ID should be assigned to any authorised entity requiring access. Accounts of personnel leaving the company or project should be controlled and these employees have their access cancelled.

The operator should enforce a strong password policy, using cryptographic protection. Remote access should be controlled and implemented using an encrypted channel, such as Secure Sockets Layer (SSL) and/or Virtual Private Network (VPN). It should use multi-factor authentication, such as a user password plus a one-time password/PIN.

Hard copies of confidential information and all electronic media containing such information should be securely stored and protected. The transfer of confidential information in electronic format should be via secure channels only. Data delivered on removable media shall be encrypted. Backups containing confidential information shall be kept secure.

SECURITY CLEARANCE

Various roles during the SuC implementation may be defined as 'designated positions', as determined under the national law, by the operator or national security authorities. For these positions, personnel from the operator, supplier or its subcontractors may be required to undergo background and security reliability checks, and to obtain security clearance before being appointed to the various positions, in accordance with the procedures of the operator and/or the national security authorities. Only qualified personnel who have passed the reliability checks may be allowed to hold these Designated Positions and may, from time to time, have to undergo periodic confirmations of security reliability or additional security reliability checks. The ISS should define which of these positions will require clearance.

CYBERSECURITY TRAINING (INTERNAL/EXTERNAL)

The ISS should define what type of cybersecurity training will be required for employees who will design or implement the SuC to be procured. A general cybersecurity awareness process will be implemented for all vendors' employees working on the SuC project. Specific training programmes may be added to the RFP. The vendors may develop a specific cybersecurity training programme.

STANDARDS TO BE ENFORCED

All railway SuC procurement processes should consider the ISO 27001 standard, IEC 62443 standards and, where applicable, prioritise its more specific declination for OT railway systems in TS 50701. Thus an SuC procurement process that would fall under the IT classification should consider the ISO 27001 standard. In the case of an SuC running on an OT network - particularly if it concerns a safety-critical system - the procurement process shall enforce the technical specifications of IEC 62443, and particularly TS 50701.

SECURITY ADMINISTRATION

Security policies and procedures, managed by the organisation CISO shall be edited and maintained. Classification and designation of sensitive information running on railway assets shall be updated, ideally in real time through an Asset Management system. These assets classified into Security Levels, should consider the importance, integrity, availability and value of the data generated by the SuC. The administration should ensure that separation of duties is accounted for.

ASSET INVENTORY AND CONFIGURATION MANAGEMENT

Asset management is a critical component of the foundation of cybersecurity operations across Public Transport Operations. Without it, no real cyber protection is possible, and no compliance can be achieved. Indeed, this process identifies on a continuous, real-time basis, the thousands of IT/OT assets that the operator owns and the potential security risks or gaps that affect each one. These assets take many forms, from the traditional PCs and servers, to the specialised IoT, OT devices and software-defined resources, like a cloud-based database or a company-owned domain. Asset management provides the visibility needed to build a comprehensive security strategy to mitigate threats quickly and proactively. Though asset management could theoretically be done manually, continuous monitoring systems are essential to provide real-time network visibility, physical mapping and asset inventory, enabling the management of these thousands network components.

Having said that, not all continuous monitoring system can propose the same auto-discovery features. Standard IP monitoring systems have been designed to identify IP based assets. In an exclusively IT world, IDS and firewall technologies can provide good network visibility. Newer generation can even provide greater visibility with features such as SSL inspection. However, these IDS and firewall technologies are focused on IT assets. Even when they are able to detect an IP address automatically, they cannot understand the OT asset's operational environment and identify if this asset is behaving abnormally. To do that, the asset management system must stream in real-time the dataflow, performing Deep-Packet-Inspection on the OT network. For instance, DPI of non-IP networks are essential to understanding that a signalling's interlocking system, or the PLCs and RTUs of a SCADA system require a new patch or are behaving abnormally.

Setting a baseline upon which the entire railway ISS defence strategy will be based upon requires a deep understanding of the railway, telecom and SCADA protocols, which are often proprietary. Selecting a technology that is agnostic to the Vendor's proprietary protocols is vital,

particularly if the PTO wants to deal with its OT configuration management and gain visibility on all its hardware, firmware and OS versions running on its networks.

It is strongly recommended to select railway-specific continuous monitoring systems that provide automatic discovery of the railway assets' functionality, enabling their identification as a field element or interlocking in a signalling system, a VCU running on a TCMS in a rolling stock, or a RTU protecting a traction sub-station. These modern tools not only eliminate blind spots in the network by showing the actual assets existing in the network but also picture the networks' topology, display updated active connections between network assets as well as their Security Levels. These, we will see, must be split according to zones and conduits, as required by TS 50701.

Moreover, some newer continuous monitoring systems can provide a physical display of the assets in the railway environment. This feature becomes extremely useful in PTO environments where assets can be installed in hundreds of stations or in tunnels. Knowing where the asset is physically located allows the cyber- and physical security teams to be deployed and check whether an incident is due to product failure or a malevolent act.

SECURITY ARCHITECTURE

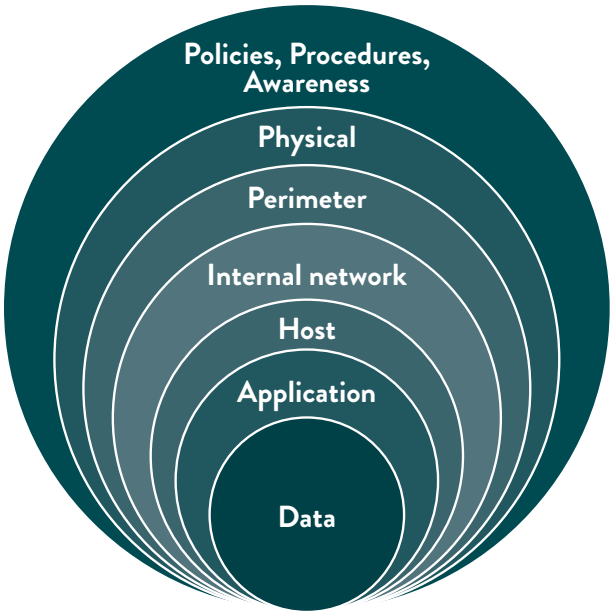
Best practices based on no-nonsense policies and procedures, well-trained employees and an organisation that has the compliance with the main cybersecurity standards at heart can go a long way in protecting railway and public transport operators against cybersecurity attacks. However, the scale of the attack surface, the complexity and the number of interconnected IT and OT systems running in PTO environments, make technological choices vital for implementing efficient cyber-protection measures in railways.

Since there is no one-size-fits-all solution, TS 50701 strongly recommends that operators adopt the DID principle, where a succession of complementary technological barriers are erected around the assets. Clearly, one of the underlying bases for such a fencing strategy is that all assets running on any SuC or network have already been identified, as described in the previous paragraph (asset management). Without this, any cyber attacker can penetrate via an unidentified asset and inflict severe damage to the network.

DEFENCE-IN-DEPTH PRINCIPLES

DID is used by TS 50701 as a guiding design principle to ensure that any human or equipment failure, at one level of defence, cannot propagate to subsequent levels. The

Fig 11: Defence-in-Depth protection layers



independence of these different levels of defence is a key element in meeting this objective, and should be deployed for all security controls and procedures. The SuC's design should impede a cyber intruder's progress, while enabling the SuC's network to detect and respond to the security breach, as well as providing mitigation measures to reduce or eliminate the consequences of that breach. Hence a PTO should integrate within its defence a mix of passive identification and detection solutions (for example, IDS and continuous monitoring systems) along with active protection that can either block returning malwares (for example RAT), completely physically such as a unidirectional gateway or logically through software (for example SOAR, firewall or IDP).

The DID architecture should consider security measures around the following five barriers: perimeter, network, device, application and data. For each one of these, the ISS should tackle the following technologies, suggesting which is mandatory or advisable: Network segmentation; DMZ IDS; IPS; VPN; Firewalls Antivirus software; Authentication and password security; Timed access control; Vulnerability scanners; Central control; Audits and logs (SIEM), as we will describe in the next section.

It is also important to note, that physical security (for example access control, physical barriers, etc.) is part of this DID strategy.

A sound ISS architecture based on DID principles requires that all layers provide graded protection against a wide variety of security incidents, both within the SuC or generated outside of this SuC, including human errors. In the next section, we will describe the technologies and concepts that should be enforced in PTO environments.

CYBERSECURITY PRINCIPLES

DID is one of the main principles described by TS 50701 and IEC 62443-3-3. These principles are relevant when specifying technologies, as they influence the way that cybersecurity requirements must be applied to protect OT and safety-critical systems. These standards refer to 17 principles.

1. **Secure the weakest link**: Cyber protection is as good as its weakest link.
2. **Defence-in-Depth:** See above
3. **Fail Secure:** A function must be designed in a way that - in the event of failure - the security function or system delivering the function remains secure.
4. **Grant least privilege:** Each component should have only the privileges required to accomplish its specified functions, but no others.
5. **Economise mechanism:** The integration of selected cybersecurity countermeasures realised with elegance (clarity, simplicity, necessity, expandability), together with a precise definition of the functional behaviour to support ease of analysis, inspection and testing.
6. **Authenticate requests:** It is necessary to check the identity of users (human users, components/devices and processes) to protect against unauthorised access and to ensure the identity of the sender of a network message
7. **Control access:** In railways, access to all resources, assets and objects must be controlled to only grant access to authorised entities (users, programmes, processes, or other systems).
8. **Assume secrets are not safe:** Implement measures to compensate for the leakage of the information.
9. **Make security usable:** Security that is too complicated to implement will not be used, which defeats its purpose.
10. **Promote privacy:** Collect only the minimal amount of personally identifiable data for a given user category in a given application.
11. **Audit and monitor:** These capabilities (statically for components and dynamically for dataflow) are fundamental for operating and maintaining all railway control systems.
12. **Proportionality principle:** Tailoring the cybersecurity strategies to the magnitude of the risks, accounting for the practical constraints imposed by the SuC's objectives and its environment.
13. **Precautionary principle:** This requires protective action when there is a risk to the SuC. The mere possibility of damage should be enough and doesn't need a concrete probability.
14. **Continuous protection:** All components and data used to enforce the security policy should have uninterrupted protection consistent with the security policy and the security architecture assumptions.
15. **Secure Metadata management:** Metadata must be considered as top priority with respect to security policy when a policy requires protection of information.
16. **Secure Defaults:** The default configuration of a system should reflect a restrictive and conservative enforcement of security policies.
17. **Trusted Components:** A component must be trustworthy to a level at least commensurate with the security dependencies it supports.

CYBERSECURITY TECHNOLOGICAL SPECIFICATION

As figure 11 above highlights, no technology by itself can provide the correct level of cyber protection. Hence technologies must be integrated within a favourable context where sound policies and procedures, supported by clear principles, are applied by well trained personnel. In the following sections, we will describe technologies without necessarily explaining again these security principles, procedures and policies.

To classify these technologies, we will make reference to TS 50701, which relies on the standard IEC 62443-3-3, where the cybersecurity requirements are grouped into seven Foundational Requirements classes (FRs):

- FR1: Identification and authentication control
- FR2: Use control
- FR3: System integrity
- FR4: Data Confidentiality
- FR5: Restricted data flow
- FR6: Time Response to Events
- FR7: Resource Availability

For each one of these, a four-stage security level should be established. The minimum Security Level Target (SL-T) is 1, and the maximum is 4. This must be done for each asset and conduit within the SuC. To gain a better understanding on how this SL-T rating is done, check Annex 2, which describes how to specify a signalling system (such as the SuC) with the right level of cybersecurity protection.

In this section, we highlight the main cybersecurity technologies, which together enable the coverage of the 17 principles described. Figure 12 is a matrix showing the relevance of a principle for a given FR. It also describes the SRs for an SuC, which can be found in the TS 50701 standard.

TS 50701 describes around 50 SRs (for example, SR.1.1 human user identification and authentication). However, this report does not pretend to cover all of these, and the reader should look at TS 50701 for more precise information.

For clarity reasons, we have decided to present the various technologies in function of these seven FRs, rather than the SRs. Furthermore, in addition to this simpler presentation, some technologies can satisfy a number of security requirements (for example, continuous monitoring solution that for example provides – as well as monitoring - IDS protection, virtual segmentation, asset

Fig 12: Matrix of principles, foundational requirements and security requirements; source Serge Van Themsche

No	Principles	FR1 (IAC)	FR2 (UC)	FR3 (SI)	FR4 (DC)	FR5 (RDF)	FR6 (TRE)	FR7 (RA)
1	Secure the weakest link	SR1.6		SR3.2		SR5.1, SR5.2		SR7.7
2	Defense-in-Depth			SR3.2, SR3.5	SR4.3	SR5.1, SR5.2, SR5.3		SR7.1, SR7.2
3	Fail secure			SR3.3, SR3.6				SR7.3, SR7.4, SR7.6, SR7.8
4	Grant Least privilege	SR1.1, SR1.2	SR2.1	SR3.9	SR4.1		SR6.1	SR7.2, SR7.7
5	Economise mechanism	SR1.3	SR2.2, SR2.5, SR2.7					
6	Authenticate requests	SR1.1, SR1.2, SR1.3, SR1.4, SR1.5, SR1.6, SR1.7, SR1.9, SR1.11, SR1.12	SR2.1, SR2.2, SR2.3, SR2.4, SR2.12	SR3.1	SR4.1, SR4.3		SR6.1, SR6.2	SR7.2
7	Control Access	SR1.1, SR1.2, SR1.3, SR1.6, SR1.11	SR2.1, SR2.2, SR2.3, SR2.4, SR2.5, SR2.7	SR3.2, SR3.5	SR4.1, SR4.2	SR5.2	SR6.1, SR6.2	SR7.1, SR7.2
8	Assume secret not safe	SR1.5, SR1.7, SR1.8, SR1.9, SR1.10			SR4.1, SR4.2, SR4.3			SR7.3, SR7.4, SR7.6
9	Make security usable	SR1.3, SR1.4, SR1.5, SR1.7, SR1.8, SR1.9, SR1.10, SR1.11, SR1.12		SR3.2, SR3.4, SR3.7, SR3.8			SR6.1	
10	Promote privacy	SR1.12		SR3.7	SR4.1			

No	Principles	FR1 (IAC)	FR2 (UC)	FR3 (SI)	FR4 (DC)	FR5 (RDF)	FR6 (TRE)	FR7 (RA)
11	Audit and Monitor	SR1.13	SR2.8, SR2.9, SR2.10, SR2.11	SR3.2, SR3.3, SR3.7			SR6.1, SR6.2	
12	Proportionality principle	SR1.1, SR1.2, SR1.6		SR3.2, SR3.6, SR3.9				
13	Precautionary principle	SR1.1, SR1.2		SR3.2, SR3.6				SR7.8
14	Continuous protection			SR3.1, SR3.2, SR3.4, SR3.5			SR6.1, SR6.2	SR7.3, SR7.4, SR7.5, SR7.6
15	Secure Metadata management				SR4.1, SR4.2			SR7.3, SR7.4, SR7.6
16	Secure defaults	SR1.7	SR2.3, SR2.4		SR4.1, SR4.2			SR7.3, SR7.4, SR7.6, SR7.7
17	Trusted Components			SR3.2				

management), making any description based on SRs tedious. It should be noted that we will introduced the various technologies in a FR, which in our opinion is the most relevant for fulfilling this FR's Security Requirements.

We recommend that the procurement process for a cybersecurity solution requires, from the SuC supplier, a clause-by-clause analysis based on Table 6 of the TS 50701 standard. This should describe - for each of these FRs - the specific system security requirements. We also wish to highlight that the procurement team should consult Section 6 of the UITP Report "Wireless Networks and Cybersecurity", in which most of the following technologies are included and described in depth, along with their strengths and weaknesses.

FR1: IDENTIFICATION AND AUTHENTICATION CONTROL

Physical or virtual access control to OT/IT assets is obtained through a mix of technologies, which will identify and authenticate the person or system trying to gain access and will authorise that individual or device. TS 50701 identifies 12 principles that are affected by SRs (see Fig 12) for this FR. We will not describe all these SRs, but will indicate those technologies that we recommend using to meet them.

Network Access Control

A Network Access Control (NAC) provides network visibility and supports access management through policy enforcement on devices and users of the PTO's corporate networks. Through its access management capabilities, it can deny network access to non-compliant devices and their users, isolate these devices in a quarantined area, or give them only restricted access to computing resources. Other important functionalities include:

- **Lifecycle management:** Policy enforcement for all operating scenarios.
- **Visibility:** Recognition of users with their devices, avoiding damage from malicious code.
- **Guest access granting:** Management of guest registration and authentication through a guest management portal.
- **Security posture check:** Evaluation of security policy compliance according to specific criteria (for example, user type, assets or OS).
- **Incidence response:** Mitigation of network threats by enforcing security policies.

Most NAC technologies can integrate with other security and network solutions, which will help authenticate the users and their devices.

Simple Authentication apps

Simple application interfaces (for example, web servers, FTP servers, OPCs and remote desktop interfaces) can provide network access to human users. However, these apps could be supported by other external authentication solutions, including physical security measures in railways (for example fingerprint authentication for access control).

Multi-factor authentication

As its name suggests, multi-factor authentication (MFA) technologies combine verification technologies from at least two different groups or authentication factors. Increasingly common, three-factor authentication solutions consider using one mechanism from each of the following three methods:

- **Knowledge:** for example, password or PIN, security question or social login.
- **Possession:** for example, badge (SMS, Email, Hardware, or software) token, smartcard or smartphone.
- **Inherence:** fingerprints, iris or voice biometrics.

The objective of MFA is obviously to complicate access to the protected network by adding several steps with uncorrelated authentication mechanisms.

Certificate-based authentication

Certificate-based authentication is a cryptographic mechanism that identify users, machines or devices by using digital certificates. The user possesses a private key that is password protected (if the key is not located in a secure keystore). The public key cryptography verifies that this private key, used to sign certain information, corresponds to the public key in that certificate. The technology checks that the certificate has been correctly signed (for example, following the correct format) or will immediately be discarded. Additional requirements are that the signing public key must be found in a 'Trusted Certificates' store, and that the certificate, as well as the store, can be trusted for authentication purposes.

FR2: USE CONTROL

Cybersecurity Use Controls are the measures that a company deploys to enforce access authorisation into the SuC's network, following the check on the authentication request. TS 50701/IEC 62443-3-3 identifies six principles affecting this FR (see Figure 12). These are the leading issues associated with the implementation of the main technologies.

Access Control models

There are several ways of controlling access to a SuC networks. Railway and public transport operators should avoid granting access exclusively at the personal or file level. It should rather be granted on models that integrate the context in which a critical SuC is being used by the person or machine (for example general access via a personal password versus access to a specific file contained in a restricted area for a specific department function). Although there are four main types of control models, for important SuCs railways should specify that the network administration enables one of the two RBAC (Rule- or Role-Based Access Control) approaches. Each of the following models provides different levels of permissions and methods of assigning the access:

- **Discretionary access control:** Grants personnel complete control over any owned objects and any programmes associated with such objects. This is a basic capability desirable in all assets.
- **Role-based access control:** Provides access based on an individual's position in the PTO organisation. Access depends greatly on users being logged into a particular network or application so that their credentials can be verified.
- **Rule-based access control:** Grants or denies access to a user based on a set of dynamic rules and limitations defined by the owner or system administrator. Such rules may limit the access based on unique situations, such as the individual's location, the time of day or the type of device being used. Rule-based access may be applied to more broad and overreaching scenarios, such as allowing all traffic from specific IP addresses or during specific hours, rather than simply from specific user groups.
- **Mandatory access control:** Allows the system's owner to control and manage access, based on the settings laid out by the system's parameters, even for software and users with system-level privileges. This capability

is applied most commonly to software servers that run constantly and occasionally require system-level privileges. It prevents a compromised server from using system-level privileges indiscriminately.

In some situations, it may be necessary to apply both rule-based and role-based access controls simultaneously.

Access control enforcement: As insider malevolent acts account for a few of the OT attacks, such enforcement should not be undertaken by simple approval by an IT administrator, but rather require dual-approval mechanisms, particularly for special situations. Indeed, in railways access, override by supervisor is common to manually accept these special situations, which are documented in a legal way.

LAN (Local Area Network) and WAN (Wide Area Network)

As access control management with its two pillar - user authentication and access authorisation - is a key element of the DID strategy, organisations seek ways of extending the networks that are under their control. In other words, they will adopt technologies that transformed untrusted networks such as the internet or third-party vendors' intranet, in their "own network". That technology is often described as an "armure around the connection" which can only be penetrated from both endpoints. The word tunnel or tunnelling is often utilized for this kind of technology or process of going through this protected path. Over and above the concept of LAN and WAN, which we will now examine, we describe these tunnelling technologies in the section on data confidentiality, as they also play a crucial role in fighting eavesdropping.

The concept of LAN describes a group of connected computers and network devices, usually within the same building. As connections through several sites are nowadays more the rule than the exception, LANs have been extended to WANs.

Originally, WANs were mostly defined by specific protocols (at layers 1 and 2) but as they now are usually connected via ethernet, they generally describe a larger geographical area than a LAN, or a network connecting several LANs. These WANs may be accessible to the public (for example, the internet) or limited to an enterprise. In this latter case, a service provider will supply the operator with a private WAN that connects their various offices and sites. A WAN is usually highly secure, as it uses a physical cable that connects both end points, and the operator will retain the exclusive use of this WAN.

Operators are cautioned that using tunnelling technologies (even when encrypted) for highly sensitive safety-critical or reliability-critical networks that pass through the internet, is still high risk. Vulnerabilities and even zero-day vulnerabilities are found and exploited in tunnelling and other software routinely. Relying on tunnelling, firewall or other software alone to protect critical OT components from the internet is unwise.

Automated Audit Management software

Components and subsystems that log events locally should ensure the monitoring and logging information is transferred to a centrally managed system. Such software provides a unified view of active directory permissions, helping track changes and checking adherence to security policy. Such technology instantly detects data risks by flagging insecure accounts and misconfigured credentials. It provides drill-down reports to help detect suspicious user account access and activities.

Non-repudiation and Message Authentication code

Non-repudiation provides a proof of the origin, authenticity and integrity of data. It assures the sender that their message was delivered, as well as proof of the sender's identity to the recipient. This way, neither party can deny that a message was sent, received and processed.

Non-repudiation is achieved by cryptographical means such as digital signatures, and includes other services for authentication, auditing and logging. In online transactions, digital signatures ensure that a party cannot later deny having sent the information or the authenticity of its signature. A digital signature is created using a private key of an asymmetric key pair, which is a public key cryptography, verified with a corresponding public key.

In cryptography, a Message Authentication Code (MAC) is used to authenticate a message or confirm that the message came from the stated sender and was not changed along the way. Unlike digital signatures, MAC values are generated and verified using the same secret key, which the sender and recipient must agree on before initiating communication.

Non-repudiation is a common requirement for e-commerce applications with business partners, as well as for the most sensitive engineering configurations or other changes to deployed systems.

FR3: SYSTEM INTEGRITY

It is essential that an SuC's mandated operational and technical parameters are within the prescribed limits and that all its intended functionalities are unimpaired and free from deliberate or inadvertent unauthorised manipulation of the SuC. Therefore, solutions that protect an SuC's integrity should ensure logical reliability of the operating system and completeness of the hardware /

software that implement the protection mechanisms, as well as communication and data integrity.

TS 50701 identifies 13 principles relevant for this FR (see Fig 12) associated with the SRs. Once access authentication and authorisation have been verified, the following issues must be considered and the recommended technologies implemented.

Protection against malicious code

The integrity of a system is undermined by malware that will create different types of attacks, as described below:

Figure 13: example of main malwares with their likely impact

Malware	What does it do?
Virus	Modifies other legitimate host files in such a way that when a victim's file is run, the virus is also executed.
Ransomware	Disables the victim's access to data until the ransom is paid.
Fileless malware	Makes changes to files that are native to the OS.
Spyware	Collects user activity data without their knowledge.
Adware	Serves unwanted advertisements.
Trojans	Disguises itself as desirable code. Remote Access Trojans (RATs) includes a back door for administrative control over the target device
Worms	Spreads through a network by replicating itself
Rootkits	Provides attackers with an unprivileged access to a system, granting them unlimited privilege, so that they can do anything they want to the machine.
Keyloggers	Monitors and/or records users' keystrokes.
Bots	Launches a broad flood of attacks.
Mobile malware	Infects mobile devices.

Nowadays, most malwares are a combination of traditional malicious programmes, often including parts of trojans, worms and viruses. They usually initiate as a trojan, but once executed attack other victims over the network like a worm.

Several technologies are designed to detect the source code of these malware. These identify a bit sequence or execution command that has already been associated with a previous attack and already exposed by the industry. These features are usually identified from a Common Vulnerability and Exposure (CVE) system, which provides a reference method for publicly known information-security vulnerabilities.

Figure 14: Example of CVE 2021-37181

CVE ID	CWE ID	# of Exploits	Vulner. Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf	Integ	Avail
CVE-2021-37181	502		Exec Code	2021-09-14	2021-09-24	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

A vulnerability has been identified in Cerberus DMS V4.0 (all versions), Cerberus DMS V4.1 (all versions), Cerberus DMS V4.2 (all versions), Cerberus DMS V5.0 (all versions < v5.0 QU1), Desigo CC Compact V4.0 (all versions), Desigo CC Compact V4.1 (all versions), Desigo CC Compact V4.2 (all versions), Desigo CC Compact V5.0 (all versions < V5.0 QU1), Desigo CC V4.0 (all versions), Desigo CC V4.1 (all versions), Desigo CC V4.2 (all versions), Desigo CC V5.0 (all versions < V5.0 QU1). The application deserialises untrusted data without sufficient validations, which could result in an arbitrary deserialisation. This could allow an unauthenticated attacker to execute code in the affected system. The CCOM communication component used for Windows App / Click-Once and IE Web / XBAP client connectivity are affected by the vulnerability.

Whitelisting technologies

To protect an SuC against malware, TS 50701 specifies the use of a secure boot mechanism and an executable file-based whitelisting application. The objective is to manage untrusted code at the operating system/firmware and application layers, ensuring that only authorised software is permitted to be executed. Inspection of suspicious code should be performed at the entry and exit points.

More generally, whitelisting technologies explicitly permit some identified sources to access a particular privilege, service, mobility or recognition, allowing specific actions and denying all the others by default. For instance, spam filters often include the ability to 'whitelist' certain sender IP addresses, email addresses or domain names to protect email from being rejected or sent to a junk mail folder.

In NAC systems, LAN or MAC address whitelisting are frequently used mechanisms, filtering data at the OSI level 2 stack. Firewall whitelisting works at OSI levels 3 and 4. Application whitelisting, which works at level 7, is used to permit only some application-level operations, but not others. An example of application-level whitelisting in the IT realm is a firewall rule that permits users to log into Facebook, consume content, update their status, but does not allow users to upload images.

Sandboxing technologies

Sandboxing technologies can also protect railway and public transport assets from suspicious code. A sandbox is a separate system that runs unchecked software or opens unchecked documents in standard software packages, such as Microsoft Word or Adobe PDF Reader. Such cybersecurity practice allows you to run code and open documents, observe and analyse the suspect content in a secure, isolated network that mimics the users operating environments. Hence, sandboxing prevents many kinds of malware from entering the network and is frequently used to inspect an untested or untrusted code. By keeping content under test to a restricted environment, sandboxing ensures that the software or file cannot infect or cause damage to the host machine or operating system.

Another benefit of sandboxing technology is that it allows testing of malicious code in an isolated environment to understand how it works, often aiding future detection of similar malware attacks.

Vulnerability scanners

These search for, and report on, known vulnerabilities present in an organisation's IT/OT infrastructure. There are several types of scanners, based on the location of the scan - network, host, wireless, application, web application and database-based scanners. These scanners don't necessarily look at malware codes but may test for unsecure server configuration, cross-site scripting or unexpected injections (for example, SQL and command injection). Many commercial and open-source vulnerability scanners are available with their own strengths and weaknesses.

Anti-malware software

This software is designed to detect and remove malware, particularly viruses and are installed on end devices or servers. Running in the background, they periodically scan a device's directories and files for malicious patterns and code. They tap into a database of virus definitions and signatures - usually from the CVE - to check if there are comparable executable malicious codes. When there is a match, it blocks or quarantines the files. As new malware pops up almost every day, anti-malware vendors must update their database frequently.

End-point solutions

Such solutions are deployed and operated directly on endpoints, often integrating antivirus, whitelisting, host firewalls, permissions management and other protections. Endpoint security products often serve as the last line of defence against attacks seeking to compromise end devices whenever network security tools have failed to find, block and alert on threats reaching this endpoint. These platforms offer more holistic protection for networks and devices than anti-malware, by incorporating features that help filter web traffic, detect threats, remotely control and monitor devices. Newer technologies called Endpoint Detection and Response (EDRs) tools have gained popularity. Rather than solely looking for threat signatures, EDRs also monitor device behaviour over time and alerts administrators when the device deviates from baseline normal behaviour.

The major advantage of endpoint solutions over network security protection is that they are installed directly on the endpoint and follow the devices wherever they go. As an increasing number of people are working remotely, endpoint security becomes increasingly important. For OT environments, network protection makes more sense, particularly since much purpose-built hardware (for example, IoT) and OS devices may be incompatible with end-point solutions. Furthermore, in safety critical environments, such solution cannot easily be deployed (for example, lagging, patching, update and safety-case issues).

Network firewalls

Endpoint security and network firewalls both provide a degree of malware protection. However, while endpoint security performs other tasks such as patching, logging and monitoring, firewalls are mainly responsible for filtering the traffic flowing into and out of a network, based on a set of security rules applied according to network segmentation criteria (see FR5: Restricted dataflow). Firewalls provides visibility for these traffic flows and the ability to block any traffic that violates these predefined security policies.

There are three types of network firewalls:

Host firewall: firewall software running on a computer or other device tasked with protecting only the device the software runs on – the 'host'.

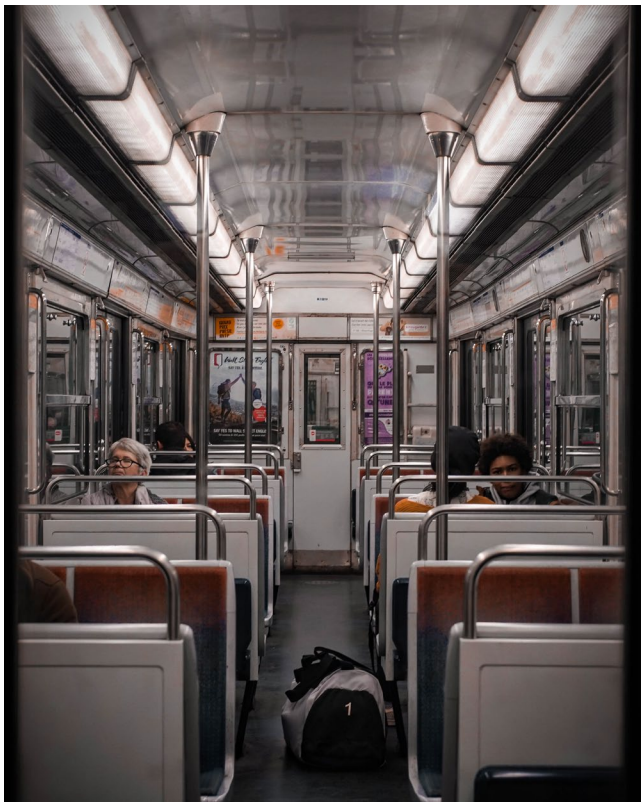
Network firewall: firewall software running on a device, such as a network appliance, or even on a virtual machine, tasked with filtering the flow of traffic between two networks.

Cloud Firewalls: Virtual network firewall appliances, specifically designed to be deployed in the cloud. These may be available as either standalone virtual machines or as an SaaS offering.

Modern firewalls often provide additional functions to basic network traffic filtering. Modern firewalls may include in-line anti-virus scanners searching for malware in file transfer streams, in-line network intrusion detection scanners looking for attack signatures or network traffic anomalies, as well as virtual private networks (VPNs), two-factor VPN authentication and many other functions.

Next Generation firewalls

Next Generation firewalls (NGFWs) generally include several additional functionalities. These include application awareness and control, intrusion prevention, SSL inspection, deep-packet inspection, reputation-based malware detection and cloud-delivered threat intelligence. Even although NGFWs and EDRs typically take



a more application-centric approach to traffic classification, they struggle to detect the new breed of advanced attacks such as zero-day, targeted attacks or advanced persistent threat (APT) attacks. However, some NGFWs - called Layer 7 - may provide some protection against application-layer DDoS attacks, which are usually carried on HTTP traffic. All things considered, NGFWs are efficient tools for an IT environment but are generally much more limited in their understanding for, and protection of, OT-centric protocols.

Intrusion Detection Systems and Intrusion Protection Systems

An Intrusion Detection System (IDS) is an automated system that detects attacks in progress. As we have seen, firewalls limit access between networks to prevent intrusion, but no firewall is perfect, and attacks from insiders and other scenarios may originate inside of protected networks. External IDS generally receive a copy of some or all traffic in part of a network. The system will then evaluate that traffic against a database of attack signatures, look for traffic anomalies and/or use other criteria to detect intrusions. When a potential intrusion is detected, the IDS reports one or more alarms, typically to a SIEM.

Inline or pass-through IDS capabilities are built into some firewall offerings. Passive IDS technology most commonly receives a copy of network packets through an ethernet TAP or a mirror port on a managed switch. In these scenarios, the network connection receiving the packets does not have an IP address, and thus to a large extent is 'invisible' to the network being monitored.

An Intrusion Prevention System (IPS) is an IDS that - when it detects an attack in progress -has the option of interrupting it. An inline IPS, such as one built into a firewall, can simply drop the packet or packets that constitute the attack in progress. A passive IPS must generally send messages, such as TCP RESET packets, back through mirror ports or otherwise into the monitored network to interrupt the attacks.

FR4: DATA CONFIDENTIALITY

Data confidentiality is about protecting data against unintentional, unlawful, or unauthorised access, disclosure or theft. It concerns privacy of information, including authorisations to view, share and use. Several measures already presented can be taken to assist with confidentiality, such as secure access control enforcement (for example, through multifactor authentication), strong passwords policies, segregation of data and assigning users appropriate user privilege levels. Encryption is another approach that we will present in this section.

TS 50701 identifies eight principles affected by this FR (see Fig 12). The following technologies should be considered.

Virtual Private Network

A Virtual Private Network (VPN) is theoretically the same as a LAN, but uses the internet or any other public network to allow people to remotely connect to their network. Hence, it creates a 'virtual' private, encrypted connection from a host on a public network (for example, the internet) or private (subgroups connected to a WAN). MPLS VPNs constitute such private WANs, built upon a service providers network. The service provider ensures that the endpoints never communicate with another entity's endpoints. Furthermore, an IPsec

VPN encrypts the connection, prohibiting potential hackers to eavesdrop on the transmission. It prevents the ISP or employer from spying on the traffic and the work being done online by its employees and can also provide authentication functionality to the endpoints.

Proxy Servers

A proxy server is simply a computer with its own IP address; its role is to take the request from the sender's device and transmit it to the internet resource on behalf of the sender's computer. The feedback is then channelled back to this device via the proxy server. Hence the sender's request remains anonymous, as the computer's IP address is masked, allowing misdirection. Proxy servers can also carry out other functions, most commonly caching web requests and responses to minimise network traffic.

Web Servers

A web server is a computer that stores web server software and a website's component files. The most basic web server is called an HTTP server. This uses software that understands URLs (such as web addresses) and hypertext protocol, to provide content and other services to the browsers used to view webpages. HTTP servers communicate in plain text and these are comparatively easy to hijack. PTOs should procure HTTPS servers. HTPPS is a version of the HTTP protocol, encrypted with the TLNS protocol that uses encryption, digital certificates and other handshakes. This provides much more effective protection against eavesdroppers and tampering.

Encryption technologies

TS 50701 suggests that the SuC supplier should document the practices and procedures for cryptographic key establishment and management. The railway application should use established and tested encryption and makes direct reference to the advanced encryption standard.

Data encryption is the process of converting data from a readable format - understandable to humans or machines - into scrambled information (called ciphertext) which in theory is incomprehensible without the encryption keys to reconvert it into readable format. The role of encryption is twofold. It discourages and impedes the possibility of understanding the content when eavesdropping. It also makes session hijacking more difficult – an attack where a third party seeks to insert commands into a connection established between two legitimate parties.

There are basically two types of encryption techniques.

Symmetric Encryption Method: This uses the principle of a private key that both the sender and receiver have access to. This works best for closed systems, which have less risk of third-party intrusion.

Asymmetric Encryption Method: This uses the principle of two keys (one public and the other private), which are mathematically linked. The user employs one key for encryption and the other for decryption. Both keys are simply large numbers that aren't identical but are paired with each other in an asymmetric way. Although slower to execute than symmetric encryption, these methods tend to be safer due to digital signature authentication and the increased security linked to the privacy of the decryption keys.

In both systems, key distribution is a problem that designer and vendors must address. In symmetric encryption, there must be a way to distribute and authenticate legitimate keys to communicating components so that they can decrypt each other's messages. Asymmetric encryption generally uses the Public Key Infrastructure (PKI) to issue certificates to authenticate servers to clients. PKI is a good fit for the open internet, where there are many clients and a much smaller number of servers with reliable access to well-known certificate authorities. PKI is a harder fit for OT networks, where every PLC can be considered a server requiring a certificate, where organisations may not have the skills to manage a secure certificate authority and where connections to IT networks or the internet to leverage external certificate authorities is an unacceptable security risk.

Advanced Encryption Standard (AES): This is based on a 128-bit symmetric encryption algorithm (256-bit also exists for demanding environments). It is currently considered invulnerable to all Man-in-the-Middle (MiM) attacks, except for brute force (and obviously if hackers gain access to an unsafely stored secret key). However, encryption standards 'age' as mathematicians continue to study them and discover new weaknesses. Owners and operators should plan to eventually replace AESs

with more robust algorithms and software if and when AES is sufficiently weakened over time.

Hashing technologies

TS 50701 also recommends using hashing technologies. Hashing uses encryption but is very different than the encryption method described earlier. Hashing techniques basically translate information about a file into a key (fixed-size bit string code). This string code can be considered a generated unique signature, which is mathematically designed to be practically impossible to decipher or to reverse back to its original form. In fact, with good hashing algorithms, any minor change to the information is easily trackable, making cryptographically signed hashing a great technique for detecting if a message has been tampered with.

In PTO environments, hashing is often used to verify the integrity of a file after it has been transferred from one place to another, typically using file backup programmes (for example, SyncBack, Acronis, MSP360 and other online backup solutions). To ensure the transferred file is not corrupted, a user can compare the hash value of both files. If they are the same, then the transferred file is an identical copy. Hashing techniques are also used to compare whether two files are equal, without opening the files. Signed hashes can be used to assert that an authority of some sort has vouched for the legitimacy of the file.

There are many hashing technologies, but the most commonly used for file integrity checks are MD5 (broken and should no longer be used) and SHA-2 (a newer version developed by the US National Security Agency). CRC32 is technically a hash function, and is widely used to detect accidental changes. However, it is not strong enough to resist deliberate attacks.

Data loss prevention software

Data loss prevention is a strategy for making sure that sensitive information does not leave the corporate network. It describes any solution or process that identifies and tracks the journey of sensitive data or enforces policies to prevent unauthorised or accidental disclosure. Data loss prevention software detects potential data breaches / data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in use, in motion and at rest.

FR5: RESTRICTED DATAFLOW

Restricted data flow: TS 50701 specifies that *"Operational networks should be segmented to limit the consequences of a successful attack on one part of the network, impeding access to other parts."* The standard imposes independence from non-controlled networks, promoting the creation of closed networks. The separation of operations networks from internet-exposed business networks is particularly important, as a widespread and powerful attack technique is to compromise hosts first on IT networks, and then pivot from there through those compromised hosts into more consequential operations.

Closed network: A railway or public transport operation network should be designed to prohibit access to or from the operational network. TS 50701 indicates that *"if data needs to be sent from within the operational network, a data diode (allowing only unidirectional data flow) should be used. Such a device prevents access to the operational network from the outside, but still allows the sending of data outside to the external network. This allows for remote diagnosis, export of data to cloud systems and external intrusion detection analysis. If bidirectional data flow is required between the operational network and an external network, a demilitarised zone (DMZ) is required."*

If physical separation through a closed network isn't technically feasible, a logical segregation is acceptable, strictly associated with a series of SRs (SR 1.2, SR 1.5, SR 1.8, SR 1.9, SR 3.1, SR 3.7, SR 4.1 and SR 6.2). In both cases, this physical and logical isolation must be designed according to the criticality of a railway application, which is determined by the detailed risk assessment. Furthermore, this segmentation must be based on an in-depth analysis of the existing network and its data flows between installed assets. A communication matrix showing the routing restrictions should be created.

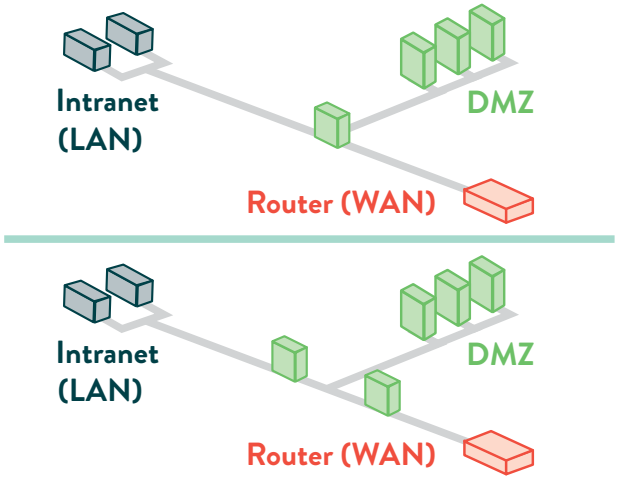
TS 50701 identifies three principles affected by the SRs for this FR (see Fig 12). The following network architecture and the technologies associated with their implementation are described in this section.

Demilitarised zones

A Demilitarised Zone (DMZ) is a physical or logical subnetwork that contains and exposes a network's external-facing services to an untrusted, usually larger, network exposing operations servers to a business or IT network. A DMZ can be visualised as an intermediate network, which communicates with both the IT and OT networks while sitting between the two. Its purpose is to add an additional layer of security to the more sensitive network. When implemented correctly, an external network node cannot access any protected OT host directly, while external hosts and users can access only those hosts and services exposed in the DMZ.

There are many ways to design a DMZ network. Figure 15 describes two of the most basic DMZ architectures. In the first IT network configuration (called a three-legged model) where networks are separated by one firewall. In the second somewhat stronger configuration (called a back-to-back model) there are two application-level firewalls, with at least one hardened server that terminates the data transfer between two networks (called a bastion host). Transmission restriction from the DMZ should be based on 'deny all' principles (address ranges, protocols, or commands). No TCP or other connection should be allowed to pass through the firewalls from the IT network into the OT network or vice-versa.

Figure 15: Description of back-to-back (2 firewalls) and three-legged (1 firewall) DMZ models



Data diode

A true data diode is a network communication device that is physically able to send information in only one direction. A data diode maintains a physical and electrical separation between source and destination networks, and provides the greatest benefit when the hardware is oriented to transmit information from a higher-criticality to a lower-criticality network.

Physical segmentation: The highest quality data diodes use optical separation: a device or circuit board in the source network that has a fibreoptic transmitter but no receiver; a receiving device or circuit board that has a fibreoptic receiver but no transmitter, and a short fibreoptic cable which connects the two components. The receiving network is physically unable to send any signal through the diode into the source network. When deployed as the sole online connection between two networks, the receiving network is unable to send any attack information or other information into the source network through online means.

Data diodes tend to be hardware-intensive, with little or no software support. A data diode connecting two network switches, for example, is able to send only ethernet broadcast frames from one switch to the other, which means the only internet protocol packets able to be communicated from one network to the other are UDP/IP packets.

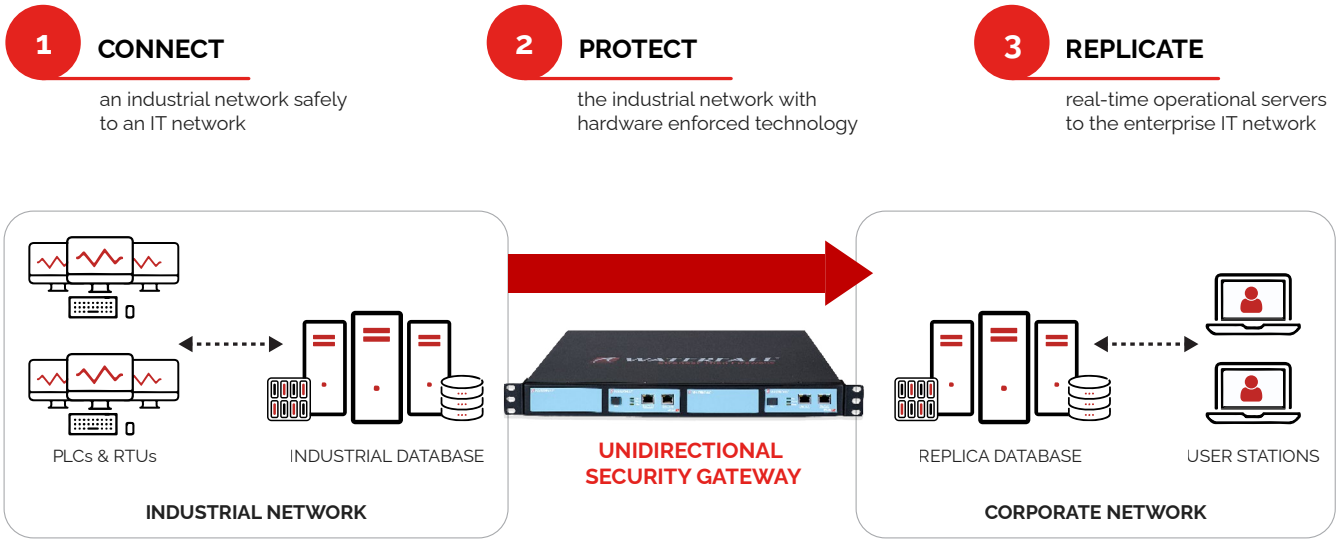
Unidirectional Gateway

Unidirectional gateways are a combination of hardware and software. Like a data diode, the hardware is also physically able to transmit information only in one direction, while the software makes copies of servers and emulates devices in real-time.

The highest quality unidirectional gateways integrate multiple layers of unidirectionality in their hardware and software design (for example, internal electrical and optical isolation; software doing low-level unidirectional control; circuit boards using gate array logic (i.e., general purpose integrated circuit that can be wired up) not a CPUs); separate power supplies and appliances).

Server replication and device emulation: Unidirectional gateway software connects to data sources on the source network, such as Programmable Logic Controllers (PLCs), OPC servers and historian or SQL database servers. The software logs into the data source and requests all recent data. The software converts the data into formats and protocols suitable for transmitting through the unidirectional hardware and transmits the snapshot of data and state information. The receiving unidirectional software most often logs into an identical server on the external network, and then inserts the latest data update into that server. External users and applications use the data in the replica server rather than send queries, or possibly attacks, into the source network. As well as providing an inviolable physical barrier, unidirectional vendors provide software connectors that replicate specific environments. For example, some connectors available from commercial off-the-shelf providers include:

Figure 16: How Unidirectional gateway work; Source Waterfall



- Historians and databases from a variety of vendors (for example, AVEVA, GE, Schneider Electric, Rockwell, Microsoft and Oracle).
- File transfer (for example, FTP/S, SFTP, TFTP, SMB, CIFS, NFS, HTTPFS, as well as Folder and log mirroring).
- Industrial applications and protocols (for example, Siemens, Modbus, OPC DA, OPC HDA and OPC UA).
- Enterprise monitoring (for example, SIEM from Splunk, ArcSight, Q-Radar and Thales Aramis).
- Anti-virus signature updaters.

Physical or Logical segmentation?

TS 50701 defines a framework in which communication flow is tolerated or prohibited according to the criticality of the SuC. As mentioned previously, this criticality is measured by the risk and vulnerability assessment. The following table describes this flow for communication between wayside assets in standard operational usage, enabling temporary connection for remote maintenance conditions:

In this table, the signs '+' is for data flow allowed in both directions, '-' for prohibited dataflow and 'R' for restricted dataflow to read-mode only, through appropriate technical solutions (for example, a data diode). As indicated in the table, pairs of zones with significantly different criticality and marked with a '-' must not be allowed to communicate either directly or via firewalled connections. Direct connections between such networks are permitted only via true data diodes or hardware-enforced unidirectional gateways.

Cyber-sabotage attacks are, and will always be, information-based. Hence, physically blocking the flow of attacks and other information from one network to another means controlling both the current flow of attacks and all future such attacks. This is a important feature of unidirectional protection in designs expected to be deployed and operated essentially unchanged for up to decades in a rapidly evolving threat environment. This future-proof capability is not true of firewalls, nor of any software-based approach to network segmentation, as malware and attack techniques are constantly evolving, and new zero-day vulnerabilities are constantly being discovered and exploited.

Other limitations of firewalls include complex configurations that are subject to errors and omissions that weaken firewall protections. This is particularly the case in networks containing large numbers of assets, as those networks evolve slowly over time, as well as susceptibility to different forms of tunnelling attacks (for example, DNS tunnelling). Modern attacks, such as ransomware, which impact thousands of enterprise IT networks every year, are evidence of this. All these hacked enterprises had a firewall between the IT network and the internet, which means that every one of those thousands of ransomware attacks penetrated the firewall in the course of compromising the IT network. However, despite these limitations, firewalls are still effective tools for so-called 'horizontal' network segmentation – providing a degree of separation between networks at matching safety or reliability-criticality levels.

A continuous monitoring system can augment, but cannot replace, network segmentation. Unlike firewalls, monitoring systems apply rules and policies according to

Figure 17: Table F5 from TS 50701: Communication matrix landside to landside

Zone criticallity and communication matrix • landside - landsite									
Zone criticallity landsite (ZV-L)	**Security Maturity**	**Example**	**ZC-L 5s**	**ZC-L 5**	**ZC-L 4**	**ZC-L 3**	**ZC-L 2**	**ZC-L 1**	**ZC-L 0**
ZC-L 5s	Highly secure/safety	Safety: interlocking, high voltage	+	R	-	-	-	-	-
ZC-L 5	Highly secure/critical	SCADA, central ICS	+	+	R	-	-	-	-
ZC-L 4	Secure.	Data centre, internal DMZ, ICS/automation	-	+	+	+	-	-	-
ZC-L 3	Medium	Internal network, office and business network	-	-	+	+	+	+	-
ZC-L 2	Low	Gateway area, external DMZ	-	-	-	+	+	-	+
ZC-L 1	Low	External partner/ companies	-	-	-	+	-	+	-
ZC-L 0	Untrusted	Internet	-	-	-	-	+	+	+

zones and conduits. Also unlike firewalls, policies do not need to be applied for each asset, but rather at the group level (in other words, all the assets pertaining to a zone or conduit). These rules can be easily applied at each protocol layer and communication can be flagged as permitted (or not) in both unidirectional and bidirectional flows. Continuous monitoring systems cannot block messages in the way that firewalls and unidirectional gateways can; rather these systems flag prohibited communication and alert appropriate personnel. This means that truly passive monitoring systems can often be used to monitor traffic into, out of and within safety-critical systems.

When segmenting an SuC's network segments, zones and conduits, one should consider the following applicable TS 50701 partitioning criteria:

- Worst-case consequences of compromise
- Risk to information, in terms of integrity, availability and confidentiality
- Type of interfaces or connection to the other parts of the SuC (for example, wireless)
- Physical or logical location
- Access requirements
- Operational functions
- Organisational responsibilities for each asset
- Safety aspects
- Technology lifecycles, for example, product lifecycle and/or obsolescence.

FR6: TIME RESPONSE TO EVENTS

All log access should be monitored and auditable. All components and data used to enforce the security policy should have uninterrupted protection consistent with the security policy and the security architecture assumptions.

TS 50701 defines six principles that are affected by the SRs for this FR (see Figure 12).

While no log monitoring or combination of monitoring solutions can be guaranteed to detect all attacks in progress, these solutions do provide a valuable type of situational awareness. This section present cybersecurity technologies that enable log access monitoring and the support incident response in the event of malevolent acts, as well as the physical regrouping of the cybersecurity experts using these technologies

Security Information and Event Management System

A Security Information and Event Management (SIEM) system is software that aggregates and correlates data from multiple sources, identifying suspicious patterns of activity, alerting security analysts to those patterns and prioritising those alerts likely to indicate the most consequential attacks. Generally, a SIEM incorporates, at minimum, a high-speed data store and a correlation engine using rules, statistical correlations and other means to establish relationships between alerts, events, logs and other data. Frequently, a SIEM hierarchically deploys multiple collection agents, responsible for gathering security-related events from user devices, servers and

network equipment as well as specialised security equipment such as firewalls, IDS/IPS, Continuous Monitoring Systems. These agents collect, aggregate, summarise and forward relevant data to a centralised management console, where security analysts 'connect the dots' and decide on what to do next.

TS 50701 emphasises that ***"Malware and malicious code protection should be centrally managed for integrity and consistency in railways. SIEM protection is largely a dynamic anomaly detection/protection mechanism and may prove inadequate for malicious code protection."*** Hence a SIEM requires other cybersecurity technologies such as firewalls, IDS/IPS and continuous monitoring systems to understand the cyber posture in real time.

Network Intrusion Detection System

A network intrusion detection system monitors network communications and alerts keyholders to suspicious activity. Intrusion detection systems may be signature-based, anomaly-based or both. Signature-based systems use databases of known attack patterns and raise alarms when network packets match these. Anomaly-based systems use various means to characterise 'normal' connections and alert when any other communications are detected. What is deemed 'normal' can be determined in many ways, including:

- A database of rules describing what kinds of communications are normal.
- Observing, sometimes called 'learning', what is assumed to be normal network traffic for a period of time and matching future communications against that baseline.
- Looking at which devices are routinely communicating with others and the nature and volume of such communications.
- Looking at aggregate traffic types and volumes.

Intrusion detection systems may be active or passive. Active systems from time to time interact with monitored networks and hosts by sending messages or queries into those networks. Passive systems analyse only copies of network messages received from SPAN, mirror or tap ports, and in normal operation send no messages into monitored networks. Therefore, passive systems are often appropriate for monitoring safety-critical network communications.

Note however that many SPAN, mirror ports and taps are either bidirectional or can be configured or compromised to become bidirectional by an attacker. Hardware-enforced unidirectional communications such as a data diode or unidirectional gateway provide stronger assurances of passive monitoring for networks.

OCC / SOCC

The capacity to react quickly to an incident depends heavily on receiving important and relevant information to support the decision-making process. It also relies on having qualified and trained decision makers available to understand the alerts and act accordingly, using tools and other incident responders available to implement the decisions.

Operational Control Centres (OCC) are physical rooms where most IT/OT critical systems are visualised through appropriate General User Interface (GUI) and staffed with the appropriate subject matter experts to operate a

transportation system. In PTO environments, they tend to be centralised in a secured facility.

Security Operational Control Centres (SOCC) are also physical rooms, which can be included within the OCC or separated, focused on security matters. Typically in such a room, security specialists assisted by a SIEM and a continuous monitoring system will have a 360° view of all assets, disposing of the necessary tools to clarify the context in which an incident has occurred. They will also have access to the controls that allow the implementation of mitigation measures.

Continuous Monitoring System

As already introduced, a continuous monitoring system enables the efficient management of all assets. This technology lies at the heart of any OT cybersecurity strategy, as it offers broad visibility, 24/7, into all of the PTO's thousands of digital assets - across all devices, endpoints and environments. As required by TS 50701, it offers a complete visibility into the PTO network, from the SuC's topology to the granular level of each asset. This in-depth view eliminates blind spots, reveals asset connections and classifies redundant assets. When network monitoring is performed through a span port or a tap, and provided it is guaranteed that no message or other signal can enter the switch through the SPAN/mirror port or tap, the monitoring system will not interfere with the dataflow. This means that this class of solution can be applied within safety-critical networks without having to redo the entire safety case, a costly and time consuming process.

Railway specific monitoring systems should rely not only on the main databases of CVEs that are generally tuned to IT malwares, but should also capitalise on identified, railway specific vulnerabilities. Furthermore, these monitoring systems dynamically scan the network for malware signature and - using market intelligence - detect new members of an already-known virus 'family' by associating evolved strings with patterns of the original virus.

The most advanced OT solutions integrate rules-based detection, recognising some zero-day attacks that wouldn't obviously be part of any CVE or market intelligence report through network abnormal behaviours. When using Deep-Packet-Inspection (DPI) technology, these solutions understand railway business logic and protect against many semantic attacks, that is, malware hidden within the application layers (for example, CBTC's RaSTA protocol), which may impact the safety of the railway network.

These advanced solutions integrate a quick escalation of cyber threats for decision-making. They provide an effective response and forensics insights directly in their user interface or via a SIEM. They also integrate analytic tools that retrieve data on an attack to establish its root cause.

Network Operational Centre

The Network Operational Centre (NOC) is a centralised place from which the IT/OT PTO administrators supervise, monitor and maintain a telecommunication network. It provides visualisations of the railway's fixed and wireless networks being monitored. The NOC acts as a nervous system, managing and optimising business-critical tasks such as network troubleshooting, software distribution and updating, router and domain name management, performance monitoring and coordination with affiliated networks.

SOAR

SOAR (security orchestration, automation and response) is software that deals with threat and vulnerability management, incident response and security operations automation. The security automation process executes cyber tasks - such as scanning for vulnerabilities or searching for logs - without human intervention. The orchestration refers to the ability to define, supervise and execute workflows, primarily for potential incident investigations and incident response processes. This orchestration enables the streamline of security processes and powers the security automation.

FR7: RESOURCE AVAILABILITY

This FR deals with the actions required when an asset or a network is made unavailable by an unintentional (for example, power shortage, malfunction) or intentional (for example, Denial-of-Service attack) incident. This FR is more process oriented than technology driven.

TS 50701 identifies 11 principles affected by the SRs, broken down according to the associated required functionalities.

Under a DDoS attack, and when normal operation is impossible, the SuC should revert to a degraded mode where essential safety and local control functions are maintained. In such an event, any effects should comply with applicable failsafe principles. The means provided to ensure operation of the node in the event of a DDoS attack should be implemented and described in manufacturer documentation. The SuC should manage resources in a way that prevents lower-priority processes (for example, network scans) from interfering with higher-priority processes (for example, control, monitoring and alarm functions).

The SuC should support system-level backup operations. This ability to conduct backups - specifically the critical information and files - should be supported by railway application. In view of the safety critical nature, railway and public transport operations must have strict policies on recovery and reconstitution to ensure a safe state in addition to a secure state. In today's era of ransomware, offline backups are particularly important. If a ransomware attack encrypts both important systems and their backups, then recovery becomes extremely difficult, with downtime extending to weeks or even months.

Upon restoration of power following a switch-off or power failure, components should start/boot, ready for the intended operation, without any loss of configuration (in other words, the previous configuration should be retained). The SuC should be able to generate a machine-readable report - or export its configuration to a file - with its current security settings. Applications or components serving essential and important functions should be able to prevent installation, enabling and use of unnecessary or irrelevant functions, ports, protocols and/or services. It should be possible to identify the SuC's hardware and software type and version. This includes version/revision of configurable elements.

CONCLUSION

This document provides a general framework to help public transport and railway operators integrate cybersecurity requirements into a tender process, whenever the SuC to be purchased can be considered OT related. The process should start by clearly differentiating IT and OT systems and continue by choosing the relevant frameworks and standards relevant for the OT segment. The TS-50701 is, as of today, the most comprehensive and detailed guideline for cybersecurity in railways systems, as it is derived from the IEC 62443 family of standards, with added considerations for extended security levels and safety. This White Paper evaluated some of the relevant FRs and the associated technology requirements. This document also contains the following information to aid in the process:

- *A quick reference guide for cybersecurity procurement,*
- *An example of the procurement of PIS/AVSL for a bus operation,*
- *An example of the procurement of an OT SuC: signalling system for a metro operation.*
- *A survey report for procurement in cybersecurity.*
- *A glossary with acronyms.*

It also includes the results of a survey completed by PTOs of the UITP security committee.

REFERENCES

An Acid Test for Europeanisation: Public Cyber Security Procurement in the European Union, Jukka Ruohonen1 Received: 22 May 2019 / Accepted: 28 September 2019 / Published online: 5 October 2019.

TED website https://ted.europa.eu/udl?uri=TED:NOTICE:567971-2019:TEXT:SL:HTML&tabId=1; Norway-Oslo: Railway traffic control software development services; 2019/S 231-567971; Contract notice – utilities; Services.

Security PHA Review, by Edward Marzal and Jim McGlone, ISA, 2020, ISBN 1643311174.

Secure Operations Technology, by Andrew Ginter, Abterra Technologies Inc., 2018, ISBN 978-0-9952984-2-2.

Critical Phases in the Process of Awarding Public Procurement Contracts: A Romania Case, Mirela Patraș, Cristian-Silviu Banacu; 31 July 2016.

Obsolescence on operational environment and cybersecurity, UITP report (UITP MyLibrary)

QUICK REFERENCE GUIDE FOR CYBERSECURITY PROCUREMENT

DEFINE IF THE SYSTEM IS AN OT OR IT SYSTEM

- Evaluate whether the SuC is classified as an IT or OT system.
  - OT and IT systems require different standards and compliance requirements.
  - They require different protection measures and evaluation processes.
- If deemed as an IT system, follow the standard procurement process and cybersecurity requirements for IT systems.
  - The procurements process should follow the requirements of documents such as ISO 27001.
- If deemed as an OT system, follow TS 50701 with the help of this white paper
  - Define the necessary Critical Level of the SuC, which is derived from the consequences of a successful cyberattack to the SuC.

SELECT APPROPRIATE LEGAL FRAMEWORK, CERTIFICATION AND STANDARDS

- Ensure all RFPs are supported by a legal framework relevant for the SuC being procured.
  - Three different types of legal constraints apply to any tendering process; the national tender regulations, national cybersecurity authorities and the specific national regulations applying to cybersecurity.
  - Check whether the SuC should seek approval or a security certification from any of these agencies.
- Standards can be regrouped under the following categories: Specific to the SuC, specific to the railway, specific to operation and specific to cybersecurity.
  - Standards provide guidance and should be selected before writing requirements.
  - To avoid overwhelming the scope, only choose relevant standards.
  - Standards are limited in scope, and thus should be viewed as a minimum set of requirements.
- If specifying cybersecurity standards different from TS 50701, ensure they are consistent with the following Safety standard, particularly when applied to SuC relating to a safety-critical system: EN 50126, EN 50128 and EN 50129.
  - In some cases, a cybersecurity requirement should be stated as a safety clause.
- IEC 62443 is today considered the worldwide standard for cybersecurity, particularly in the OT world. It is applicable to all Industrial Control Systems (ICS), including railway and passenger transport operations.
  - IEC 62443 defines security levels (1-4) widely used in a range of industries; however, it may be too horizontal and limiting for rail.
  - IEC 62443 is a cross-industry standard, and minimally compliant security levels may not be suitable for safety-critical systems.
  - IEC 62443 is divided in different sections for process and system requirements.
- TS 50701 should be considered as the main guideline for the cybersecurity process in tendering for European railways.
  - While still not a standard but a technical specification, it is the most comprehensive guide, focused on railway cybersecurity.
  - TS 50701 is based on IEC 62443 and on railways standards such as EN50126.
  - Signalling and control systems have defined security levels in TS 50701.
- Vendors should be certified under ISO 27000 and/or ISO 27001.
- The UITP guideline 'Obsolescence on Operational Environment and Cybersecurity' should be consulted to guide the process of ageing products.

DEFINE THE SECURITY REQUIREMENTS

- Assign a member of the OT/IT security team in the organisation to support the procurement team and be involved in the SuC's procurement process.
- Security requirements should be clearly identified as part of the evaluation process, and should be used for ranking the vendor's solution.
  - This approach ensures a level playing field, helping avoid costly design modifications that may lead to litigation measures.
- Create an Information Security System (ISS) document, in which the main railway cybersecurity principles and requirements are detailed.

- Some or all of the ISS document should be included in all tender documents of relevant SuCs.
- It should integrate constraints that will ensure future good operation.
- The ISS should address IT and OT environments.

- Create a high-level architecture in which the SuC is positioned in a segmented network.
  - At minimum, the SuC should be positioned in any of the following networks: safety-critical, reliability-critical, enterprise systems and third-party systems. A finer grade of criticality maybe required, according to the standards selected.
- OT cybersecurity principles in the ISS must reflect the sensitivity and security level of protected systems.
  - For example if the work is considered very sensitive, the specification should indicate that it can only be performed by qualified and potentially approved personnel.
- PT operation should drive the ISS solution and not the opposite, and scalability of the proposal.
- The ISS should include security requirements based on the DID concept.
- Security principles should apply to all layers of the OSI stack, and should consider the following elements: data, application, host, network, perimeter.
- The ISS must consider personnel, procedural, technical and physical security for the entire duration of the SuC's lifecycle.
- Vendors should be able to demonstrate the concept of 'security by design'.
  - IEC 62443 describes different levels of maturity in a product development process and the Operator may require from the vendors to be homologated at the right level.
- The cybersecurity solutions, which provide protection against threats that are evolving daily, should always specify the use of updates. These updates should be released following the identification of new high-risk malware or at minimum every six months.
  - Antivirus and IDS are examples of solutions requiring updates to perform correctly.
- Create a risk and vulnerability assessment for the SuC.
  - The PTO should create a preliminary assessment, completed by the SuC/solution supplier.
  - It should assess worst-case physical consequences when an attack perpetrated by outsiders and insiders is performed on the SuC, mis-operating the system's CPUs and other components.
- A high-level cybersecurity architecture, in the form of diagram, should be included and shared with suppliers and vendors and should include pre-defined security levels. If the procurement process includes any test and testbed for evaluation of the product, the results should also include any cybersecurity test ahead of the system's approval.
- Contingency plans should be developed, documented in the ISS and maintained to ensure that essential level of service is provided following any loss of processing capability or destruction of IT/OT systems.
  - Contingency plans should include the backup policies.
- Account for interoperability issues, in particular where different policies are considered for IT and OT.
- A continuous monitoring process for identification, authentication, authorisation and access control and administration of information infrastructure security should be developed for OT and IT environments, in order to determine whether proper security has been established and maintained.
- Security event logs should be kept for each device and system for a minimum of one year and protected from unauthorised access, modification and deletion.
- The ISS should stress that accessing confidential information environments must require authentication and be restricted to legitimate business needs.
  - User privileges should be allocated on 'need to know' and 'least privilege' business principles.
  - Recommend multi-factor authentication.

TECHNOLOGICAL CHOICES

- The ISS should list the technology choices for the foundational requirements and security levels assigned in the architecture.
- The following figure shows a summary of the technologies that should be considered under TS50701 / IEC 62443

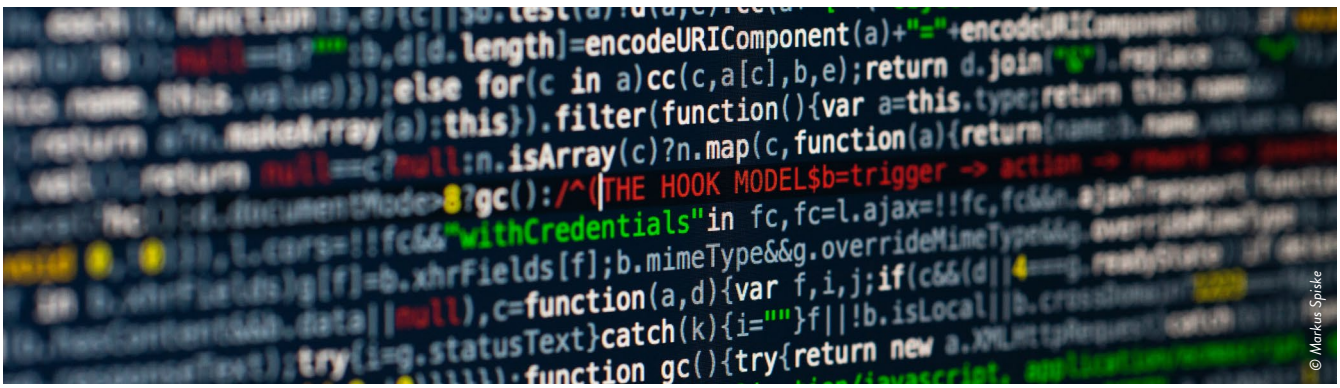
Figure 18: Summary of the main technologies covering the seven foundational requirements; source Serge Van Themsche

Foundamental Requirements	Description
FR1: Identification and authentication control	Network Access Control
	Simple Authentication Apps
	Multi-Factor Authentication
	Certificate-Based Authentication
FR2: Use control	Access Control Models
	LAN
	WAN
	Automated Audit management Software
	Non-Repudiation and Message Authentication
FR3: System integrity	Whitelisting Technologies
	Sandbowing technologies
	Vulnerability scanners
	Anti-malware software
	End-point solutions
	Firewalls
	Intrusion Detection System
	Intrusion Protection System
FR4: Data confidentiality	Virtual Private Network
	Proxy Servers
	Web Servers
	Encryption technologies
	Hashing technologies
	Data Loss Prevention software
FR5: Restricted Dataflow	Demilitarized Zone
	Data diode
	Unidirectional gateway
	Firewalls
	Continuous Monitoring System
FR6: Time to respond to events	SIEM
	OCC/SOCC
	Continuous Monitoring System
	Network Operational control
	SOAR
FR7: Resource Availability	

GLOSSARY AND WORD DEFINITION

1. ACN: Administrative Communication Network
2. AES: Advanced Encryption Standard
3. ATC: Automatic Train Control
4. ATO: Automatic Train Operation
5. ATP: Automatic Train Protection
6. ATS: Automatic Train Supervision
7. AVLS: Automatic Vehicle Location System
8. C2: Command and Control Centre
9. CBTC: Communication-Based Train Control
10. CCSC: Common Component Security Constraints
11. CVE: Common Vulnerability and Exposure
12. COTS: commercial off-the-shelf; conforming to the manufacturer's datasheet and available to any purchaser
13. DDoS: Distributed Denial of Service
14. DTU: Driverless Train Operation
15. DMZ: Demilitarized zone
16. DPI: Deep-Packet-Inspection
17. EDR: Endpoint Detection and Response
18. EOP: end of production; date of discontinuance from manufacture
19. ESS: Enterprise Security System
20. FR: Foundational Requirement
21. GDPR: General Data Protection Regulation
22. HTTP: Hypertext Transfer Protocol
23. HTTPS: Hypertext Transfer Protocol Secure
24. IoT: internet of Things
25. IDS: Intrusion Detection System
26. IPS: Intrusion Protection System
27. ISMS: Information Security Management Systems
28. ISP: internet Service provider

29. ISS: Information Security System
30. IT: Information Technologies
31. LAN: Local Area Network
32. LMA: Limit of Movement Authority
33. MAC: Message Authentication Code
34. MFA: Multi-factor authentication
35. MiM: Man-in-the-Middle
36. MPLS VPN: MultiProtocol Label Switching VPN
37. MFA: Multi-factor authentication
38. NAC: Network Access Control
39. NGFW: Next Generation firewalls
40. NTP servers: Network Time Protocol servers
41. NMS: Network Management System
42. OCC: Operational Control Centre
43. OCN: Operational Communication Network
44. OJEU: Official Journal of the European Union (contract notice)
45. OT: Operational Technologies
46. PKI: Public Key Infrastructure
47. PII: Personally Identifiable Information
48. PIS: Passenger Information System
49. PLC: Programmable Logic Controller
50. PPP: Private-Public Partnership
51. RaSTA: Railway Safe Transport Application (protocol)
52. RAT: Remote Access Trojan
53. RBAC: Rule or role Based Access Control
54. RFI: Request For Information
55. RFP: Request For Proposal
56. RFQ: Request for Quotation
57. RBAC: Rule or role Based Access Control
58. SBOM: Software Bill Of Material
59. SCADA: Supervisory control and data acquisition
60. SCN: Safety Communication Network
61. SDLC: Software Development Life Cycle
62. SDN: Software Defined Networking
63. SecRAC SECurity-Related Application Condition
64. SIEM: Security Information and Event Management
65. SL: Security Level
66. SLA: Service Level Agreement
67. SRAC: Safety-Related Application Condition
68. SOCC: Security Operational Control Centre
69. SL-T: Security Level Target
70. SQL: Structured Query Language
71. SSL: Secure Sockets Layer
72. SuC: System under Consideration
73. TCP: Transmission Control Protocol
74. URL: Uniform resource Locator
75. VRF: Virtual Routing Forwarding
76. VLAN: Virtual Local Area Network
77. VPN: Virtual Private Network
78. WAN: Wide Area Network



ACKNOWLEDGEMENTS

We would like to express our special thanks to the following people:

- Paul GWYNN, Chairman of the UITP Cybersecurity Committee, active member of the Cybersecurity Working Group, this Report and Director International Business Development at Init Group.
- Carlo CAFASSO, Leader of the Cybersecurity Working Group, Work this Report and Head of Operation and Maintenance – Operational Technology ATM.
- Serge VAN THEMSCHE, Co-Leader of the Cybersecurity Working Group, this Report and Business Development Advisor at Cylus.
- Baldvin GISLASON BERN, Active member of the Cybersecurity Working Group, this Report and Expert Engineer at the Software Security Group at Axis Communications.
- Cristiano STIFINI, Active member of the Cybersecurity Working Group, this Report and Corporate Security Operational Coordinator at ATAC Roma.
- Andrew GINTER, active member of the Cybersecurity Working Group, this Report and Vice-President Industrial at Security Waterfall Cybersecurity.
- Jesus MOLINA, active member of the Cybersecurity Working Group, this Report and Critical Infrastructure Cyberprotector at Security Waterfall Cybersecurity.
- Eddy THESEE, Active member of the Cybersecurity Working Group, this Report and Vice President Cybersecurity at ALSTOM.
- Simon TONKS, Active member of the Cybersecurity Working Group, this Report and Regional Cybersecurity Director at ALSTOM
- Luc DANANCHY, Active member of the Cybersecurity Working Group, this Report and Commercial Chief Technology Officer at AKKA Technologies Belgium (now Akkodis.com)
- Mats ZUIDAM, Active member of the Cybersecurity Working Group, this Report and Information Security Officer at GVB
- Israel BARON, Active member of the Cybersecurity Working Group, this Report and Vice President Customer Relations at Cervello
- Denis LUYTEN, Security consultant and manager of the Cybersecurity Working Group, this Report at UITP
- Benjamin STEENS, Service Excellence Unit Officer at UITP

ANNEX 1: EXAMPLE OF THE PROCUREMENT OF PIS/AVLS FOR A BUS OPERATION

Figure 19: Transmilenio BRT operation in Bogota, Columbia. Source: Felipe Restrepo Acosta, [8]

Digitalisation is taking bus operations by storm, as public authorities realise that new IT technology improves productivity, reduces operating and maintenance costs and - more importantly - improves the passenger experience. Obviously, bus operations and their associated digital technologies vary tremendously. Hence it is difficult to provide an example that would be simultaneously relevant for procurement teams managing high-capacity transit systems such as a Bus Rapid Transit (BRT) or a high-density fleet and for a small operator's buyer procuring a simple system for a small conventional fleet.

Indeed, the difficulty resides in the fact that high-capacity bus networks rely on onboard and roadside systems that are increasingly like those found in Light Rail Transit (LTR) systems. On the other hand, small bus operators are only investing in simple, real-time passenger information system. Thus from a tender process perspective, the specification of cybersecurity requirements is very different. More concretely, high-capacity bus transit systems must include constraints linked to SuCs running on Operational Technology (OT) and Information Technology (IT) networks, while small operators are mainly concerned about IT systems.

PIS / AVLS DESCRIPTION

We will describe these two environments so that the reader can understand the specific challenges linked to what are two very different processes, by using a technology called a Passenger Information System (PIS). Wikipedia describes a PIS as ***"an electronic information system which provides real-time passenger information. It may include both predictions about arrival and departure times, as well as information about the nature and causes of disruptions. It may be used both physically within a transportation hub and remotely using a web browser or mobile device".*** A PIS primarily depends on the bus real-time location; thus the PIS may often be extended to what is called an AVLSs (Automatic Vehicle Location Systems).

AVLSs and Control Systems: Regardless of the level of network sophistication of the fleet to monitor, current operational information on bus services is collected from AVLS and from control systems, including incident capture systems. This real-time information is then compared with the published service timetable by programmes in order to predict how bus services are likely to run in the next few minutes to hours. These programmes

8 CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via Wikimedia Commons

can include limited information, or may integrate more sophisticated simulation programmes that consider other traffic parameters (for example, traffic jams, historical data, events planned).

Display of information: This is delivered in one or multiple languages on the onboard and/or roadside environment, via one of the following media:

- Phone (manned or an automated answering system).
- Touch screen kiosks for self-service.
- Internet, via a website browser.
- PDA or mobile phone (typically using SMS or WAP).
- LED displays and screens inside stations or on board the bus.
- Some system also includes voice messages at the various stops.

Operational context: A PIS provides travel information to passengers, enabling them to make informed decisions on modes, routes and departure times. This is based broadly on a framework divided into two contexts:

- The pre-trip context, which provides information on timings, fares and routes well before starting travel, through the internet or by SMS.
- The in-trip context, which provides information like stop location and places of interest while on the move.

COMPLEX PIS AVLS SYSTEMS

The following figures illustrate the environment of a complex bus transit network. PIS technologies are installed on the roadside (mainly PIS displays) and in the buses (PIS displays and message recording) as well as the GPS localisation system.

Data is sent back and forth from the onboard and roadside environments to the OCC, to simulate the traffic conditions and estimate the travel time to the destination. Passengers can also consult their mobiles, via an app, to get the latest updates.

Figure 20: Autobus Onboard and roadside networks; Source: Serge Van Themsche

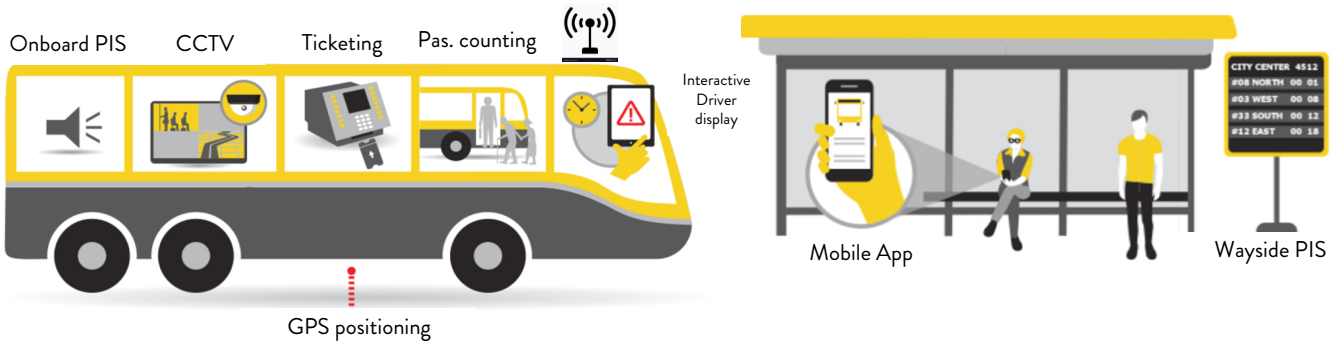
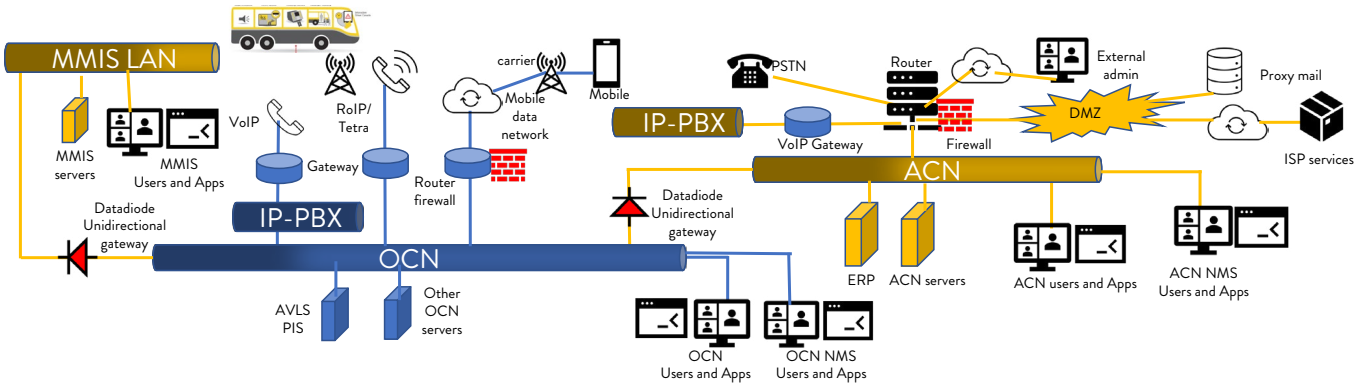


Figure 21: Example of complex autobus OCC network architecture; source: Serge Van Themsche

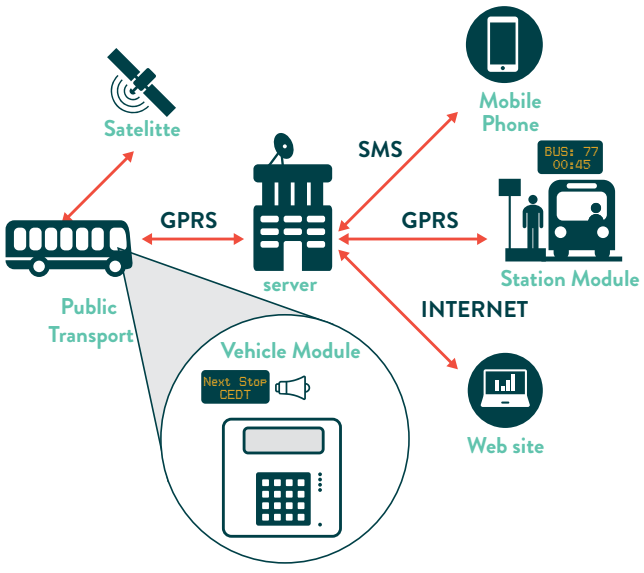


SIMPLE PIS SYSTEM

The following figure illustrate the environment of a simple bus operation. The tracking of the vehicle is done also here through GPS localisation system. Small cities can install PIS displays on the roadside or on onboard the buses but many of them will rather directly use the mobile phone of the passengers to provide scheduling information. Hence, in its most simplified architecture, a PIS must consider the following environments:

- User interface on a smart phone: This retrieves information (for example, arrival time, interval and route information for bus) by sending queries to the server via an app.
- Bus mobile device, driver interface and GPS: The bus needs to update periodically data on its location to the server.
- Server managing fleet data: This provides bus information to passengers by keeping and updating running information of buses in a database.
  - This usually sends updates to the user's device via a standardised data format (for example, extensible markup language (XML) or JavaScript object notation (JSON)).

Figure 22: Example of simple autobus network architecture.



TENDER PROCESS

We will now briefly define what type of information is usually required in Europe for the acquisition of a PIS/AVLS, without going into specifics. For further details, please check Annex 2, which is based on the example of the Swedish metro operator Sporveien.

- **Project objectives:** Description of the high-level requirements.
- **Place of performance**: Route with or without geocode standard.
- **Award criteria:** Price exclusively or other criteria taken into consideration.
- **Estimated value**: In € or US$ (excluding VAT).
- **Duration of the contract:** Including test and commissioning period.
- **Detailed procurement scope:** This describes what the expected deliverables and services.
  - It can provide CPV codes to better define the scope.
  - It should specify whether variants are accepted and if so, which ones.
- **Legal requirements:** This describes the minimum legal requirements.
- **Economic and financial standing**: Minimum average overall annual turnover of the vendor.
- **Requirements of technical and professional ability:** This describes the minimum requirements.
- **Descriptions of** objective rules and criteria for participation.
- **Deposits and guarantees required.**
- **Main financing conditions and payment arrangements and/or reference to the relevant provisions governing them.**
- **The legal form** to be taken by the group of economic operators to whom the contract is to be awarded.
- **Conditions related to the contract**: Obligation (or not) to indicate the names and professional qualifications of the staff assigned to performing the contract.
- **Type of procedure**: Negotiated or not, with prior call for competition or not.
- Other relevant administrative information

ISS TECHNICAL SPECIFICATION FOR A PIS/AVLS SYSTEM

Even the simplest PIS system needs to cyber protect its assets running on the wired and wireless networks of the bus operator. Clearly, the question is, how? To answer this - particularly in a public transport environment, where passengers' lives may be at stake - means concretely deciding which cyber standard the SuC should be following.

- IEC 62443, which is mostly relevant for Industrial Control Systems.
- TS 50701, which was conceived for rail environments where safety is a crucial element, based on IEC 62443.
- IT system and associated security guidelines.

The answer obviously depends on the complexity of the bus transit system network and of the procured SuC. In our view, for a simple PIS system, the specifier could consider using mainly security guidelines on IT systems, such as the one edited by the French national security organisation ANNSI[9]. As BRTs and high-density fleets nowadays have system requirements that are similar to LTR systems, we believe that TS 50701 is probably better adapted and easier to follow than IEC 62443. Hence, we recommend that for high-capacity bus transit systems, the cybersecurity specification document follows TS 50701 (or IEC 62443). Small bus systems can follow IT security guidelines.

INFORMATION SECURITY SYSTEM

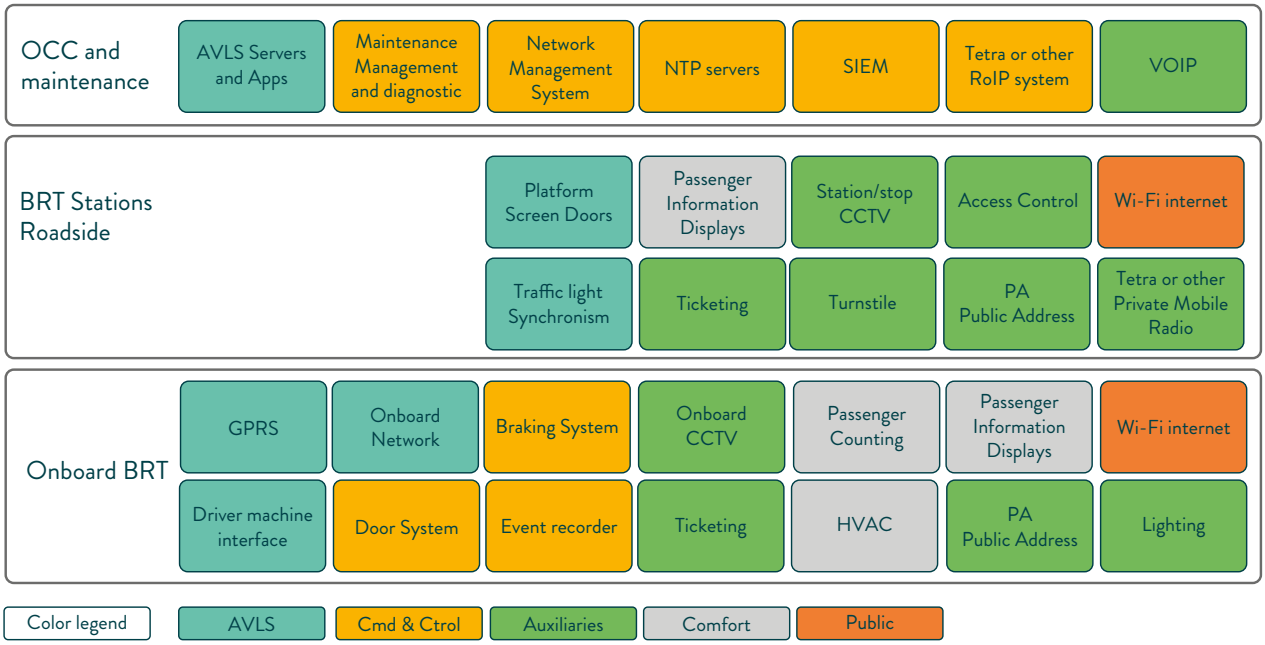
Irrespective of the methodology used for writing the SuC's cybersecurity specifications, we strongly recommend concentrating all cybersecurity requirements in a single Information Security System (ISS) document. References to this should be made in other tender documents whenever pertinent, more specific to the SuC's functionality. This ISS should be regularly updated (particularly following implementation of a newly acquired important SuC).

One of the main roles of the ISS is to present the various models that relate to the SuC. There should be three main models:

- **Bus transit asset**
- **Bus transit physical architecture**
- **Bus transit high-level zone**

Obviously, there is not much of a model for very simple bus lines. That said, it is advisable in our view to still go through this process in a simple and practical way. To simplify this process further, we have created a generic bus transit asset model (Figure 21), where most of the OT subsystems are identified. Obviously, not all BRTs integrate as many systems, such as platform screen doors, passenger counting or turnstiles. Nevertheless, the adaptation of this model to a specific environment is quite simple. From there, the bus transit physical architecture and high-level zone model can easily be derived. This process is described in more detail in Annex 2 for metro environments.

Figure 23: Example of Generic BRT asset model; Source: Serge Van Themsche adapted from TS 50701



9 Recommendations to secure administration of IT systems; ANSSI-PA-022-EN GUIDELINES; 24/04/2018

Obsolescence problem: Obsolescence of products, firmware and software is an increasing complex challenge. Annex 2 explains how this subject should be addressed for a metro. Lifecycles for a bus environment are usually much shorter than in railways. Nevertheless, end-of-life for a bus is usually set at 12 years and never later than 15 years. Thus it might be worthwhile for the specifiers to go to the process and create an obsolescence map (see figure 33). For simple PIS systems - and since most elements are IT driven -, a five-year lifecycle can probably be considered, greatly simplifying this process.

Initial risk assessment: PIS System definition (ZCR 1)

The ISS should provide a preliminary risk assessment, the objective of which is to clarify the role of the SuC to be procured. It is usually performed via a functional analysis of the SuC. Annex 2 provides a good example of what needs to be done and can easily be adapted to a BRT environment.

As shown in this paragraph, this exercise should produce an asset mapping based on physically and logically autonomous networks, including for instance:

- OCN (Operational Communication Network)
- ACN (Administrative Communication Network)
- Traffic Control System (for the unsegregated portion of the tracks)
- Untrusted networks.

The PIS/AVLS can be considered as running on the OCN, and does not necessarily need to be considered as running on a safety-critical network.

This process should end-up with a dataflow matrix, as shown in Figure 36.

For more information on this process, please check the WP4 report on risk and vulnerability assessment from UITP.

Initial risk assessment: Performing the risk analysis (ZCR 2)

TS 50701 provides a qualitative approach to performing the risk analysis. This qualitative approach is sufficient for writing the BRT's ISS tender document. The example of Annex 2 can easily be adapted to the PIS/AVLS SuC in a bus transit environment.

The end result of the complete preliminary risk analysis should be a simple and easy-to-use risk matrix, which could be calibrated by the tender specifier to reflect a more conservative or more optimistic approach to risk.

Figure 24: Likelihood assessment qualitative rating for a PIS/AVLS system; Source Serge Van Themsche

PIS/ AVLS Main assets	ASSET Availability				ASSET integrity				ASSET confidentiality			
	Human health & Safety	Operational Availability	Financial Stability	Impact Rating	Human health & Safety	Operational Availability	Financial Stability	Impact Rating	Human health & Safety	Operational Availability	Financial Stability	Impact Rating
PIS onboard	D	D	D	D	D	D	D	C	D	D	D	D
PIS wayside	D	D	D	D	D	D	D	C	D	D	D	D
GPS onboard	C	B	C	B	C	B	B	B	D	D	D	D
Driver machine interface	C	C	C	C	C	B	B	B	B	C	C	B
Passenger App	D	D	D	D	D	D	D	D	B	B	B	B
Traffic light interface	B	B	B	B	B	B	B	B	D	D	D	D
4G Telecom	C	C	C	C	B	B	B	B	C	C	C	C
Route scheduling	D	C	D	C	D	B	C	C	D	D	D	D
Onboard Network	C	B	C	B	C	B	B	B	C	C	C	C
Cybersecurity solution e.g., SIEM	D	D	D	D	D	D	D	D	D	D	D	D
PSD	B	B	B	B	B	B	B	B	D	D	D	D

Figure 25: Risk matrix; adapted from TS 50701 by Serge Van Themsche

PIS/ AVLS Main assets	Exp	EQP	WOO	TIM	Likelihood Rating
PIS onboard	Expert	Standard Equipment	Short	Short	Medium
PIS wayside	Expert	Specialized COTS	Short	Short	Medium
GPS onboard	Expert	Standard Equipment	Short	Short	Medium
Driver machine interface	Expert	Standard Equipment	Short	Moderate	Medium
Passenger App	Proficient	Standard Equipment	Short	Short	High
Traffic light interface	Proficient	Specialized COTS	Short	Short	Medium
4G Telecom	Expert	Specialized equipment	Moderate	Moderate	Low
Route scheduling	Expert	Specialized COTS	Moderate	Moderate	Medium
Onboard Network	Expert	Standard Equipment	Short	Short	Medium
Cybersecurity solution e.g., SIEM	Expert	Specialized equipment	Long	Long	Low
PSD	Expert	Specialized COTS	Long	Long	Low

Figure 26: Risk matrix; adapted from TS 50701 by Serge Van Themsche

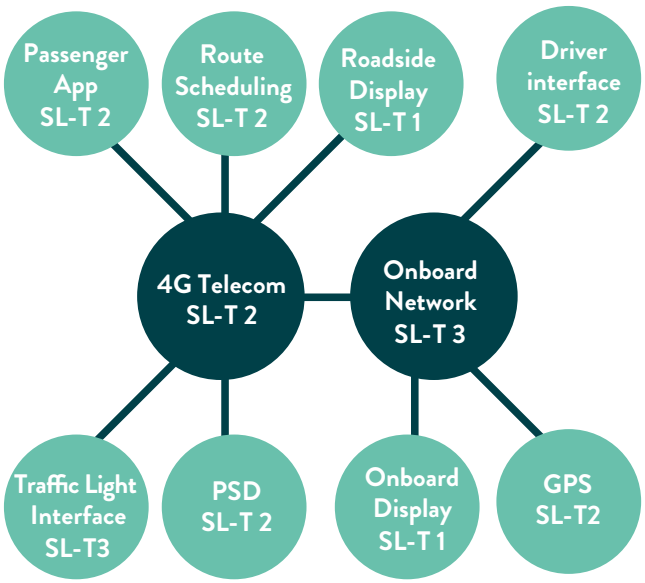
Risk evaluation		Impact rating		
PIS/ AVLS Main assets	Likelihood Rating	Asset Availability	Asset Integrity	Asset Confident.
PIS onboard	Medium	D	C	D
			Low	
PIS wayside	Medium	D	C	D
			Low	
GPS onboard	Medium	B	B	D
			Medium	
Driver machine interface	Medium	C	B	B
			Medium	
Passenger App	High	D	D	B
			Medium	
Traffic light interface	Medium	B	B	D
			Significant	
4G Telecom	Low	C	B	C
			Medium	
Route scheduling	Medium	C	C	D
			Medium	
Onboard Network	Medium	B	B	C
			Significant	
Cybersecurity solution e.g., SIEM	Low	D	D	D
			Low	
PSD	Low	B	B	D
			Medium	

The preliminary risk evaluation performed above shows the PIS/AVLS assets evaluation. The last phase of ZCR 2 is then to translate the qualitative risk evaluation into a security target for each asset. For example, the low-risk assets could have a minimum target security level, which according to TS 50701 is 1 (SL-T =1). The medium-risk assets would have a SLT-2. The traffic-light interface would have a SL-T of 3 in our view and not 4, since hi-jacking the traffic-light system could create a dangerous situation; however, the bus driver would most likely still be able to detect this abnormal situation and brake accordingly.

Initial risk assessment: Partitioning of the PIS/ AVLS (ZCR 3)

The assets must now be assigned to consistent security zones, connected through conduits. TS 50701 identifies eight pertinent cybersecurity requirements for PTOs, enabling the regrouping of these assets into zones and conduits. In our view, partitioning for a BRT system should be based at least on the risk criteria of the assets (in terms of integrity, availability and confidentiality) and physical location.

Figure 27: PIS/AVLS segmentation; source Serge Van Themsche (Conduits in blue, Zones in green)



The next step of this process is to define the criticality of the different zones. Annex 2 defines to do this for a CBTC system, and can easily be adapted to the SuC's bus various environments:

- Communication between onboard and roadside assets.
- Communication between onboard bus assets
- Communication between roadside assets

Based on the rule of thumb in that paragraph, we propose the following zone criticalities for Road (ZC-R) and Bus (ZC-B) assets:

- SCN: Safety-critical network: None.
- OCN: Operational communication network: ZCR-4 and ZCB-4.
- ACN: Administrative communication network: ZCR-3 and ZCB-3.
  - External DMZ, gateway area: ZCR-2; ZCB-2.
  - External link to a third-party network (for example, partner or cloud provider): ZCR-1 and ZCB-1, whatever their own network criticality (for example, connection to a third-party ACN network).
- Direct internet link: ZCR-0; ZCB-0.

Indeed, in our view the fact that drivers can always intervene justifies a relatively lower criticality ranking than, for example, a signalling or SCADA system. Figure 28 provides a guideline for defining the communication allowed or prohibited between different zone criticality of a bus (e.g., ZC-B 4 of a Door Control Unit) to a roadside equipment (e.g WC-R 1 external partner's network). Check section Annex 2, to create the complete communication matrix interfaces.

The last step in this process is to apply such a segmentation to the zones and conduits, physically or virtually. Annex 2 provides ample information on how to do this.

Specifying the minimum cyber protection requirements

The next step of this process is to establish the minimum cybersecurity requirements needed to protect against the anticipated threats and envisioned vulnerabilities, as developed in the previous paragraph of this example, but also as well as the means to enforce this through appropriate segmentation. We cannot overemphasise the need to adopt the DID strategy. Section 6 describes various cybersecurity technologies that should be considered for generating such a progressive barrier mechanism, introducing them through the seven FR classes. However, in our view an approach using these seven FRs would be an overkill for bus transit systems. This is even more the case for a simple PIS / AVLS system. This is why we make recommendations on which security solutions should be applied to a bus network DID strategy.

It should also be noted that, depending on the cybersecurity solutions already implemented in the bus transit system, the ISS should specify whether the vendor must make, or only ensure that, the solution is compatible with the existing IT/OT infrastructure.

Asset management:

Asset inventory is a critical component of the foundation of cybersecurity operations. For a simple PIS/AVLS, a list of assets updated in an Excel file, is sufficient. However, a complex bus transit system should consider solu-

Figure 28: Zone criticality and communication matrix from Bus to Roadside: Source TS 50701, adapted by Serge Van Themsche

			Datacenter, int DMZ, ICS/autom.	Corporate network	Gateway area, ext DMZ	Ext. partner / Traffic light	Internet
			Secure	Medium	Low	Low	Untrusted
		FROM	ZC-R 4	ZC-R 3	ZC-R 2	ZC-R 1	ZC-R 0
Zone criticality	Security maturity	SuCs					
ZC-B 4	Secure	Cmd&Control: Onboard network, DCU, Breaking Sys	Prohibited	Allowed	Prohibited	Prohibited	Prohibited
ZC-B 3	Medium	Auxiliary: CCTV, Autodiagnostic	Prohibited	Allowed	Prohibited	Prohibited	Prohibited
ZC-B 2	Low	Comfort: PIS display, HVAC	Prohibited	Allowed	Prohibited	Prohibited	Prohibited
ZC-B 1	Low	Public interface: Route scheduling APP, Wi-Fi,	Prohibited	Prohibited	Prohibited	Allowed	Allowed
ZC-B 0	Untrusted	External Com channel: Bus-to-roadside, B-to-B	Prohibited	Allowed (tech DMZ)	Prohibited	Prohibited	Allowed

tions using a continuous monitoring system, which can automatically identify and update in real time, data on the thousands of assets running on their IT and OT networks. Hence the recommendation that the ISS either specifies such a solution associated with the AVLS/PIS system, or at least ensures that it is compatible with it.

Security Solutions for applying a DID strategy:

A DID strategy requires the use of a multitude of security mechanisms. The ISS document can either specify the solutions to be implemented, or indicate the protections to consider and the cybersecurity functionalities to be implemented, then allow the vendor to select them.

Here is a list of technologies that should be considered:

- Unidirectional gateways: Segmenting and protecting the OT systems from the highly vulnerable IT environment.
- Deploying, where possible, at least one layer of hardware-enforced unidirectional gateway protection in a layered network / firewall defence-in-depth architecture to eliminate the risk of importing malware into the system through online connections. It should also eliminate the possibility of high-risk RAT attacks pivoting through layers of firewalls from the internet into safety-critical or reliability-critical networks.
- Firewalls: Establishing zone structure. Controlling which of the protected targets are exposed to connections, traffic and other information arriving from other networks.
- VPN: Establish encrypted tunnels for traffic passing through networks not controlled by the PTO.
- VLAN: Use of VLANs to separate network traffic.[10]
- Strong password and two-factor authentication.
- Antivirus solutions: Detecting threats on computers.
- Backup: Secure a working environment to restore.
- Continuous asset monitoring of roadside and onboard assets.
- IPS/IDS: Detecting and preventing threats in the network.
- Encrypting data: Securing data if media, devices or PCs are lost.
- Network Access Control (NAC): Maintaining control on connected devices and connection attempts.
- Logging: Centralised logging with a management GUI for event control and trouble shooting.
- Encrypting communications: All communications should be encrypted and authenticated.
- External media access: Reducing and removing the use of USBs, CD-ROMs / DVD-ROMs, unused RJ45, memory card readers and similar - where possible - minimises the potential risk of importing malware into the system.

Mandatory functionalities:

The PIS/AVLS system should support user identification to all configuration between client and host. It should provide a central log system and be compatible with a time system (such as an NTP server). It should provide or support a central monitoring solution of its assets for all security breaches and be fully compatible with a NAC. It should either provide or support a central monitoring solution for the OT infrastructure, raising alarms whenever anomalies are detected and provide relevant information for troubleshooting, relying on a baseline. Bus transit specifiers can also follow the TS 50701 tender processing, to provide a more holistic approach and avoid missing other important functionalities.

10 Note: VLANs should not be used to separate traffic from networks at different security levels – such networks should be physically separate.

ANNEX 2: EXAMPLE OF THE PROCUREMENT OF AN OT SUC: SIGNALLING SYSTEM FOR A METRO OPERATION

The example to illustrate a procurement of an OT SuC is the procurement of a signalling system within a metro environment. We will describe a typical procurement process for a technology called CBTC, which can evolve into an unmanned operational environment (Driverless Train Operation or DTU). Hence, we will not consider existing metro applications, where the new system would need to interface with existing signalling and other technologies to maintain a continuity of operation (in other words, there is no need to overlay the CBTC equipment over an existing signalling system). To help the readers understand this procurement process, we will now briefly explain a CBTC system.

CBTC SYSTEM PRESENTATION

Wikipedia defines a CBTC system as a *"continuous, automatic train control system utilising high-resolution train location determination, independent from track circuits; continuous, high-capacity, bidirectional train-to-wayside data communications; and trainborne and wayside processors capable of implementing Automatic Train Protection (ATP) functions, as well as optional Automatic Train Operation (ATO) and Automatic Train Supervision (ATS) functions"*, as defined in the IEEE 1474 standard.

For automatically operated metro, the concept of Automatic Train Control (ATC) has been adopted around the world. It refers to the whole system, which includes all the other automatic functions. Therefore, ATC is the package that includes ATP, ATO and ATS. Although there are many variations of ATC technology, they all adopt the following principles:

- **The ATP** provides safety, preventing over-speeding and signal overruns.
  - The metro is given a Limit of Movement Authority (LMA). On driverless metros, the LMA data is transmitted from the track to the train, where the onboard computer registers the current speed, and calculates the target speed that the train must reach and by when. It is composed of onboard and trackside equipment.
  - The core of the trackside ATP is the zone control centre. It tracks all the metro vehicles under its jurisdiction, by means of metro position data. This tracing function enables it to generate a Movement Authority (MA) according to the switch location and route information (sent by an interlocking) and metro location (sent by onboard ATP). It processes temporary speed restriction coming from the OCC, which are sent with the MA to the onboard ATP. It also has a few other safety functionalities.
  - The Onboard ATP is responsible for establishing the speed threshold. It includes the vital computing structure (for example, mainframe, driver's display unit, speed and distance measurement unit, train-to-ground communication system, train interface unit or train management unit).
- **The ATO** provides the controls replacing the driver.
  - It starts the train, allows it to accelerate up to the permitted speed, slows it where necessary for speed restrictions and stops at designated stations in the correct location. In other words, it manages the train running from one station (or predetermined operational stopping point) to the next, automatically adjusting the train speed with appropriate traction and braking commands. This is also composed of onboard and trackside equipment.
  - The onboard ATO is responsible for automatically controlling the traction and braking effort to meet the threshold set by the onboard ATP.
  - The trackside ATO oversees the control of the destination and regulation targets of every metro.
- **The ATS** checks the running times and adjusts the metro vehicle's running accordingly.
  - It acts as the interface between the public operator and the system, managing the traffic according to the specific regulation criteria.

As well as the ATC, a CBTC system relies on a train-to-wayside communication subsystem. This is based on a digital networked radio system, by means of antennae or leaky feeder cable for the bidirectional communication between the track equipment and the trains, usually using the 2.47Hz band, the same as for wi-fi.

CBTC PROCUREMENT PROCESS

For an example that can easily be followed by other PTOs for the procurement of an OT system, we decided to select a real case figure, based on available public information. The following information is based on extracts from a procurement process (2019/S 231-567971), which was published in 2019 on the European TED website by Sporveien AS, the PTO of Oslo metro and tramways.

This information is itself a summary from the procurement strategy, the legal framework, the contractual

documents and the technical specification. Following such a TED template can help the procurement process establish the main objectives needed to be followed by any PTO procurement team responsible for purchasing an OT SuC.

General project presentation

The scope included a new CBTC system with an operation management and supervision system for the complete Oslo Metro network, including depots, a new line (from Majorstuen to Fornebu) as well as equipping and modifying the rolling stock.

The **Project objectives** were: To replace the legacy signalling systems with the CBTC system; to increase the transport capacity for Oslo Metro and; to improve the safety and punctuality of the Oslo Metro operation. This CBTC System should be adaptable to new needs as well as changes to the Oslo Metro infrastructure and rolling stock during the whole technical lifetime of the system.

Place of performance (based on Nuts Code, which is a geocode standard for referencing the subdivisions of countries for statistical purposes): NO011 Oslo

Award criteria: Price was not the only award criterion. These criteria were stated only in the procurement documents.

Estimated value: NOK 4,900,000 000 (€494m), excluding VAT.

Duration of the contract: from 30 June 2021 to 31 December 2053 without any renewal, so 32 years.

Detailed procurement scope

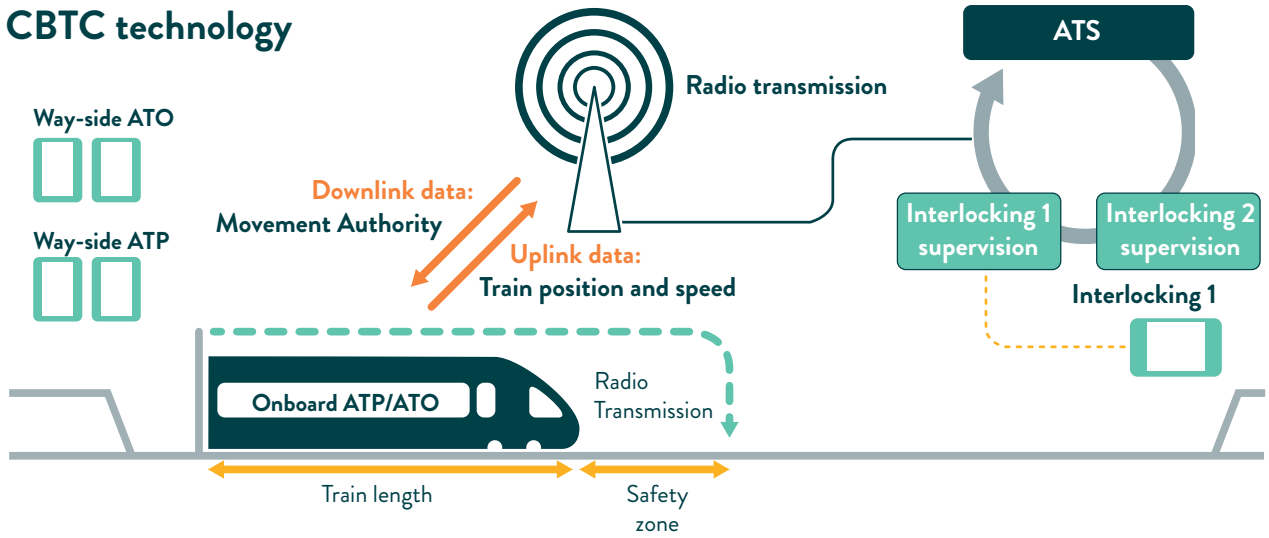
Contracting authority intended to procure a new CBTC system comprising of the following main deliveries and functions:

- Signalling and interlocking for the entire Oslo Metro network including Fornebubanen and depots.
- Operation management and supervision system integrated in the OCC.
- CBTC integration in passenger trains and maintenance vehicles.
- Automatic train operation (GoA2) for passenger trains and maintenance vehicles.
- Updating of the existing driving cab simulator to CBTC functionality.
- Traffic management simulator.

The scope of work includes all deliveries and services required to replace the existing signalling and train control system with a new CBTC system. The delivery includes design, integration, installation, testing, commissioning, documentation, training and putting into service a complete and fully operational CBTC signalling system in Oslo Metro in accordance with agreed time schedule, including maintenance and support services of the CBTC System for 25 years following final acceptance.

The contracting authority will provide resources for first- and second-line maintenance under the supervision and responsibility of contractor.

Figure 29: A typical radio-based CBTC; source; 'The advent of unmanned electric vehicles'; Author: Serge Van Themsche



Sporveien gave CPV (Classification of Public Procurement) codes to better define the scope:

- 34942000 Signalling equipment
- 45316200 Installation of signalling equipment
- 71320000 Engineering design services
- 50324100 System maintenance services
- 50000000 Repair and maintenance services
- 34632000 Railways traffic-control equipment
- 34632200 Electrical signalling equipment for railways
- 34632300 Electrical installations for railways
- 45234120 Urban railway works
- 48140000 Railway traffic control software package
- 45234115 Railway signalling works
- 72200000 Software programming and consultancy services
- 72227000 Software integration consultancy services
- 34943000 Train-monitoring system.

Variants were accepted

Options related to CBTC functionality and supporting systems:

1) Additional functionality related to crew management.

2) Additional functionality related to train and fleet management.

3) GoA4 functionality through an upgrade, which would enable driverless operation (DTO).

4) Many others that are relevant to the process but not to this report.

Requirements for participation

Legal requirements: Participants should be a legally established company.

Economic and financial standing: candidates should have solid financial standing and have an average overall annual turnover of NOK 500,000,000.

Technical and professional ability

List and brief description of selection criteria: Participants shall:

- Demonstrate ethical conduct and corporate social responsibility.
- Have an adequate quality management system.
  - Have implemented the latest versions of EN 50126/128/129 /159 in their quality management systems.
- Have an adequate HSE management system.
- Have an adequate information security system management.
- Have technical expertise and capacity to fulfil the contract.
- Have knowledge of relevant standards and approval processes for the delivery.
- Have solid technical and professional maturity.

Objective rules and criteria for participation

A minimum of three and maximum of six of the best-qualified candidates will be invited to submit tenders. The candidate's response to the selection criteria will be scored on a scale from 0 to 10, and those with the highest weighted total scores will be selected. The selection criterion is: 'The candidates with the most relevant experience in delivering CBTC - signalling system projects will be selected'.

Deposits and guarantees required: This information is stated in the procurement documents.

Main financing conditions and payment arrangements and/or reference to the relevant provisions governing them: This information is stated in the tender documents.

Legal form to be taken by the group of economic operators to whom the contract is to be awarded: The contracting authority may require a group of economic operators to assume a specific legal form once it has been awarded the contract, to the extent that such a requirement is needed for the satisfactory performance of the contract. The economic operators of the group shall be jointly liable for the execution of the contract.

Conditions related to the contract: An obligation to indicate the names and professional qualifications of the staff assigned to performing the contract

Type of procedure: Negotiated procedure with prior call for competition. Recourse to staged procedure to gradually reduce the number of solutions to be discussed or tenders to be negotiated. The procurement is covered by the government procurement agreement.

Administrative information

- Previous publication concerning this procedure is in the RFI 2017/S 104-209025, based on the European Directive 2014/25/EU

- The time limit for receipt of tenders or requests to participate Date: 7 February 2020 at 12:00.
- Estimated date of dispatch of invitations to tender to selected candidates: Date: 3 April 2020
- Languages in which tenders or requests to participate may be submitted: English
- Minimum time frame during which the tenderer must maintain the tender: 12 months from the date stated for receipt of tender.
- Date of dispatch of this notice: 26 November 2019
- Review procedure: Any request for a preliminary injunction against the contracting authority's decision to reject a request shall be submitted to the court within 15 days of such a notice being sent.

ISS TECHNICAL SPECIFICATION FOR A CBTC SYSTEM

To provide a more useful generic guideline on how to establish cybersecurity measures according to TS 50701, the following section will not be based solely on the Oslo CBTC tender documents. We will add sections based on TS 50701, which in our view could have been contemplated for the Sporveien tender if TS 50701 had been published at that time. That said, the cybersecurity scope had been thoroughly described in these tender documents, although in different sections (for example, Attachment 2.4.1 / other technical requirements specification, and Attachment 2.4.1.B concept development study IT security).

As we already recommended, in our view it is better to regroup all cybersecurity matters in a single ISS. Whenever pertinent, references to this document should be made in other tender documents. One of the main roles of the ISS is to present the various models that relate to the SuC. These are necessary to give the general environment in which the SuC will be implemented, and must be protected against cybersecurity threats. Not provided in the Sporveien tender documents, such models help the vendors establish the general context in which the SuC must be protected against cyberattacks.

Metro Asset model

TS 50701 indicates that railway and public transport operators must define an asset model of their network. Assets should be divided into groups corresponding to physical areas and functional criticality levels (for example, signalling, command and control, comfort, auxiliary and public). The resulting model is an input to define the SuC. Figure 30 shows an example of a metro asset model. Assets are divided in these five groups, showing their physical area. Each asset is identified by its functional name (for example, 'ATP') and illustrated using a five-colour scheme.

Figure 30: An example of a metro asset model. Adapted from TS 50701 by Serge Van Themsche

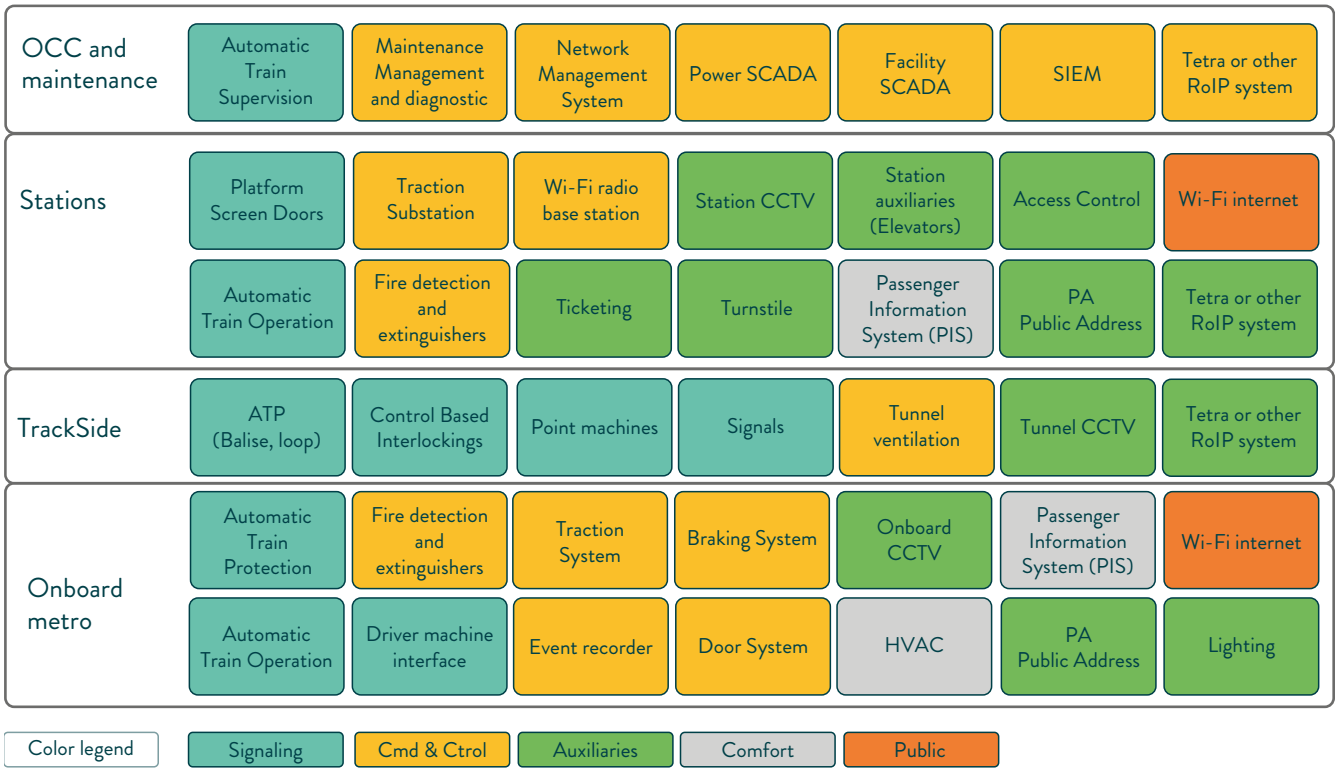
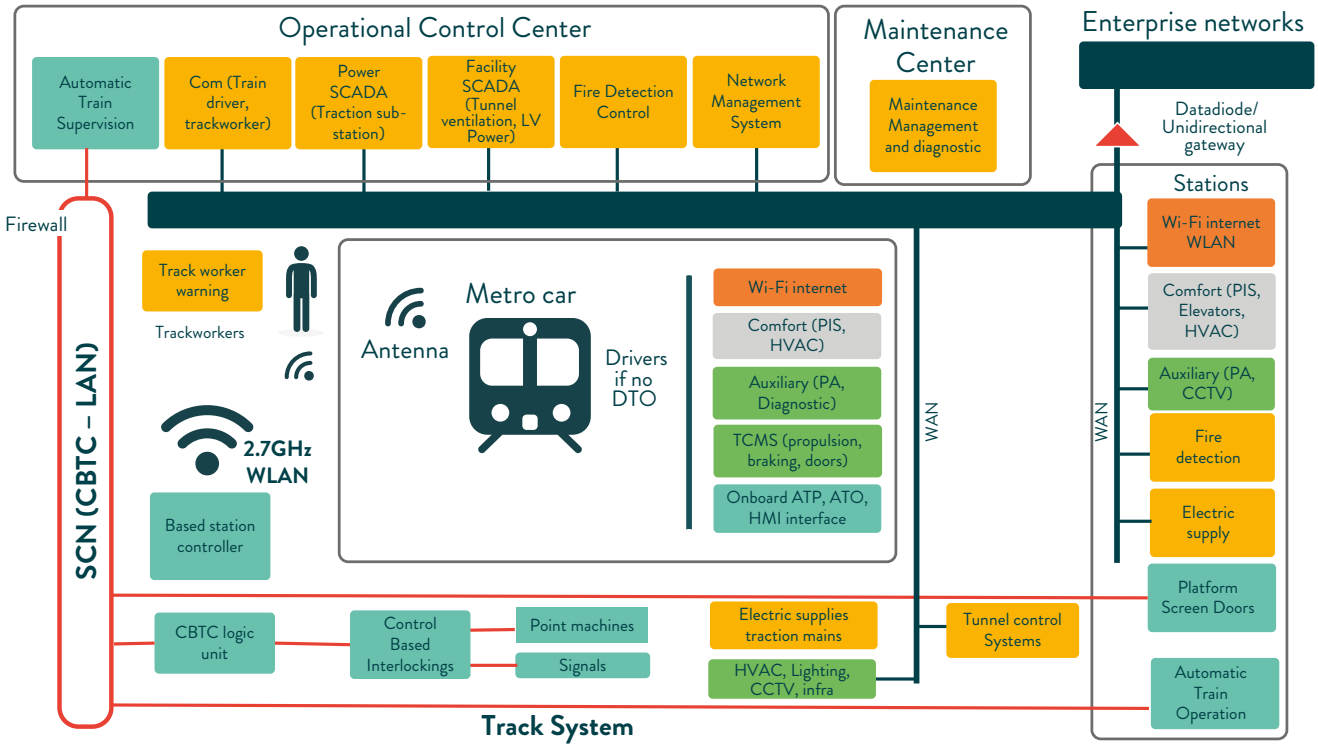


Figure 31: An example of a metro physical architecture model with CBTC.
Adapted from TS 50701 by Serge Van Themsche



Metro physical architecture model

From a cybersecurity perspective, the distributed locations of the different components and subsystems - as well as their physical security features - are to be considered, particularly in risk analysis. Figure 31 shows a simplified architecture for a metro system based around a CBTC signalling system.

High-Level Zone model

The railway operator must provide, in the ISS tender documents, a high-level railway zone model to be used as input for the SuC identification, initial risk assessment and SuC zoning activities. The preliminary zoning principles used should be enforced according to Chapter 6 of TS 50701. When segmenting the assets into zones, special care should be taken to encapsulate specific functionalities, to keep the SuC's important services working in the event of an incident in another zone. The combination of zones, conduits, subsystems and zone priorities results in a generic zoning model, which must include communication rules. Figure 32 shows the generic railway zoning reference according to the design principles of IEC/TS 62443-1-1:2019, the zoning principles of EN IEC 62443-3-2:2020 and the risk-based approach.

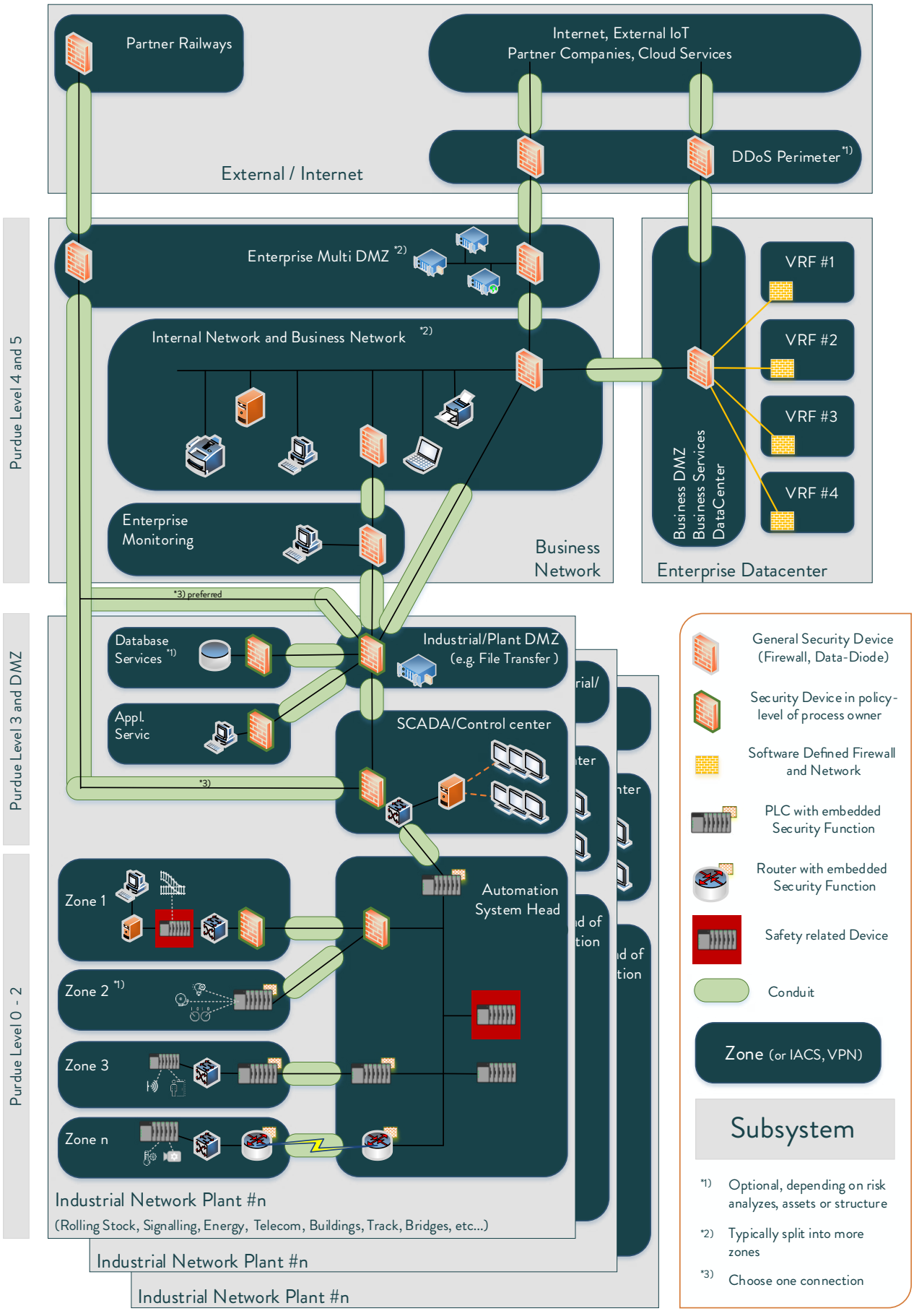
Signalling lifecycle and obsolescence problem

TS 50701 makes a reference to the lifecycle in V (as shown in Figure 4). The CBTC system lifecycle is usually specified for a long period, which - in the case of Spoorveien - corresponds to 32 years. Such a long time obviously creates problems for the CBTC vendor, as such a requirement isn't aligned with the hardware and software lifecycles, particularly for COTS products and OS software increasingly used in signalling systems. Obsolescence issues will have to be managed during this 32-year lifecycle. Since obsolescence creates system vulnerabilities, the associated cybersecurity problems will need to be addressed during that period. Hence, the PTO must manage two problems relating to the lifecycle:

- Hardware and software obsolescence within the CBTC system itself.
- Cybersecurity issues originating from this lifecycle misalignment between the signalling and the COTS product used.

As set out in section 8.3.5 of the UITP report "Obsolescence on Operational Environment and Cybersecurity", these obsolescence issues should be considered during the tender phase. As well as sharing the obsolescence risk with the supplier, the procurement team must establish the asset's lifecycle, including for each component of its subsystem. The buyer should also define the lifecycle of each component of the SuC, possibly using historical data or standards applied to the asset, highlighting the estimated period of:

Figure 32: An example of a high-level metro system zone model for CBTC. extract from TS 50701



- End of sale
- End of support
- End of life (EOP).

Armed with this information, the buyer should define a timeline for the procured asset and for all its main components, highlighting the moment when they go out of support. Figure 33 provides a simplified example of an obsolescence map for a CBTC system, based on a 32-year lifecycle.

The problem is obviously that unless there is a contractual link between the vendor and the PTO, the obsolescence issue will be difficult to enforce. One way of solving this problem is to transfer the responsibility of managing obsolescence by engaging the SuC's vendor in a long-term maintenance contract. This is what Spoorveien has done within their CBTC tender.

However, cybersecurity problems created by obsolescence will not be solved by this transfer, unless the cybersecurity responsibility is also transferred. It is a key aspect of cybersecurity, often forgotten by the tender specification of an SuC, which is linked to the long-term management of the railway assets.

Indeed, the above map doesn't show the evolution of standards, proprietary protocols and components that are inherently part of a CBTC system. With thousands of assets to be installed and maintained for 32 years, such a map becomes impossible to manage by the procurement team at a finer granularity. However, without such granularity, showing the mandatory updates due to these changes and their inevitable associated vulnerabilities, any cybersecurity software used to protect the SuC won't be adapted to follow up these evolutions, nor will the cybersecurity vendor be contractually obligated to do so.

Hence, we strongly recommend that for highly critical SuCs such as a CBTC system, the procurement of a cybersecurity protection be part of the responsibility transferred to the maintainer of the CBTC system. In such cases, and to ensure a clearcut responsibility between SuC Vendors, the networks separation into two is an effective way out. The CBTC provider will have the SuC's cybersecurity responsibility, and the other networks will be treated as untrusted. The use of unidirectional gateways will physically separate the two networks, ensuring to the CBTC maintainer and the PTO that no external factors can interfere with the CBTC cybersecurity protection, avoiding incident responsibility discussions.

What should be done for cybersecurity in the event that the maintenance responsibility for a CBTC or other critical SuCs isn't transferred to the vendor? It is essential that the cybersecurity solutions be purchased with updates and sales level agreements that provides a five-year coverage. Such SLAs should ensure that the cybersecurity solutions will evolve to take into account the CBTC's OS and main firmware updates. Concretely, it means that a 32-year CBTC life cycle will generate six tendering processes for cybersecurity solutions. It is obviously time consuming and expensive to do so, and goes a long way to explaining why transferring the responsibility to the maintainer is better.

There is another issue that must be solved in case of safety-critical systems such as signalling (SIL > 0), whenever the responsibility resides with the cybersecurity vendor or the PTO. Any safety-critical system must present a safety case according to EN 50126. Any solution, including cybersecurity that would affect the SuC must be contemplated within this safety case. Hence, active cybersecurity solutions that would be purchased after its first implementation would impact the safety case and trigger the need to update it. This complex and expensive process would need to be engaged at least five times for a 30-year contract. This is why procuring passive solutions, which gain access to the network data through a mirror port, unidirectional gateway, or a tap are recommended (for example, a continuous monitoring system with only IDS functionalities and not IPS).

Safety and Cybersecurity Cases

The PTO must obtain a safety case from the CBTC vendor, which is a structured argument, supported by evidence, to justify that a system is acceptably safe for a specific application, in the railways given operating environment. This safety case is reviewed by a safety assessing company, which will need to approve it. It is only after its approval that the PTO may start commercial operations.

Nowadays, the certifying bodies that review these safety cases require that a cybersecurity case be added to the analysis for critical SuCs. This case provides evidence and argumentation that the SuC's design and development can be operated to the expected security confidence level; that is to say the cybersecurity objectives identified in the threat and risk assessment resulting in the cybersecurity requirement specification (for example, SL-T). For critical SuCs, it is strongly recommended that the PTO specifies that a cybersecurity case will need to be delivered as part of the SuC's safety case and deliverables.

This report will now give an example of how to build an initial risk assessment with a preliminary segmentation into zones and conduits. As mentioned earlier, this pre-

Figure 33: An example of an obsolescence map for a CBTC system. Source Serge Van Themsche (where Upd= up-date, Mod = Modernise and Rep = Replace)

Sub-system	Component	Y < EOS	Y7	Y12	Y16	Y17	Y20	Y21	Y22	Y27	Y32
ATO onboard	Hardware	15				Mod					Rep
	Firmware	15				Mod					Rep
	OS	8		Upd					Upd		Rep
ATO wayside	Hardware	15				Mod					Rep
	Firmware	15				Mod					Rep
	OS	8		Upd					Upd		Rep
ATP onboard	Hardware	15				Mod					Rep
	Firmware	15				Mod					Rep
	OS	8		Upd					Upd		Rep
ATP wayside	Hardware	15				Mod					Rep
	Firmware	15				Mod					Rep
	OS	8		Upd					Upd		Rep
Interlocking	Hardware	15				Mod					Rep
	Firmware	15				Mod					Rep
	OS	8		Upd					Upd		Rep
Signals	Hardware	30									Rep
	Firmware	15				Mod					Rep
Point machine	Hardware	30									Rep
	Firmware	15				Mod					Rep
Driver machine interface	Hardware	15				Mod					Rep
	Firmware	15				Mod					Rep
	OS	10		Upd					Upd		Rep
Radio base station	Hardware	15				Mod					Rep
	Firmware	15				Mod					Rep
	OS	8		Upd					Upd		Rep
Wi-fi technology	Hardware	10		Mod					Mod		Rep
	Firmware	10		Mod					Mod		Rep
	OS	8		Upd					Upd		Rep
Signaling screen in OCC	Hardware	15				Mod					Rep
	Firmware	8		Upd					Upd		Rep
	OS	8		Upd					Upd		Rep
Others to be described	Hardware	15				Mod					Rep
	Firmware	8		Upd					Upd		Rep
	OS	8		Upd					Upd		Rep
Cybersecurity solution	Hardware	5	Rep	Rep		Rep			Rep	Rep	Rep
	Firmware	5	Rep	Rep		Rep			Rep	Rep	Rep
	OS	5	Pep	Rep		Rep			Rep	Rep	Rep
External to CBTC: e.g., PSD	Hardware	15				Mod					Rep
	Firmware	15				Mod					Rep
	OS	8		Upd					Upd		Rep

liminary information is mandatory, and should be part of the ISS tender document. Depending on the criticality of the SuC, this ISS document may be included - in part or in whole - within the tender documents. We will then define the specific tender requirements that should be part of a CBTC system. Based on this information, the SuC vendor should be capable of building such a cybersecurity case. Readers will be able to use this example to replicate to other SuCs.

Initial risk assessment: CBTC System definition (ZCR 1)

The first phase of the risk assessment is to properly understand the role of the SuC to be procured. The best way to do this is to perform a functional analysis of the SuC in question, which is a methodology used to explain the workings of a complex system. The idea is that a system is viewed as computing a function or more generally, as solving an information processing problem. It assumes that such processing can be explained by deconstructing the complex functions into a set of simpler ones that can be computed. The objective is that when this type of deconstruction is performed, the subfunctions that are defined will be simpler than the original function, and as a result will become easier to explain.

Here is a high-level functional description of the CBTC system, as provided by Sporveien. The procured CBTC must provide the following **main functions for operation, management and supervision:**

- managing the daily timetable
- managing the train service
- supervising train operations
- controlling traction power
- managing the interface with the HMI
- providing the interface with the communications system for passengers and staff
- providing the interface with the passenger information system
- providing the interface with passenger surveillance systems
- supporting maintenance
- managing rolling stock and staff resources
- OCC and backup control centre.

And the following **main functions for train operation:**

- ensuring safe movement of trains
- driving the train
- supervising the guideway
- supervising passenger transfer
- operating a train
- ensuring detection and management of emergencies
- functional requirements during migration phase.

Functional Subsystems' Mapping:

Any SuC risk analysis is based on a functional mapping of relevant subsystems and modules required to be or already implemented in the different railway and passenger transport networks. Such mapping should be implemented based on physically and logically autonomous networks including:

- SCN (Signalling Communication Network)
- OCN (Operational Communication Network)
- ACN (Administrative Communication Network)
- SFDS (Smoke and Fire Detection) Network
- Traffic control system (for the unsegregated portion of the tracks)
- Untrusted networks.

Figure 34 shows (in part) the functional elements of the Sporveien CBTC system. It also gives a brief mapping of the functional subsystems. However, it focuses exclusively on the CBTC system and avoids describing the other networks. Unfortunately, many risks can originate within the corporate IT network, and a brief description of these subnetworks would be advisable.

Figure 35 provides additional information on the dataflow between the CBTC and other subsystems, describing their physical and non-physical interfaces. Such a figure is preliminary and doesn't provide the complete overview. The contracted vendor should be responsible for updating and completing this CBTC system context diagram during the project execution and delivering what is necessary to fulfil the contract.

Figure 34: Example of a CBTC architecture explaining the functional interface; Source: Sporveien tender documents

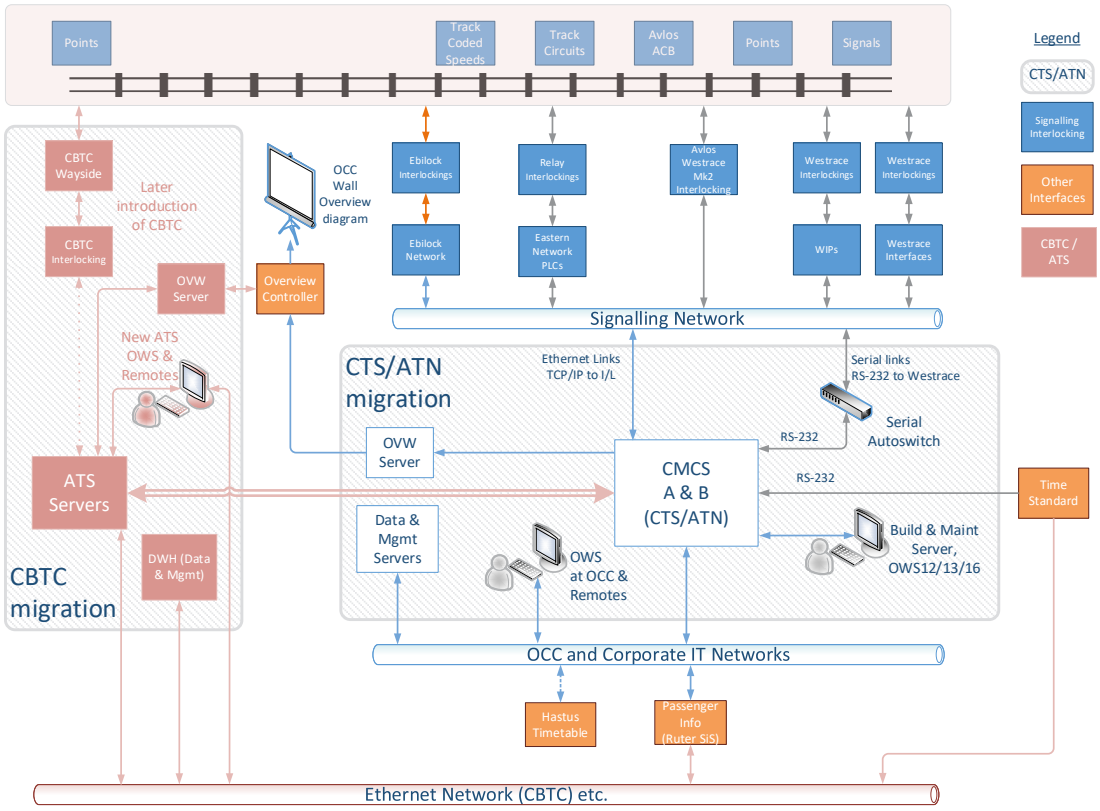
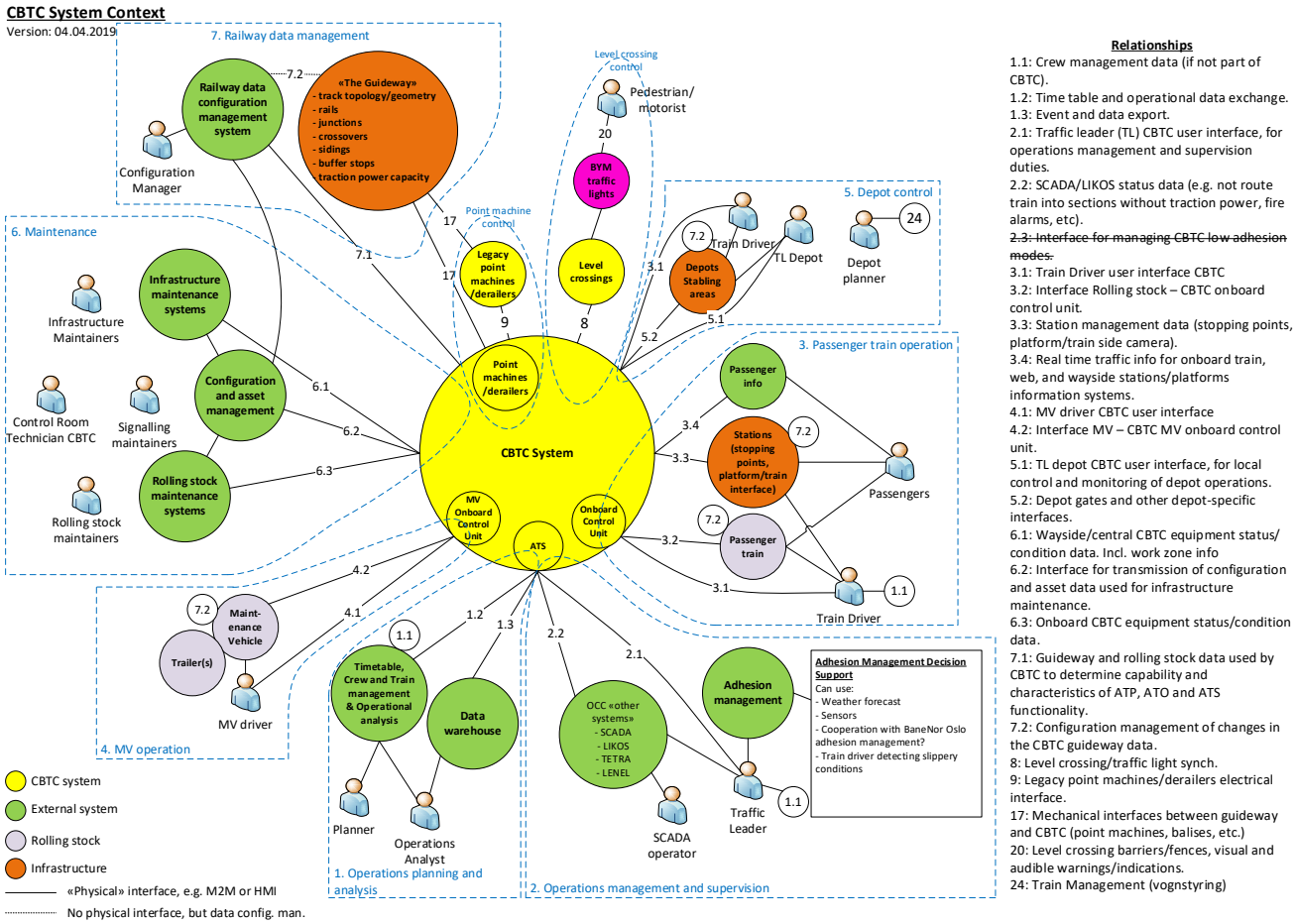


Figure 35: High Level CBTC Context diagram; Source: Sporveien tender documents



Relationships

1.1: Crew management data (if not part of CBTC).
1.2: Time table and operational data exchange.
1.3: Event and data export.
2.1: Traffic leader (TL) CBTC user interface, for operations management and supervision duties.
2.2: SCADA/LIKOS status data (e.g. not route train into sections without traction power, fire alarms, etc).
~~2.3: Interface for managing CBTC low adhesion modes.~~
3.1: Train Driver user interface CBTC
3.2: Interface Rolling stock – CBTC onboard control unit.
3.3: Station management data (stopping points, platform/train side camera).
3.4: Real time traffic info for onboard train, web, and wayside stations/platforms information systems.
4.1: MV driver CBTC user interface
4.2: Interface MV – CBTC MV onboard control unit.
5.1: TL depot CBTC user interface, for local control and monitoring of depot operations.
5.2: Depot gates and other depot-specific interfaces.
6.1: Wayside/central CBTC equipment status/ condition data. Incl. work zone info
6.2: Interface for transmission of configuration and asset data used for infrastructure maintenance.
6.3: Onboard CBTC equipment status/condition data.
7.1: Guideway and rolling stock data used by CBTC to determine capability and characteristics of ATP, ATO and ATS functionality.
7.2: Configuration management of changes in the CBTC guideway data.
8: Level crossing/traffic light synch.
9: Legacy point machines/derailers electrical interface.
17: Mechanical interfaces between guideway and CBTC (point machines, balises, etc.)
20: Level crossing barriers/fences, visual and audible warnings/indications.
24: Train Management (vognstyring)

Based on all the previous models and diagrams, the ISS document should provide a list of the subsystems and their networks, along with their interoperability. Figure 36 summarises these elements in an indicative and non-exhaustive way, indicating whether the considered dataflow should be unidirectional or bidirectional. The contracted vendor should also be responsible for updating and completing this CBTC dataflow during the project execution and deliver what is necessary to fulfil the Contract.

The dataflow description completes the first phase of the zone and conduit requirement specification, inspired by TS 50701 (ZCR 1) defining the SuC.

Initial risk assessment: Performing the risk analysis (ZCR 2)

In its section 6.3, TS 50701 provides a qualitative approach to performing the risk analysis. This qualitative approach is usually sufficient for writing the ISS tender documents. This is not the case for the detailed risk assessment, which is to be provided by the vendor following the design phase, considering a quantitative assessment. TS 50701 provides, in its Annex E, two methodologies for performing this detailed risk assessment. The first is based on an adaptation of the risk approach in the standard EN50126-1. The second is usually developed by railway system integrators and turnkey suppliers as a tool in their solution security risk assessment. This approach is generally deployed for large scale projects, both in metros and mainline railways. Its structure is based on ISO/IEC 27005.

Since a new CBTC system is probably the most critical SuC, it might be in the interest of the specifier to take the extra effort required to use this more detailed approach, such as this second methodology. The ISS document can then describe a semi-qualitative approach.

Threat landscape: To build an appropriate cybersecurity strategy, railway and public transport operators should establish and maintain updated a consistent list of generic cybersecurity threats capable of jeopardising their application. TS 50701 recommends that threat libraries and reports such as the following should be taken as inputs:

- ENISA Threat Landscape Yearly report
- ISO/IEC 27005
- NIST SP 800-30

This threat landscape is an important input to be extended in the detailed threat identification. This landscape should be provided within the ISS documents, with a focus on the SuC.

Figure 36: Example of a metro dataflow between subsystems and their networks and if it is uni- or bidirectional; source Serge Van Themsche

Location	Sub-system	SCN	OCN	ACN	SFDS	TCS	Untrusted
OCC and maintenance depot	ATS	Bi					
	MMS		Uni	Bi			
	NMS	Bi	Bi	Bi	Bi	Bi	
	Power SCADA		Bi				
	Facility SCADA		Bi		Bi	Bi	
	SIEM			Uni			
	RoIP		Bi				
Stations	PSD	Bi	Bi				
	Traction SS		Bi				
	Wi-fi RBS	Bi	Bi				
	Station CCTV		Bi				
	Station Aux		Uni				
	Access Control		Bi				
	Wi-fi internet						Bi
	ATO	Bi					
	Fire system				Bi		
	Ticketing			Uni			
	Turnstile			Uni			
	PIS	Uni	Bi				
	PA		Bi				
	RoIP		Bi				
Trackside	ATP	Bi					
	CBI	Bi					
	Point Mach	Bi					
	Signals	Bi					
	Tunnel Vent.		Bi		Bi		
	RoIP		Bi				
Onboard metro	ATP	Bi					
	Fire detection		Bi				
	Traction Sys		Bi				
	Braking sys		Bi				
	CCTV		Bi				
	PIS	Uni	Bi				
	Wi-fi internet						Bi
	ATO	Bi				Bi	
	Drive Mach Int	Bi				Bi	
	Event recorder	Uni	Uni				
	Door System		Bi				
	HVAC		Bi				
	TCMS	Uni	Bi				
	PA		Bi				

Figure 37 provides the highest threats for 2020 - as compiled by ENISA (the European Union Agency for Cybersecurity) - that are tainted by an IT perspective. It should be adapted to an SuC such as a CBTC. For example, forging or abuse of rights, eavesdropping and similar threats should probably be considered, rather than web-based or crypto-jacking attacks.

Figure 37: ENISA top 15 threats of 2022

Sporveien provided a list of threat actors based on background information, which is a good starting point for PTOs who want to build their own landscape.

Terrorist groups

- Attempts to change data and information to cause harm or fear
- Collection of data for use in planning or executing attacks

Neighbourhood and system activists

- Neighbour quarrels
- Protest groups against electromagnetic radiation from cell towers and wi-fi.

Espionage

- Attempts to obtain data and information without detection.

Corporate espionage and competition

- Attempts to obtain data and information without detection
- Attempts to create false information to alter public opinion.

Hackers

- Individuals looking for self-promotion and technological challenges
- Attempts to use customer infrastructure to attack other third parties.

Thieves and criminals

- Attempts to realise financial gains
  - through IT ransomware
  - through theft of goods (copper/electronics).

Employees

- Disgruntled Employees
  - Malicious actions
  - Discontent.
- Unfaithful employees (criminals)
  - Can use provided access and knowledge to seek personal financial gain.
- Accidental and unintended employee actions
  - Overconfident employees
  - Insufficient employee training
  - Rights not given using the principle of least privilege
  - Configuration errors.

Environmental influences

- Electromagnetic interference from nearby infrastructure.

Radio interference

- Other / stronger radio traffic on the same frequencies
- Deliberate jamming.

Impact assessment: For each of the main assets supporting the essential functions of the SuC, the ISS should provide the consequences of losing the asset's integrity, availability or confidentiality. Railway and public transport operators may add other criteria in the ISS that they judge important. For instance, Sporveien added on that list the 'Reputation' criterion.

It is important to note that detailed risk assessments often include an analysis in their impact assessment according to all seven FRs shown in TS 50701.

For railway and public transport operators, the angle of the assessment of the ISS should at least consider the impact on:

- Human health and safety
- Operational availability
- Financial stability.

TS 50701 gives guidelines for the qualitative impact assessment, which should be followed in the ISS tender documents. Unlike the detailed risk assessment, where quantification of the risk is mandatory, TS 50701 recommends, as a minimum, using a qualitative approach with at least four different categories (A to D), as set out in Figure 38.

Figure 38: Qualitative Impact Assessment example; source TS 50701

Impact	Human health and safety	Operational availability	Financial impact
A	One or several fatalities	Most of operations disturbed during more than 1 week	Could lead to organization bankrupt
B	Several severe or critical injuries	Most of operation disturbed between 1 day and 1 week. Important operation disturbed during more than 1 week	Impact in a significant way the organization annual budget {>10 % of revenue)
C	One severe injury or several injuries requiring hospitalization	Most of operation disturbed between 1 h and 1 day Important operation disturbed between 1 day and 1 week	Impact in a significant way the organization annual benefits.
D	One injury requiring hospitalization or several light injuries {not requiring any hopitalization)	Important operation disturbed less than 1 day.	Impact not visible on annual basis

Sporveien tender requirements used a semi-qualitative approach that provided guidelines based on their security risk management plan. Levels were defined on a scale from 1-5 (lowest to highest). For the 'confidentiality' criterion, the CBTC system needed to meet all confidentiality levels depending on the nature of data to be protected. The ranking was: 1: Public; 2: Internal; 3: Moderate; 4: Serious; 5 Very Serious. For the 'integrity' criterion, it specified that the CBTC system should meet a minimum integrity level of 3. The ranking was from 1 (the system can be compromised by external users for example, through the internet) to 4 (cannot be uncompromised). Level 3 was selected to strike a balance between the need for security while maintaining usability. For the 'Availability' criterion, Sporveien specified that unavailability was unacceptable (Level 4).

Sporveien specified that the use of lower levels could be proposed as long as they were described, documented and rationalised and would be subject to customer approval on a case-by-case evaluation.

Exposures: The ISS can also mention potential attack surfaces, which - by describing the source of risk - will support the likelihood assessment. For example, the Sporveien tender document described the following:

External hacking

- Gaining access to customer systems through internet-based services.

Internal hacking

- Gaining access to customer systems through the internal administrative infrastructure.

External infrastructure hacking

- Gaining access to customer systems through the external peripheral technical infrastructure.

Human interfaces

- External
- Previous employees
- Current employees (internal).

Vulnerabilities: These are usually linked to an already-implemented SuC, explaining probably why Sporveien didn't mention any vulnerabilities. Having said that, we recommend that the ISS provide a list of preliminary anticipated vulnerability for the SuC. The tender document can either be broad, for example describing key system components prone to security attack targeting, such as:

- Servers
- Workstations
- Gateways
- Telecommunications equipment
- Specialised equipment (to be specified).

It can also be a little more specific describing some of the functional requirements and interfaces of these components that could be vulnerable. On the other hand, the detailed security analysis must make an in-depth analysis and define the security requirements for providing adequate security protection. For example, below is a non-exhaustive list of likely vulnerabilities for a CBTC system:

- lack of identification and authentication mechanisms (for example, user identification)
- unprotected password tables, poor password management, unprotected connection to a workstation
- lack of identification and authentication of sender and receiver
- lack of security mechanisms in Windows-based machines
- disposal or reuse of storage media without proper erasure
- lack of security measures to prevent spoofing of train control commands over wireless link
- lack of security measures to prevent changing signal aspects.

Figure 39: Preliminary qualitative Impact Assessment for a CBTC; source Serge Van Themsche

CBTC Main assets	ASSET Availability				ASSET integrity				ASSET confidentiality			
	Human health & Safety	Operational Availability	Financial Stability	Impact Rating	Human health & Safety	Operational Availability	Financial Stability	Impact Rating	Human health & Safety	Operational Availability	Financial Stability	Impact Rating
ATO onboard	A	B	B	A	A	A	A	A	S	B	D	B
ATO wayside	A	A	A	A	A	A	A	A	A	A	D	A
ATP onboard	A	S	B	A	A	A	A	A	S	B	D	B
ATP wayside	A	A	A	A	A	A	A	A	A	A	D	A
ATS	D	A	A	S	A	A	A	A	S	S	C	B
Interlocking	A	A	A	A	A	A	A	A	A	A	D	A
Signals	A	B	B	A	A	A	A	A	A	A	D	A
Point machine	A	A	A	A	A	A	A	A	A	A	D	A
Driver machine interface	C	C	C	C	A	A	A	A	S	B	B	B
Radio base station	C	A	B	B	A	A	A	A	A	A	D	A
Wi-fi technology	A	A	A	A	A	A	A	A	A	A	D	A
Signaling screen in OCC	C	C	B	B	S	S	S	B	S	B	C	B
Others to be described	TSO	TSO	TSO	TBD	TSO	TBD	TSO	TBD	TSO	TBD	TBD	TBD
Cybersecurity solution e.g., SIEM	D	D	C	C	C	B	B	B	B	B	B	B
External to CBTC: e.g., PSD	S	B	C	S	A	A	A	A	S	B	D	B

In addition, even the most thoroughly protected of systems are vulnerable to misuse by attackers, when such as attackers reach into a target via a RAT and have acquired access to the systems through stolen credentials.

Likelihood assessment:

TS 50701 qualitatively addresses the likelihood of attacks in terms of the following criteria:

- Expertise level (EXP)
- Equipment Needed (EQP)
- Window of Opportunity (WOO)
- Time required (TIM).

It suggests four qualitative measures for these criteria, resulting in a likelihood of low to very high.

The ISS can use Table 40 to assess each main assets in a qualitative manner. However, it is also possible to perform a semi-quantitative approach at this stage, by using the system integrator's approach described in TS 50701's Annex E. The rating of each main asset is then obtained by the sum of the rated exposure and rated vulnerability.

It should be noted that TS 50701 recommends, for the preliminary risk assessment, to consider the worst-case result for each asset (the highest likelihood without any cybersecurity countermeasure) to determine the probability of the occurrence of a threat.

Figure 40: Likelihood assessment criteria: Source TS 50701

EXP	EQP	WOO	TIM	Likelihood
Multiple experts required	Bespoke equipment	Short	Long	**Low**
Expert	Specialised equipment	Moderate	Moderate	**Medium**
Proficient	Specialised COTS	Long	Short	**High**
Laity	Standard equipment	Unlimited	Very short	**Very high**

Figure 41: Likelihood assessment qualitative rating for a CBTC system; source Serge Van Themsche

CBTC Main assets	EXP	EQP	WOO	TIM	Likelihood Rating
ATO onboard	Multiple experts	Bespoke equipment	Short	Long	Low
ATO wayside	Multiple experts	Bespoke equipment	Short	Long	Low
ATP onboard	Multiple experts	Bespoke equipment	Short	Long	Low
ATP wayside	Multiple experts	Bespoke equipment	Short	Long	Low
ATS	Expert	Specialized equipment	Moderate	Moderate	Medium
Interlocking	Multiple experts	Bespoke equipment	Short	Long	Low
Signals	Expert	Specialized equipment	Moderate	Moderate	Medium
Point machine	Expert	Specialized equipment	Moderate	Moderate	Medium
Driver machine interface	Expert	Specialized equipment	Moderate	Moderate	Medium
Radio base station	Expert	Specialized equipment	Moderate	Moderate	Medium
Wi-fi technology	Proficient	Specialized COTS	Long	Short	High
Signaling screen in OCC	Proficient	Specialized COTS	Long	Short	High
Others to be described	TBD	TBD	TBD	TBD	TBD
Cybersecurity solution e.g., SIEM	Expert	Specialized COTS	Moderate	Long	Medium
External to CBTC: e.g., PSD	Expert	Specialized COTS	Moderate	Long	High

Risk evaluation:

The ISS should provide an initial risk evaluation performed for each main asset supporting the SuC's essential functions. This preliminary risk evaluation is characterised by the system definition considering the mission profile and the identified threat landscape, which is usually translated into a risk matrix in which the likelihood and the impact of the threats are related, as can be shown in figure 43.

To get to figure 43 results, it may be useful to describe the realisation of risks within the ISS documents. The extent of damage in each case depends upon the functionality supported by each subsystem as well as the effect on the functionality caused by the specific damage influence and impact.

The following list indicates how the risks above can be realised for each of the various system functions identified:

- Damage to system components
  - Prevent functioning
  - Cause improper functioning.
- Damage to database
  - Prevent access
  - Provide incorrect data.
- Damage to application programme functioning
  - Prevent functioning
  - Cause incorrect functioning of the programme
  - Provide incorrect data to the programme.
- Damage within telecommunications network
  - Prevent transport of messages
  - Update or change of messages during transport with incorrect data
  - Send messages with incorrect data (including masquerading as a legitimate user).
- Revelation of information on the network structure to aid in planning attack
  - Components, including operating systems, data base, applications and/or data structure
  - Connections, including topology and limitations
  - Users and credentials; security mechanisms and policies in effect.

The Figure below shows a very simple and easy-to-use risk matrix, which could be calibrated by the tender specifier to reflect a more conservative or optimistic approach to risk. The ISS document may provide also a semi-qualitative approach.

Figure 42: Risk matrix; adapted from TS 50701 by Serge Van Themsche

		Impact			
	Rating	D(Low)	C(Medium)	B(High)	A(VH)
Likelihood	Low	Low	Low	Medium	Significant
	Medium	Low	Medium	Significant	Significant
	High	Medium	Significant	Significant	High

Based on the risk matrix, the ISS must provide a preliminary risk evaluation relying on the average of the lost properties (the asset's availability, integrity and confidentiality) or the asset's most critical property lost. In the initial risk assessment, the risk ranking of the assets is determined by the risk matrix, because the evaluation is performed as a worst-case evaluation without any countermeasures, unlike the detailed risk evaluation.

The preliminary risk evaluation performed above shows that all main CBTC assets are considered to be significantly risky. This should not come as a surprise, as the inherent nature of these assets strongly correlate with safety and the catastrophic consequences that a successful attack would have on the PTO's financial position, operational stability and the health of its passengers.

The last phase of ZCR 2 is then to translate the qualitative risk evaluation into a security target for each asset. For example - and based on results pictured in figure 43 - all the main assets described above should have a maximum target security level, which according to TS 50701 should be 4 (SL-T =4).

Initial risk assessment: Partitioning of the CBTC (ZCR 3)

Based on the output of this Preliminary Risk Assessment, the assets should be assigned to consistent security zones, connected through conduits. It means that all assets in the same zone and all data flowing through the same conduit must share similar cybersecurity requirements.

Partitioning criteria: TS 50701 identifies eight pertinent cybersecurity requirements for PTOs, enabling the re-grouping of these assets into zones and conduits:

Risk of the assets, in terms of integrity, availability and confidentiality

- Type of interfaces or connections to the other parts of the SuC (for example, wireless)
- Physical or logical location
- Access requirements
- Operational function
- Organisational responsibilities for each asset
- Safety aspect (for example, security integrated levels)
- Technology lifecycle (for example, product lifecycle or obsolescence)

The objective of this partitioning is to identify assets that share cybersecurity requirements, which would enable implementing common coherent cybersecurity mitigation means. For the ISS tender document, the criteria 'risk, physical location and safety aspect' should at least be specified to break down the SuC into zones and conduits, and allow the vendors to provide the appropriate mitigation measures.

Figure 43: Preliminary risk evaluation of a CBTC System; Source Serge Van Themsche

Risk evaluation		Impact rating		
CBTC Main assets	Likelihood rating	Asset Avaliability	Asset Integrity	Asset Confident.
ATO onboard	Low	A	A	B
		Significant		
ATO wayside	Low	A	A	A
		Significant		
ATP onboard	Low	A	A	B
		Significant		
ATP wayside	Low	A	A	A
		Significant		
ATS	Medium	B	A	B
		Significant		
Interlocking	Low	A	A	A
		Significant		
Signals	Medium	A	A	A
		Significant		
Point machine	Medium	A	A	A
		Significant		
Driver machine interface	Medium	C	A	B
		Significant		
Radio base station	Medium	B	A	A
		Significant		
Wi-fi technology	High	A	A	A
		Significant		
Signaling screen in OCC	High	B	B	B
		Significant		
Others to be described	TBD	TDB	TDB	TDB
		Significant		
Cybersecurity solution e.g., SIEM	Medium	C	B	B
		Significant		
External to CBTC: e.g., PSD	High	B	A	A
		Significant		

Figure 44 goes beyond this, and provides some of the eight additional partitioning criteria. During the design phase, the selected vendor will finalise the breakdown of the SuC into zones and conduits, providing two levels of monitoring.

The first level is usually described as subnets, which is a macro-segmentation as shown in the figures above. Figure 45 shows a screenshot from a continuous monitoring system describing sub-nets of a CBTC System with finer granularity.

Readers should realise that the ultimate goal of this entire process is to provide vendors with the requirements to design a cybersecurity architecture that enables a DID strategy. Figure 45 provides a screenshot from a continuous monitoring system describing the final CBTC system segmentation per security zone, at the appropriate granularity level.

We will now describe how to write the specification to ensure that the selected vendors produce the right security zones during the design phase and apply the appropriate DID protection solutions.

So far, we have mainly focused on the SuC's zones and conduits without fully considering the global railway environment. However, Figure 36 reminds us that the SuC is not a closed environment, hence we must now consider the access to and from an asset to and from other subsystems. These dataflows cannot be achieved without designing the appropriate architecture.

This is where TS 50701 proves valuable, with its recommended communication matrix from wayside-to-wayside (Figure 47) and train-to-train (Figure 48) as well as between these two environments (Figure 49 and 50). This design must focus on Zone Criticality (ZC).

Zone Criticality: This represents the security demands - in a simplified expression - to define the communications allowed between zones.

Figure 44: Criteria for partitioning a CBTC System; source Serge Van Themsche

CBTC Main assets	Risk Availability	Risk Integrity	Risk Confident.	Interface	Location	Safety	Org. Responsible	Life cycle
ATO onboard	A	A	B	Wired	Onboard	SIL 4	Operations	15
ATO wayside	A	A	A	Wired	Track	SIL 4	Operations	15
ATP onboard	A	a	B	Wired	Onboard	SIL 4	Operations	15
ATP wayside	A	A	A	Wired	Track	SIL 4	Operations	15
ATS	B	A	B	Wired	OCC	SIL 2	OCC manager	10
Interlocking	A	A	A	Wired	Track	SIL 4	Operations	15
Signals	A	A	A	Wired	Track	SIL 4	Operations	30
Point machine	A	A	A	Wired	Track	SIL 4	Operations	30
Driver machine interface	C	A	B	Wired	Medium	SIL 2	Operations	15
Radio base station	B	A	A	Wireless	Track	SIL 4	Operations	15
Wi-fi technology	A	A	A	Wireless	Track	SIL 4	Operations	10
Signaling screen in OCC	B	B	B	Wired	OCC	SIL 0	OCC manager	10
Others to be described	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
Cybersecurity solution e.g., SIEM	C	B	B	Wired	OCC	SIL 0	CISO	5
External to CBTC: e.g., PSD	B	A	A	Wired	Track	SIL 3	Operations	15

Figure 45: CBTC Subnet segmentation as shown by a Continuous Monitoring System: Source Cylus;
The blue bubbles show the conduits and the grey bubbles shows the subnets (Zones at the macro level)

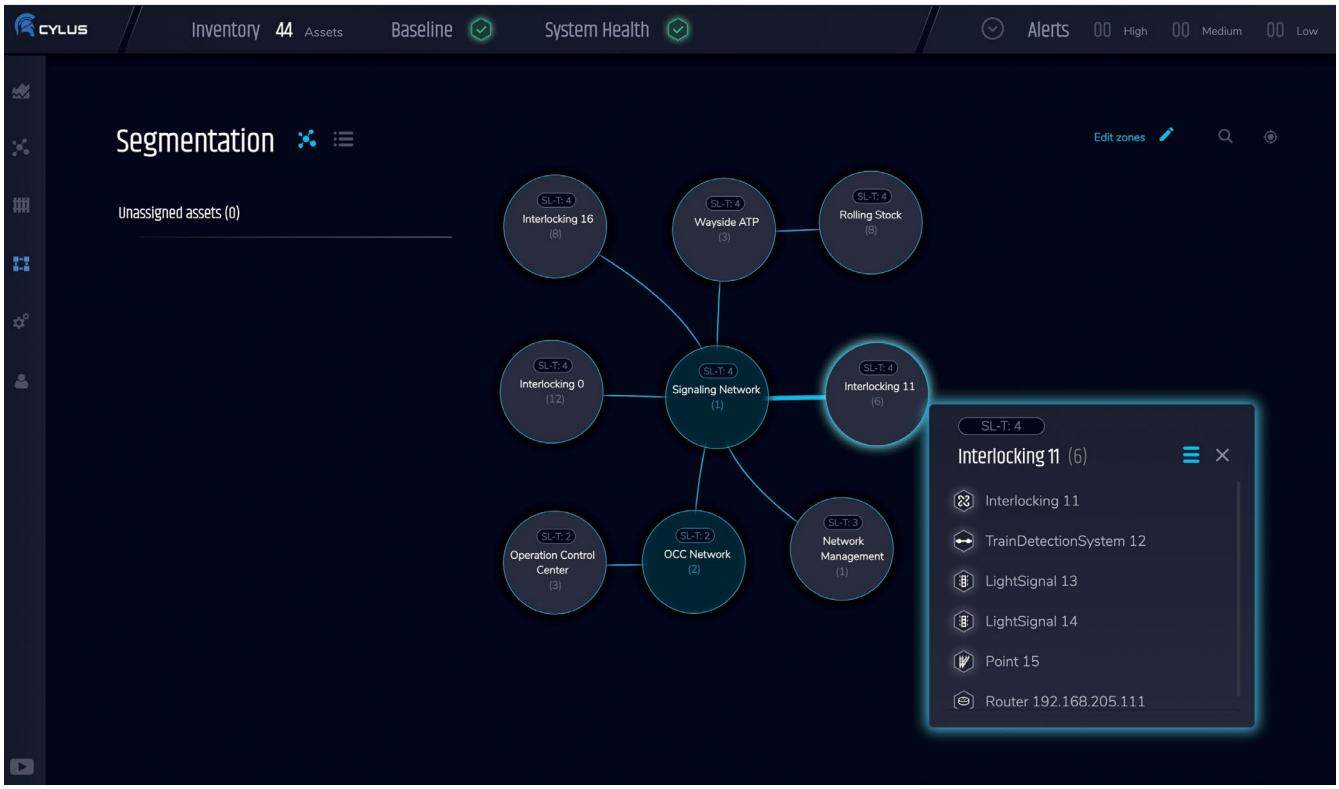
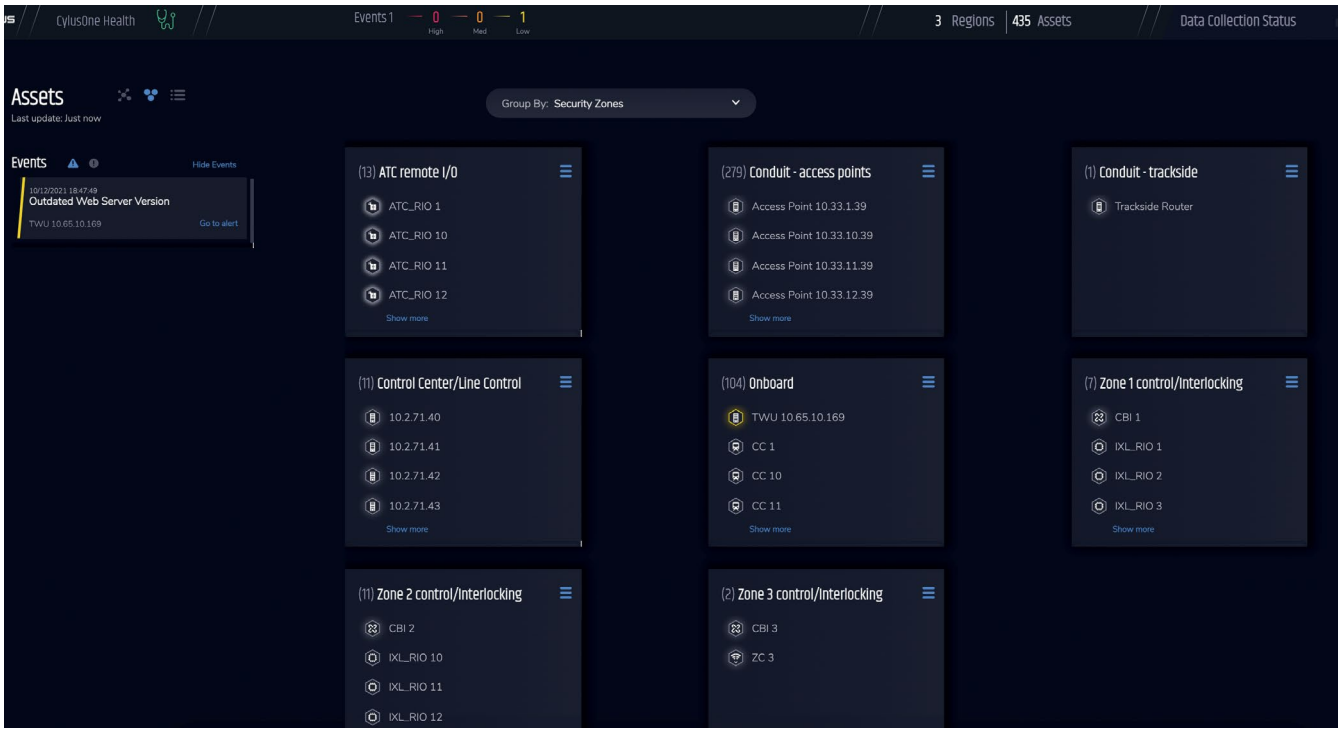


Figure 46: CBTC segmentation per security zones as shown by a Continuous Monitoring System: source Cylus



Zone Criticality for Landside (Wayside) – ZC-L: This defines the criticality of each zone in comparison to all other network zones in order to define communication rules at railway operator level (infrastructure manager) for signalling and fixed installation.

Zone Criticality for Rolling Stock – ZC-RS: This defines the criticality of each zone in comparison to all other network zones to define communication rules at railway operator level (railway undertaker) in the rolling stock environment.

TS 50701 gives some recommendations on how to design the dataflow. Step 1 is linked to this process we developed for the CBTC system.

- Each zone identified in the preliminary risk assessment should be classified according to its risk criticality.
  - We have seen that – in the case of CBTC assets - it is classified as 'significant' (SL-T = 4).
- Direct communication between zones with well-known risks and unknown risks should be refused (for example, zones with well-known and fixed mounted OT devices directly communicating with for example, office zones with laptops, printer, internet connectivity).
- Direct communication is only allowed between zones with the same or a subsequent zone criticality.

In Step 2, the specifier should define the criticality of the zones ZC-L and ZC-RS, as the CBTC assets are installed within these two environments.

- The number of zones and criticality levels can be chosen individually by the railway operator or infrastructure manager, but should be identical for their entire infrastructure. In the TS 50701 example, six plus one zone criticality levels are defined (ZC-L 5s to 0).

We recommend following the TS 50701 examples of breakdown, which is illustrated in Figures 47 to 50, adapting it to the PTO's specific requirements.

Step 3 requires establishing the communication matrix, according to the results of Steps 1 and 2. We recommend following the TS 50701 examples of communication matrix, adapting it to the specific requirements of the PTO. Furthermore, to establish where another SuC fits within this matrix (for example, PIS, Ticketing system, ERP system.), we recommend using the following rule of thumb, linked to the network to which the SuC's asset is connected:

- SCN: Safety-critical network: ZCL-5s or ZCL-5; ZCRS-5s or ZCRS-5.
- OCN: Operational Communication Network: ZCL-5 or ZCL-4; ZCRS-5 or ZCRS-4.
- ACN: Administrative Communication Network: ZCL-4 or ZCL-3; ZCRS-4 or ZCRS-3.
- External DMZ, gateway area: ZCL-2; ZCRS-2.
- External link to a third-party network (for example, partner, cloud provider): ZCL-1; ZCRS-1.
  - Whatever their own network criticality (for example, connection to a third-party OCN network that would be rated WCL-4)
- Direct internet link: ZCL-0; ZCRS-0.

Figure 47: Zone criticality and communication matrix from wayside to wayside: Source TS 50701, adapted by Serge Van Themsche

			Zone criticality	Safety (CBTC), HV Power	SCADA, Central ICS	Datacenter, int DMZ, ICS/autom.	Corporate network	Gateway area, ext DMZ	External partner / Companies	Internet
			Security maturity	Highly Secure Safety	Highly Secure Critical	Secure	Medium	Low	Low	Untrusted
		FROM	TO	ZC-L 5s	ZC-L 5	ZC-L 4	ZC-L 3	ZC-L 2	ZC-L 1	ZC-L 0
Zone criticality	Security maturity	SuCs								
ZC-L 5s	Highly Secure Safety	Safety (CBTC), HV Power		Allowed	Restricted	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
ZC-L 5	Highly Secure Critical	SCADA, Central ICS		Allowed	Allowed	Restricted	Prohibited	Prohibited	Prohibited	Prohibited
ZC-L 4	Secure	Datacenter, int DMZ, ICS/ automation		Prohibited	Allowed	Allowed	Allowed	Prohibited	Prohibited	Prohibited
ZC-L 3	Medium	Corporate network		Prohibited	Prohibited	Allowed	Allowed	Allowed	Allowed	Prohibited
ZC-L 2	Low	Gateway area, ext DMZ		Prohibited	Prohibited	Prohibited	Allowed	Allowed	Prohibited	Allowed
ZC-L 1	Low	External partner / Companies		Prohibited	Prohibited	Prohibited	Allowed	Prohibited	Allowed	Prohibited
ZC-L 0	Untrusted	Internet		Prohibited	Prohibited	Prohibited	Prohibited	Prohibited	Allowed	Allowed

Figure 48: Zone criticality and communication matrix, from rolling stock to rolling stock: Source TS 50701, adapted by Serge Van Themsche

			Zone criticality	CBTC (ATP/ATO)	Command & Control	Auxiliary	Comfort	Public interface	External Com Channel
			Security maturity	Highly Secure Safety	Secure	Medium	Low	Low	Untrusted
		FROM	TO	ZC-RS 5	ZC-RS 4	ZC-RS 3	ZC-RS 2	ZC-RS 1	ZC-RS 0
Zone criticality	Security maturity	SuCs							
ZC-RS 5	Highly Secure Safety	CBTC (ATP/ATO)		Allowed	Allowed	Prohibited	Prohibited	Prohibited	Allowed
ZC-RS 4	Secure	Cmd&Control: TCMS, DCU, Breaking Sys		Allowed	Allowed	Allowed	Allowed	Restricted	Allowed
ZC-RS 3	Medium	Auxiliary: CCTV, Autodiagnostic		Prohibited	Allowed	Allowed	Allowed	Restricted	Allowed
ZC-RS 2	Low	Comfort: PIS, HVAC		Prohibited	Prohibited	Allowed	Allowed	Restricted	Allowed
ZC-RS 1	Low	Public interface: Entertainment, Wi-Fi		Prohibited	Prohibited	Prohibited	Prohibited	Allowed	Allowed
ZC-RS 0	Untrusted	External Com channel: T-to-wayside, T-to-T		Prohibited	Allowed	Allowed	Allowed	Allowed	Allowed

Figure 49: Zone criticality and communication matrix, from rolling stock to wayside: Source TS 50701, adapted by Serge Van Themsche

			Safety (CBTC), HV Power	SCADA, Central ICS	Datacenter, int DMZ, ICS/autom.	Corporate network	Gateway area, ext DMZ	External partner / Companies	Internet
			Highly Secure Safety	Highly Secure Critical	Secure	Medium	Low	Low	Untrusted
		FROM	ZC-L 5s	ZC-L 5	ZC-L 4	ZC-L 3	ZC-L 2	ZC-L 1	ZC-L 0
Zone criticality	Security maturity	SuCs							
ZC-RS 5	Highly Secure Safety	CBTC (ATP/ATO)	Allowed	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
ZC-RS 4	Secure	Cmd&Control: TCMS, DCU, Breaking Sys	Prohibited	Prohibited	Prohibited	Allowed	Prohibited	Prohibited	Prohibited
ZC-RS 3	Medium	Auxiliary: CCTV, Autodiagnostic	Prohibited	Prohibited	Prohibited	Allowed	Prohibited	Prohibited	Prohibited
ZC-RS 2	Low	Comfort: PIS, HVAC	Prohibited	Prohibited	Prohibited	Allowed	Prohibited	Prohibited	Prohibited
ZC-RS 1	Low	Public interface: Entertainment, Wi-Fi	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited	Allowed	Allowed
ZC-RS 0	Untrusted	External Com channel: T-to-wayside, T-to-T	Prohibited	Prohibited	Prohibited	Allowed (tech DMZ)	Prohibited	Prohibited	Allowed

Figure 50: Zone criticality and communication matrix, from wayside to rolling stock: Source TS 50701, adapted by Serge Van Themsche

			Zone criticality	CBTC (ATP/ATO)	Command & Control	Auxiliary	Comfort	Public interface	External Com Channel
			Security maturity	Highly Secure Safety	Secure	Medium	Low	Low	Untrusted
		FROM	TO	ZC-RS 5	ZC-RS 4	ZC-RS 3	ZC-RS 2	ZC-RS 1	ZC-RS 0
Zone criticality	Security maturity	SuCs							
ZC-L 5s	Highly Secure Safety	Safety (CBTC), HV Power		Allowed	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
ZC-L 5	Highly Secure Critical	SCADA, Central ICS		Prohibited	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
ZC-L 4	Secure	Datacenter, int DMZ, ICS/ automation		Prohibited	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
ZC-L 3	Medium	Corporate network		Prohibited	Allowed	Allowed	Allowed	Prohibited	Allowed (tech DMZ)
ZC-L 2	Low	Gateway area, ext DMZ		Prohibited	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
ZC-L 1	Low	External partner / Companies		Prohibited	Prohibited	Prohibited	Prohibited	Allowed	Prohibited
ZC-L 0	Untrusted	Internet		Prohibited	Prohibited	Prohibited	Prohibited	Allowed	Allowed

Creating the security zones:

Now we need to conciliate all elements in order to propose a segmentation according to security zones, along with the cybersecurity means to enforce that segmentation. The reader should realise that there is no perfect segmentation, and that ultimately the partitioning should reflect what can be enforced through technologies, policies and procedures. The recommended segmentation should also be manageable; applying an excessive amount of partitioning rules could rapidly overwhelm the cybersecurity team, making rapid updates impossible and creating loopholes that are potentially exploitable by cyber criminals.

We will start by pointing out that creating security zones according to subnets is not best practice. A subnet is a logical subdivision of an IP network. Assets that belong to the same subnet are addressed with an almost identical IP number. Splitting a large railway network into smaller subnetworks helps minimise traffic flow between routes, thus increasing network speed. Even although subnetting can assist security by quarantining compromised network sections and making it potentially more difficult to move around the railway's IP network, it cannot be considered a security partitioning criterion (and isn't indicated as such in TS 50701). Subnetting is primarily an administrative approach to partitioning the network. To provide an example, the IT department that gives and manages the IP addresses could decide to allow IP addresses in function of a location (for example, a metro station). Any assets, irrespective of their security level (for example, an IP camera and an access control) located in that station, would be allowed to communicate with each other. Obviously, one could say that no IT administrator would create a unique subnet per station, authorising, for example, a camera to communicate with an interlocking located in this same station. However, the point is that even-more intelligent segmentation based on subnets would become very quickly extremely complicated to manage. Hence, security rules based on subnets should be avoided.

The railway cyber-architectural team should focus on some of the eight partitioning criteria established in TS 50701. Segmentation based on all these criteria is hard to implement, particularly if the team doesn't dispose of a specific railway monitoring system, that automatically integrates partitioning criteria and predefines the zones. However, an SuC as complicated as a CBTC should rely on micro-segmentation enabling East-West and North-South segmentation (see 'Continuous Monitoring' hereafter). Figure 46 provides a good example on ways of creating these security zones. Hence a possible segmentation for a CBTC system could be:

- Interlocking:
  - One security zone per zone controller
    - With its field elements (for example, signals, point machines).

- Wayside ATC, which could be further broken down according to:
  - Wayside ATO
  - Wayside ATP.
- Control centre/line controller
  - ATS and other servers (for example, NMS).
- Conduits
  - Access points
  - Trackside routers
  - Train to wayside.
- Onboard ATC
  - Onboard ATO
  - Onboard ATP.
- Onboard Driver interface
- Platform Screen Doors

Implementing the segmentation: The next step in this process is to provide the means to partition the SuC. This can be done physically or virtually, with the possibility of enforcing the partition or just creating rules, with an alarm being triggered whenever the segmentation rules are broken.

Physical enforcement:

Unidirectional gateways are the only way to ensure that a dataflow will not flow back from a lower criticality zone. This capability will remain valid indefinitely, even if the malevolent capabilities of the malware were to evolve exponentially. Hence it is highly recommended that railway and public transport operators implement at least one unidirectional gateway in order to physically separate their OT and IT networks. In the event of a successful attack on their IT system, the railway's cybersecurity team will not have to cease critical operations and will retain the freedom of mind to focus resources on the IT attack.

It should be noted that the four communication matrices (Figures 47-50) are examples taken from TS 50701. These indicate what is ideally allowed, restricted or prohibited, based on common sense and business practices. For example, a priori it doesn't appear to make sense to connect the CBTC to an untrusted network through the internet (ZC-L5s to/from ZC-L0). However, supposing that the CBTC predictive maintenance is done at the depot, and that the operational team needs a connection between the CBTC network and the maintenance servers, it would be tolerated (restricted) as long as secure dataflow measures are taken (a unidirectional gateway) to transfer data from the CBTC (SIL 4) to the maintenance site (SIL 0). In fact, TS 50701 recognises such situation and indicates that:

- Direct (maintenance) access from business zones to control zones without control by a security device (for example, unidirectional gateway) or similar (for example, proxy server) should not be allowed.
- External maintenance access (for example, via the internet) should be grouped in a separate zone.

Hence, we recommend that deviations from the TS 50701 communication matrix examples (Figure 47-50) consider a unidirectional gateway. Whenever bidirectional communication is mandatory, HTTPS proxy servers may be envisioned, but with extra care. However, cybersecurity network designers should always question the need for constant bidirectional communication between zones of differing safety levels. Where the zone with the lowest security level must communicate, but only sporadically (for example, once a week for maintenance updates), unidirectional gateways offering dataflow flipping functionality can be envisioned.

Proxy servers: on top of privacy benefits, newer-generations of proxy servers provide some security protections. They can encrypt web requests to keep prying eyes from easily reading transactions or stealing web credentials. They can also prevent known malware sites from any access through the proxy server. Additionally, railway and public transport operators can couple their proxy server with a VPN, so that remote users always access the internet through the company's proxy. By combining this with a VPN, the railways can create a tunnel - which is a controlled conduit that verifies that users have access to the required resources (such as email or internal data), while also providing a reasonably secure connection. However, it should be noted a combination of newer-generation proxy servers using a VPN can still be attacked (for example through dynamic content attacks or SSL-based DDoS attacks).

Firewalls

Unlike unidirectional gateways, which physically block the dataflow, or a combination of VPN and proxy servers that encrypt and tunnel it, firewalls segment the network according to predefined rules by allowing or blocking different types of traffic. For instance, firewall rules can restrict access to a network zone, of messages coming from machines with certain logged in user profiles or running certain types of applications. It can also block certain types of traffic from crossing the boundary between two network segments.

Firewalls with different types of bundled capabilities tend to be called different things by their marketing teams. 'Stateful firewalls' is a widely-used term to describe firewalls that track connections in progress and treat those packets that appear to be part of a connection differently. 'Unified Threat Managers' (UTM) is a term often applied to firewalls with built-in intrusion detection, intrusion prevention and antivirus capabilities. 'Next Generation Firewalls' (NGFW) is a term generally applied to firewalls that coordinate with active directory servers to understand who is logged into which computers. They also have a deep understanding of some communications protocols - particularly web-based protocols - to allow users to create rules that, to a large extent, control what kinds of operations different users can carry out within specific web or cloud applications. The term 'Data Centre Firewall' (DCFW) is generally applied to a firewall with the extra throughput required to manage the high traffic volumes seen in large data centre applications.

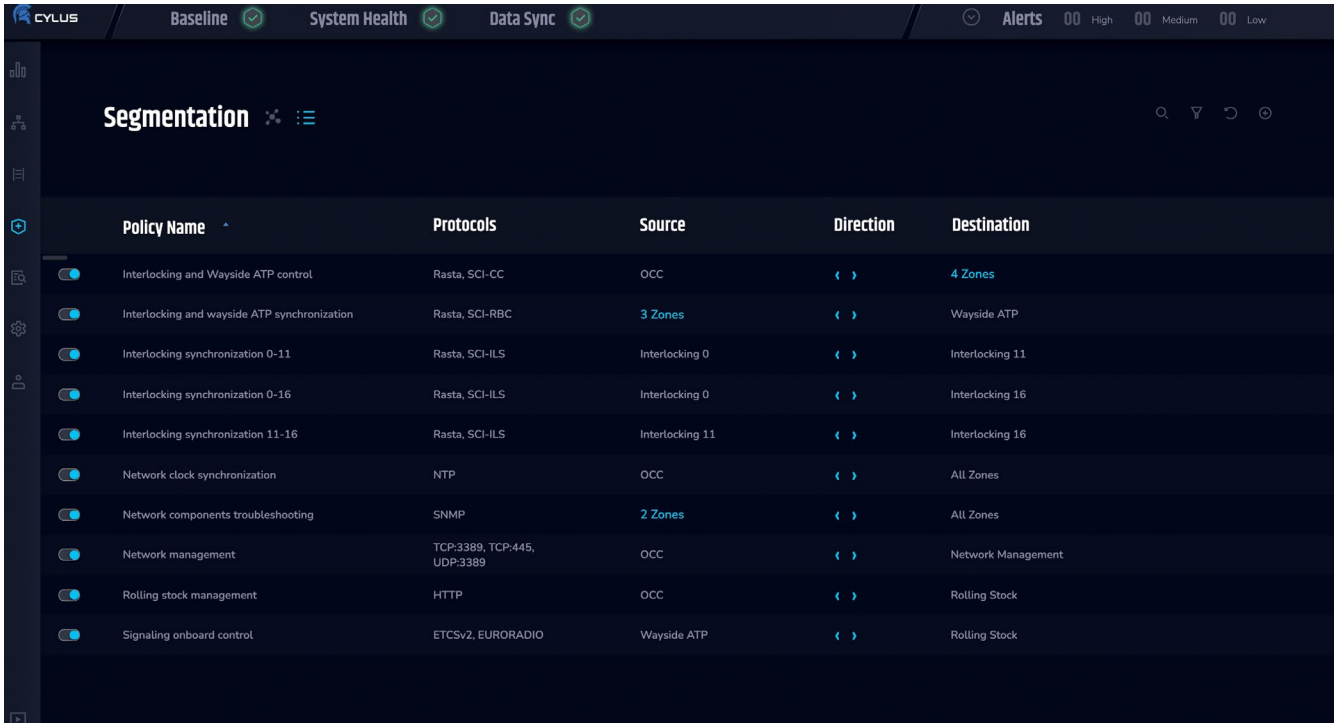
Although these firewall technologies offer different kinds of features, they still maintain primarily what is called 'North-South' protection and segmentation. In other words, they are generally deployed to protect and segment from the outside – in.

The term 'Internal Segmentation Firewall' (ISFW) is sometimes used to account for what are called 'East-West' attacks to bring about 'micro-segmentation' within an IP network. ISFWs generally encode application-level knowledge (Level 7 of the OSI stack) exclusively of protocols common in IT environments. This makes most ISFW of limited use in safety-critical networks such as a CBTC, which use non-IT protocols at the application Level (Level 6 and 7 of the OSI Stack). Furthermore, any active device - such as a firewall - deployed between safety-critical components would need to be part of the safety case, making frequent firewall firmware updates difficult to manage.

Enforcement though alarm triggering: All assets running in a safety critical network such as a CBTC must be approved and described in the safety case, according to IEC 50126. As continuous monitoring systems are passive (that is to say they gain access to the networks via taps or port mirroring), they do not affect the safety case. Railway-specific continuous monitoring systems that integrate DPI capability can read and understand the specific encapsulated messages at all layers of the OSI stack for many protocols used in railway systems. Hence rail-specific monitoring systems can be used to enable logical segmentation according to rail system application rules applied between zones. These systems sometimes also provide two types of virtual segmentation; macro (with rules controlling dataflow between zones) and micro (with rules controlling dataflow between assets or zones at the OSI layer). Any abnormal flow generated by connections breaking such rules will generate alarms, creating awareness of the state of even safety-critical networks.

Figure 51 gives an example of the outcome for a signalling system resulting from the work that presented above.

Figure 51: Example of a Segmentation with virtual enforcement of zones and conduits of a signalling system, via alarm triggering: Source Cylus



Specifying the minimum cyber protection requirements

The next step of this process is to establish the minimum cybersecurity protection that - in the views of the specifier - will not only protect against the anticipated threats and envisioned vulnerabilities (as developed in the previous sections of this example) but will also enforce this segmentation. It should be understood that other solutions may have to be considered, depending on the final architecture of the SuC proposed by the vendor. Hence, the responsibility for the final architecture and design shall remain with the selected vendor.

DID: We cannot overemphasise the need for adopting the DID strategy. Section 6 describes various cybersecurity technologies that must be considered for generating such progressive barrier mechanisms, introducing them through the seven FR classes:

- FR1: Identification and authentication control
- FR2: Use control
- FR3: System integrity
- FR4: Data Confidentiality
- FR5: Restricted data flow
- FR6: Time Response to Events
- FR7: Resource Availability

Depending on the cybersecurity solutions already implemented in the rail environment, the ISS should specify whether the contractor must deliver and potentially maintain the solution, or if they should only ensure that the proposed cybersecurity solutions are compatible with the existing IT/OT infrastructure.

The first element the contractor must establish is a continuous monitoring system that will enable the management of all CBTC assets.

Asset management:

As we described, asset inventory is a critical component of the foundation of cybersecurity operations in public transport operations. Without it, no real cyber protection is possible for an SuC. For a simple SuC, a list of assets, updated manually from time to time, is manageable. However, for complex OT SuCs, manual updates quickly become unfeasible. Hence, railway and public transport operators should consider solutions that continuously monitor their network, identifying in real time all assets running on their networks. We strongly recommend that the public transport operators consider continuous monitoring systems that are adapted to their specific rail environment. Indeed, these rail-specific continuous monitoring systems can automatically identify and update, in real time, the thousands of assets running on their CBTC network or other OT networks.

Security Solutions to consider:

A DID strategy requires the use of myriad security mechanisms that have already been described in Section 6. The ISS document can be descriptive, and indicate what these solutions are and their specific adaptation to the SuC. Alternatively, it can just indicate what are the protections to consider and let the contractor describe what factors were considered and how they are incorporated in the project delivery.

Sporveien adopted a mix of both strategies. Its ISS document provides a list of security mechanisms for the vendors to consider in their offer:

- Firewalls: Controlling network sources, targets and ports. Establishing zone structure and controlling which protected targets are exposed to connections and traffic and information arriving from other networks.
- VPN: Establishing encrypted tunnels for traffic passing through networks not controlled by Customer.
- VLAN: Using a VLAN to separate network traffic.
- Strong password and two-factor authentication: Requiring not only strong password but also a physical device (such as a smartphone or code calculator).
- Antivirus: Detecting threats on computers.
- Updates (OS/Application): Securing and fixing known vulnerabilities.
- Secure physical devices: Reducing attack possibilities.
- Backup: Securing a working environment to restore.
- Monitoring: Proactivity, being in front.
- Education (Social engineering / phishing): No technical measures will stop people from doing things they shouldn't.
- Preventing rogue software: Using unapproved software may be a threat.
- IPS/IDS: Detecting and preventing threats in the network.
- Encrypting data at rest: Securing data if media, device or PC is lost.
- Classification: Securing what is worth securing.

Network Access Control (NAC): Maintaining control of connected devices and connection attempts.

- Spectrum analyser: Maintaining control over radio traffic and frequencies
- Logging: Centralising logging with a management GUI for event control and troubleshooting.
- Remote Access Systems: Designing all remote access systems using current best practices and industry standards
- External media access: Reducing and removing - where possible - the use of USBs, CD-ROMs / DVD-ROMs, unused RJ45, memory card readers and similar minimises the potential risk of importing malware into the system.

This list is followed by mandatory functionalities that the vendor must cover in its offer. Hence it gives the vendor the choice of selecting the best cyber technology while still allowing them to propose cybersecurity solutions better adapted to the DID protection of their specific CBTC technology.

Mandatory functionalities:

For example, Sporveien specified that the Contractor should provide a detailed documentation of the OT-infrastructure, to give customer insight in how the system is installed and an overview of all dependencies related to the system.

The ISS document described the principles that should govern the interface between the CBTC system and other types of subsystems, as well as all mandatory user access management features. It required that the CBTC system supports user identification to all configuration between client and host servers. It imposed the use of a central log system and time system (NTP server). The CBTC system needed to support a central monitoring solution of its assets for all security breaches. It also specified the need to be fully compatible with a NAC. Finally, it required that the CBTC system support a central monitoring solution for the OT infrastructure, the solution being required to alert when anomalies are detected and provide relevant information for troubleshooting, relying on a baseline.

The above mandatory functionalities were in fact more detailed in the ISS document, to ensure a level playing field among the qualified vendors. Although the reader can adopt the same strategy as Sporveien, we recommend following the TS 50701 tender process as described in Section 6. This will allow a more holistic approach and avoid missing important functionalities.

Making sure that the ISS is complete

The last touch to the CBTC ISS tender document enforces that the selected vendor will have to consider:

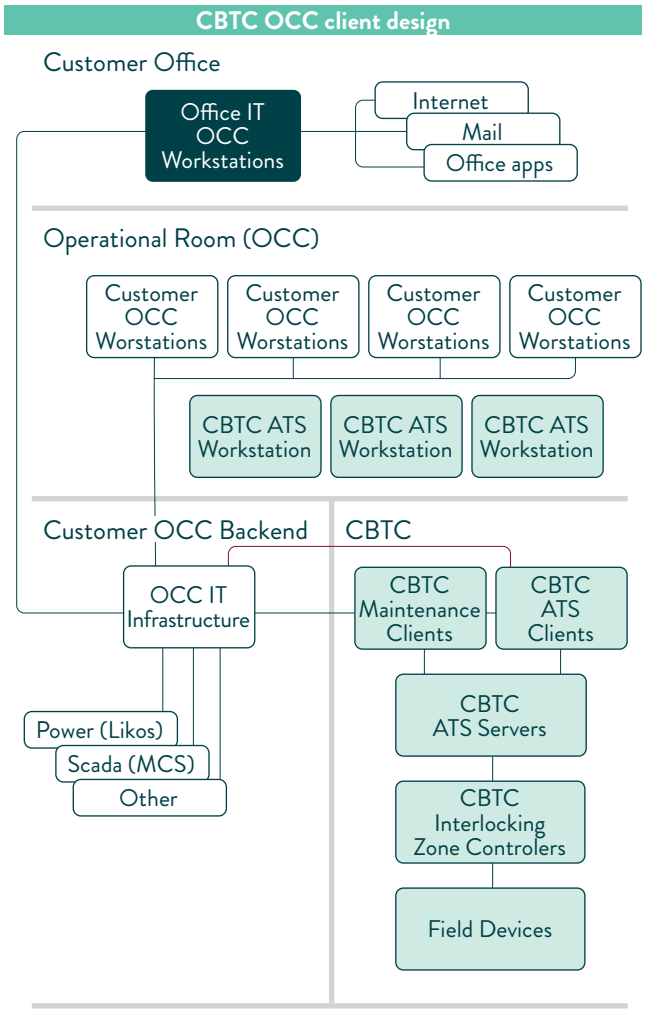
- The regulatory framework for the SuC and its cybersecurity protection (as per section 3).
- Appropriate standards for the SuC and its cybersecurity protection (as per section 3).
  - For example, Sporveien specifies that the contractor should ensure that all development, implementation and maintenance of the system delivery is performed in accordance with current (that is in 2019) relevant industry standards, such as:
  - NIST SP800-82 Revision 2(/20./)
  - IEC62443 series (/21./)
  - EN50126:2017(/22./,/23./),EN50128:2011(/24./), EN50129:2018(/25./), EN50159:2010(/12./)
  - ISO 27k family
  - OWASP
  - Nowadays, Sporveien would probably have added TS 50701.
- Deliverables of Section 4 to be completed during the design phase and before the SuC's commissioning (as per Section 4)
  - SuC's main asset obsolescence management detailed mapping, potentially with a SBOM.
  - Security by design policies and procedures.
  - Design level of maturity to be requested and homologated according to IEC 62443.
- Best cybersecurity practices as identified in Section 5
  - Security training
  - Security Administration
  - Security procedures and policies
  - Security risk management plan per subsystem
  - Cyber security testbed and modelling policies
  - Cybersecurity assurance during integration and validation activities
  - System Security Requirements and Foundational Classes
  - Defence-in-Depth protection strategy
  - Detailed Risk Assessment
  - Cybersecurity Case.

Other potentially relevant information

The specifications should ensure that the SuC's environment is well understood by vendors. In the case of Sporveien, all IT infrastructure supporting the SuC was part of the deliverables. The specification stressed that, in addition to the RFQ compliant/not compliant responses, the vendors' solution would be evaluated on the IT Security, robustness, flexibility and futureproofing. In such a tender, the contractor needed to deliver all IT infrastructure for the CBTC system delivery, including CBTC ATS workstations and the required peripherals for the OCC and a Back-up Control Centre. We will not detail what needs to be specified, since it is outside the scope of this report, but below is a list of relevant topics taken from the Sporveien tender documents.

- **OCC workplace:** The following drawing provided by Sporveien as an example of OCC design with CBTC, shows the contractor's deliverables in green boxes.

Figure 52: CBTC OCC Client design: Sporveien Technical requirement specifications



- **Virtual Machine hardware:** Servers should run virtualised.

Server software and operating system: Software should be supported by an SLA.

Redundancy: The vendor should design and build the SuC with redundancy in mind, enabling the adequate level of availability, maintainability and reliability as well as the actual and perceived uptime. Usually for a CBTC system, redundancy is required at the application level and across two geo-redundant sites (for example, OCC and BCC).

Scalability: IT infrastructure services should be able to scale in/out and up/down without impacting peration.

Core network: This should be based on IEEE 802.3 standard.(/11./).

- The SuC should support logical (VRF and VLAN) and micro (for example SDN) segmentation
- It should support customer or third-party devices in the network infrastructure for monitoring and analysing network traffic.
- It should support real-time mirroring of all network traffic, or a subset of it.
- It should have a function to physically isolate the signalling system from other systems and networks while maintaining safety and a high degree of operational awareness and operational performance.
- Isolation is used in the event of major external disturbance, for example, broadcast storm, DDOS or IT security breaches.

- **IP address:** Only IP addresses delivered from Customer IT department should be used.
- **Hardware:** All standardised x86 server hardware, networking equipment and other standardised components should be based on Commercial Of The Shelf (COTS) hardware, and run with a support agreement from the vendor.
- **Patch management:** Critical updates should be tested, verified and deployed within seven days following the updates release.
- **Identity management:** Specifies how user and access management shall be undertaken.
- **Monitoring:** All IT infrastructure services in the solution should be monitored through a central monitoring solution - provided by the contractor for maintenance purposes -that provides statuses, warnings and alarms.

- The contractor should support and provide a solution for forwarding these logs to a customer's central monitoring solutions

- **Network management:** All IT infrastructure services and devices in the solution should be managed from a central management tool.
- **Use of Sporveien IT infrastructure:** This describes what is allowed and what is forbidden.
- **Transmission:** The contractor shall design, engineer and supply a transmission system with the required RAM according to relevant requirements, as part of the system delivery.

ANNEX 3: SURVEY REPORT

A questionnaire has been sent to public transport operators to collect the solutions and best practices applied by operators on IT and OT transport technologies.

It is clear that cybersecurity is becoming a top priority for both national states and authorities, which are expanding the minimum requirement inserted in the tender for the management of transport asset. Consequently, public transport operators are improving their maturity on cybersecurity, adding a new management system that need to be properly addressed.

The report relies on data provided by seven public transport operators.

City	Country	Company
London	England	TFL (Transport For London)
Amsterdam	Netherland	GVB (Gemeentelijk Vervoer Bedrijf)
Augsburg	Germany	Stadtwerke Augsburg
Rome	Italy	ATAC
Berlin	Germany	BVG
Rio de Janeiro	Brazil	Metro de Rio de Janeiro

The data were collected during 2020-21.

Below are the questions submitted and a summary of the answers received.

1. Does your contracting authority (for example, the municipality or national government) define cybersecurity requirement for your company?

Obligations on cybersecurity are usually not reported explicitly on operation and maintenance contracts. However, most of the public transport operators consider national cybersecurity law as part of the responsibility of the operation duty.

Deployment of a cybersecurity management system is a very complex and costly set of process and procedures.

It is important that the operation and maintenance agreement between PTA and PTO clearly identifies requirements for cybersecurity.

2. Does your company provide cybersecurity requirements in the tenders?

All the interviewed companies provide cybersecurity requirements on tenders, demonstrating that the topic is no more considered an optional issue to be addressed.

3. Does your company provide data protection requirements in the tenders?

All the interviewed companies provide data protection requirements on tenders. In this case, the GDPR, published in 2016, provided focus on the importance of personal data managed by operators.

4. Does your company mention normative reference about cybersecurity in the tenders?

5. If yes, which is/are mentioned (for example, IEC 62443, NIST, 27001, TS50701, etc..)?

Although normative reference are commonly reported on tenders, there is no uniformity on the answers. The regulation scenario on cybersecurity is indeed complex.

In the present document, there is an in-depth description of regulations and standards.

6. Does your company provide specific cybersecurity requirements concerning:

a. Requirements on network access control / identity management & authentication?

b. Requirements on patch management?

c. Requirements on asset management?

d. Requirements on antivirus? (more generally endpoint protection)

e. Requirements on network segregation?

f. Secure coding or secure design ?

Most of the public transport operators interviewed provided all of those requirements.

In the present document, we provide a wide report on cybersecurity requirements that should be taken in consideration before tendering IT/OT technologies.

7. Does your company define the lifecycle of the system in the tenders:

a. Scheduling update for software and hardware?

b. Defining support for the whole lifecycle of the system from the supplier?

Most of the public transport operators interviewed define the lifecycle of the system in tenders.

The growth of IT components in the operational environment is increasing the need to review existing maintenance policy and procedures.

Preventive obsolescence management is often preferable to reactive obsolescence management.

8. Does your company include professional cybersecurity service in the tenders?

a. Cybersecurity risk management?

b. Security operation centre management?

c. Periodic vulnerability and risk assessment?

d. Periodic penetration test?

e. Data security and privacy services?

f. Business continuity services?

Some PTOs include professional cybersecurity service in tenders.

Having cybersecurity skills on operation environment is increasingly important, and often operators are not large enough to have such resources available internally.

Most of the company perform periodic vulnerability assessments and penetration tests.

Concerning the question on Security Operation Centre and business continuity Centre, the companies answered that they are commonly implemented in their rail operation, and could offer a rapidly deployable solution in order to improve cybersecurity protection.

In conclusion, the completeness of considerations emerged from the survey indicates that the issue - despite being a relatively new topic - has been discussed in depth and analysed by transport companies.

Even although it is difficult to extract a simple rule from the answers received by the panel, the considerations offer an interesting approach for engineers at all levels. It suggests that general principles could be derived to meet the needs of specific operating environments.

Technology for all aspects

of the public transportation environment

Actionable intelligence to drive better decisions

By combining high-quality video and audio solutions with intelligent analytics, the IP camera becomes the ultimate sensor, giving public transit agencies the ability to provide better business intelligence, help improve passenger experience and drive operational efficiency.

For more information, visit www.axis.com/public-transport

AXIS COMMUNICATIONS

CYLUS

The Leader in Railway Cybersecurity

Delivering visibility, resilience, and compliance, with a non-intrusive rail cybersecurity solution for rolling stock and trackside

Enable Asset Visibility

Improve Service Availability and Safety

Ensure Compliance

Address Staffing and Expertise Gap

Learn more at **cylus.com**

Certified according to ISO/IEC 27001:2017.

Complex solutions for operations control and fare management – like the ones offered by INIT – require the exchange of diversified data between user and supplier, e.g. driver data, networks data, operational data or customer data. This concerns implementation, operations and maintenance activities. Such sensitive information can cause serious damage when data is stolen or used in an impermissible manner. Having INIT as an ISO/IEC 27001:2017 certified partner assures public transport companies that the internal processes and guidelines for dealing with data and systems can be considered state-of-the-art. This is especially important because transportation, including public transport, is generally regarded as one of the critical infrastructure sectors in many cases.

> *We have reached a stage where it is no longer just a question of whether a company will become the victim of cyberattacks but of when it will happen. And the better a company is prepared for this kind of threat, the less grave the consequences will be. Our ISO 27001 certification greatly helps our customers and interested parties to have peace of mind as they know they have a reliable partner by their side who can deliver cutting-edge data and information security. By adopting the ISO standard and by committing to continuously improve in this field, we will be able to ensure that public transport is safer and more secure from cyberattacks."*
>
> Achim Becker, Managing Director INIT GmbH

init
The Future of Mobility

www.initse.com | INIT Group

waterfall-security.com

WATERFALL®
Stronger Than Firewalls

TS 50701 COMPLIANT

Unbreachable protection from cyber threats that target safe, reliable and efficient operations

100% Visibility and Unbreachable Protection for vital rail networks

To learn how Unidirectional Gateways help you be compliant with IEC 62443 & TS 50701, **please scan the code**
or visit: waterfall-security.com/rail-industry/

For a free consultation with a Waterfall Solutions Architect, **please scan the code**
or visit: waterfall-security.com/contact

This is an official Report of UITP, the International Association of Public Transport. UITP represents the interests of key players in the public transport sector. Its membership includes transport authorities, operators, both private and public, in all modes of collective passenger transport, and the industry. UITP addresses the economic, technical, organisation and management aspects of passenger transport, as well as the development of policy for mobility and public transport worldwide.

This Report was prepared by Cybersecurity Committee

JANUARY | 2023

UITP ADVANCING PUBLIC TRANSPORT

Rue Sainte-Marie 6, B-1080 Brussels, Belgium | Tel +32 (0)2 673 61 00 | Fax +32 (0)2 660 10 72 | info@uitp.org | **www.uitp.org**