|  |  |  |
| --- | --- | --- |
| Issued:30 January 2023 | Entry into force:30 January 2023 | Validity:until further notice |
| Legal basis: |
| Modification details:Version 1.0, issued on 29 June 2020, entry into force on 1 July 2020Version 1.1, issued on 1 February 2023* Chapters 1–2: Minor changes to improve understanding
* Chapter 3: Updated to correspond to situational awareness in 2022
* Chapter 3.1: Added references to section 244a of the Act on Electronic Communications Services, TS50701, Traficom instructions on reporting disruptions in rail transport, and Kybermittari (Cybermeter), among other things. Updated the description of future regulations and the international rail transport cyber security networks.
* Chapters 3.2–3.3: Minor changes, no significant impact on the content
* Chapter 4: In new OT systems, the use of TS50701 is recommended, while the use of IEC 62443 is recommended for existing systems. For IT, the primary recommendation is to use ISO/IEC 27001; an alternative framework is e.g. Kybermittari. An OT environment can also be included in an ISO/IEC 27001 management system by using standards for OT systems in addition. The frameworks mentioned above may be used to replace chapters 4.1–4.11 of this recommendation.
* Chapters 4.1–4.11 of the recommendation have been revised to correspond at least to the Kybermittari target level 1. The previous recommendations have been kept the same as far as they correspond to Kybermittari. Several new recommendations added.
* The management methods presented in the recommendation as well as the Kybermittari tool are attached
 |

RECOMMENDATION FOR PROMOTING CYBER SECURITY
IN RAIL TRANSPORT

Content

**1.** **Purpose and scope of application of the recommendation** 3

**2. Cyber security concepts** 3

**3. Cyber security in rail transport** 6

3.1. Rail transport cyber security regulations 7

3.1.1. Current situation 7

3.1.2. Future 8

3.2. Cyber security threats and risks in rail transport 8

3.3. Examples of cyber security threats and their management methods 10

**4. Recommendations for developing the cyber security of rail transport** 14

4.1. Cyber security as a part of safety management and safety culture 14

4.2. Protecting critical services 15

4.3. Asset, change and configuration management 16

4.4. Threat and vulnerability management 16

4.5. Risk management 16

4.6. Identity and access management 17

4.7. Situational awareness 17

4.8. Event and incident response, continuity of operations 18

4.9. Third-party risk management 18

4.10. Workforce management 19

4.11. Cyber security architecture 19

4.12. Increasing cooperation 20

**5.** **Appendices, further information and sources of information** 20

**Tables**

1. Key definitions used in the recommendation (p. 4)

2. Division of cyber risks in rail transport into main categories (p. 8)

3. Examples of cyber threats to rail transport (p. 10)

4. Examples of reviews of cyber security events related to the running of a train (p. 11)

5. Examples of reviews of cyber security events related to maintenance (p. 11)

**Appendices**

1. Cyber security management methods presented in the recommendation as a table

2. The Kybermittari v.2.0 (Cybermeter) tool of the National Cyber Security Centre Finland that includes a reference to this recommendation

# **Purpose and scope of application of the recommendation**

The purpose of this recommendation is to promote the comprehensive development of cyber security in rail transport and ensure the continuity of operations. The aim is to increase:

* the awareness of cyber security of rail transport sector operators,
* the understanding of rail transport operators concerning cyber security risks and cyber security attacks,
* the preparedness for and responsible protection of rail transport operators against cyber threats to their own activities through risk management, and
* cooperation between rail transport operators, so that the level of overall protection of rail transport and its systems can be raised.

The purpose is to promote the ability of organisations and authorities participating in the operation of the railway system and urban rail transport systems to detect and identify various cyber security events that affect rail transport, protect themselves against them and recover from them as quickly as possible.

The recommendation is divided into two parts. Chapters 1–3 form an introduction. The purpose of the introduction is to both introduce the reader to promoting cyber security and demonstrate the diversity of cyber security threats against rail transport to the reader. Chapter 4 presents the recommendations of the Finnish Transport and Communications Agency to rail transport operators on measures for preparing for cyber security threats and managing cyber security risks. The appendices of the recommendation contain the items of Chapter 4 as a table; the appendices are intended to improve the usability of the recommendation.

The aim of the recommendation is to act as a concrete tool in developing cyber security. This means that the way in which each operator responds to the recommendations issued in Chapter 4 depends both on the type and scope of the operator’s activities as well as the measures already taken by the operator to develop cyber security. In fact, it is of primary importance that every rail transport operator works on the recommendations issued while keeping the operator’s own activities and operating environment in mind.

The recommendation is directed both at the railway system as well as urban rail transport systems. The recommendation has mainly been written with the railway system in mind, but the concepts, challenges and management methods of cyber security reviewed in the recommendation can be easily applied to urban rail transport, too. The different examples in the recommendation are largely based on the railway system, but they will also help with understanding cyber security in urban rail transport systems.

The 2020 version of the recommendation was drawn up by the Finnish Transport and Communications Agency as part of its official duties, and rail transport operators were heard during its preparation. The update of the recommendation in 2022 has also been drawn up by the Finnish Transport and Communications Agency as a part of its official duties. The 2022 update of the recommendation was sent to selected operators to be commented in the autumn of 2022, and it was sent to all rail transport operators to be commented in November 2022.

# **2. Cyber security concepts**

The terms concerning information and cyber security are defined fairly comprehensively in the [Vocabulary of Cyber Security](https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf) by the Security Committee operating under the Ministry of Defence. For clarity, the term ‘cyber security’ is mainly used in this recommendation, even if in some sections it might be appropriate to refer to information security.[[1]](#footnote-2)

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Vulnerability** | Vulnerability can refer to any weakness that makes it possible for damage to occur or that can be used to cause damage. Vulnerabilities can be found in operational systems, information systems, processes and human activities. Vulnerabilities may be caused by things such as processes, architecture or design, configurations and maintenance, physical intrusion, software and product development of the system, communications and data networks, and lack of training and awareness. |
| **Cyber threat** | A cyber threat refers to the cause of a potential unwanted and harmful event or development that affects the cyber operating environment and, if realised, endangers functions that are dependent on it. Cyber threats may be caused not only by realised information security threats, but also acts that endanger the safety of society that are carried out in a digital communications environment or operational systems. Cyber threats may originate from within or outside the borders of the country. |
| **Cyber risk** | A cyber risk refers to the combination of a threat that exploits a vulnerability, potential events, consequences and their likelihoods. The risks can be managed with risk management methods. |
| **Cyber operating environment** | A cyber operating environment is an operating environment that consists of one or more digital information systems. A cyber operating environment is characterised by the storage, editing and transfer of data and information via communications networks. In addition, characteristic features of the cyber security environment of rail transport include geographical dispersal, control of devices through operational systems and emphasis on the integrity and availability of information. The environment also includes the physical structures related to the processing of data and information.  |
| **Cyber security** | Cyber security is a goal state with a reliable cyber operating environment with secure operations. Measures that can be used to manage and, if necessary, tolerate different kinds of cyber threats and their impact proactively are a part of cyber security. Disruptions in the operation of a cyber operating environment are often caused by the realisation of an information security threat, which means that information security is a key factor in trying to achieve cyber security. In addition to information security, measures intended to secure the functions in the physical world that are dependent on the disrupted cyber operating environment, among other things, are used to achieve cyber security. While information security refers to the availability, integrity and confidentiality of information, cyber security refers to the security of a digital and networked society or organisation and its impact on their functions.  |
| **Information security** | Information security refers to arrangements that aim to ensure the availability, integrity and confidentiality of information. Availability means that the information can be used when desired. Integrity means that information is consistent with the original information, and confidentiality means that no outsiders can access the information. Information security arrangements include access control, locking the premises, safe storage and disposal of documents, encryption and backup of information, and the use of a firewall, antivirus software and certificates. Information security includes, among other things, securing data, equipment, software, telecommunications and operations. Information security can also mean conditions in which information security risks are under control. |
| **OT, operational technology** | Operational technology (OT) refers to programmable digital systems and devices that interact with the physical environment or control devices that interact with the physical environment. OT systems are used for purposes such as managing the transport network infrastructure and rolling stock, such as operation, signalling, power sources, communications and station management. |
| **IT, information technology** | Information technology (IT) refers to IT systems that support business as well as IT systems that support operational systems and offer an interface with operational systems.Examples: Passenger information, the driver’s terminal device applications, transport monitoring systems, traffic control management systems, commonly used data transfer methods (e.g. WLAN) as well as information and communication systems. |

*Table 1 Key definitions used in the recommendation*

# **3. Cyber security in rail transport**

With the standardisation and digitalisation of the European railway system, the system has become more open and harmonised, but potentially also more vulnerable. Russia’s offensive war in Ukraine has reinforced the importance of the railway system as a part of the critical infrastructure of society. During 2022, several cyber incidents affecting the railway system have been detected in Ukraine, Belarus and the EU. These factors have led to an increase in cyber security risks in rail transport. Improving the efficiency of rail transport relies heavily on digitalisation, and a strong basic level of cyber security is required to gain the benefits made possible by the future digitalisation goals.

Compared to railway transport, urban rail transport systems are clearly more limited geographically. However, due to the number of passengers and trips, the impact of disturbances may be socially significant. Around the world, urban rail transport systems have also been targeted by cyber security attacks, which have affected the reliability and operation of the systems. The disturbances may also affect traffic safety.

In rail transport, cyber risks may be realised in many different ways. A cyber security risk may be realised either unintentionally or intentionally, in which case it may be carried out by individuals, networks, organisations or state-sponsored parties. Threat identification requires taking all threats into account, whether caused by nature or human beings, accidents, or intentional actions. An organisation may be targeted by a cyber security attack focused on it specifically. An organisation may also become the target of an untargeted cyber security attack; for example, it may have an easily detectable and exploitable vulnerability in its system. Untargeted attacks are known to happen more often than targeted ones, and even an untargeted attack may cause harm to the organisation’s operation. The source of the cyber security threat, meaning the party that aims to cause damage, may also be other than the party carrying out the cyber security attack itself. Implementers may be found within organisations, among competitors or subcontractors, or among criminals, terrorists and hackers. Traficom’s Rail Transport Services maintain situational awareness of the cyber incidents in rail transport that have been reported publicly.

Realised cyber security incidents may have a significant negative impact on rail transport. It is likely that cyber security incidents will reduce the availability of services and cause additional work and loss of reputation, but they may also cause dangerous situations or even accidents. In fact, in this recommendation cyber security is discussed especially with regard to systems that are critical to safety.

Because the railway system is increasingly becoming one common system, a cyber security incidents that has been realised may lead to disturbances that may even cover the whole system and the state rail network. Similarly, it is possible for a cyber security incident to paralyse the operation of the metro transport system in its entirety, for instance. This means that cyber security must be promoted together and on a system-oriented basis – this is the only way to prevent a situation in which the whole system suffers due to a vulnerability of one of its parts. Major disturbances in rail transport may also have an indirect impact on the functioning of other modes of transport and other critical infrastructure of society.

In promoting cyber security, it is important to understand that cyber security is a part of the safety of the rail transport system, and cyber security must not be considered or processed as a separate issue.

Cyber security in the rail transport system is regulated by the NIS Directive of the EU on the security of network and information systems[[2]](#footnote-3) ([EU Network and Information Security Directive](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN), (EU) 2016/1148). However, it is not regulated comprehensively in the EU regulations on rail transport or taken into account in the assessment criteria that guide the content of the rail transport safety management system, for example. Even though the safety management system of railway operators is based on the EU regulations on railways, it is recommended that cyber security should be included as a part of the operator’s safety management system.

## 3.1. Rail transport cyber security regulations

### 3.1.1. Current situation

The development of the rail transport cyber security regulations is expected to continue. Section 169 of the Rail Transport Act has included provisions on the obligation to take care of the management of risks related to communications networks and information systems as well as notifications on information security incidents. So far, the regulation applies only to the keeper of the rail network as well as the provider of traffic control service of the state. It is based on the NIS Directive. [Section 244 a of the Act on Electronic Communications Services](https://www.finlex.fi/en/laki/kaannokset/2014/20140917#O9L29P244a) obliges, under certain conditions, the key operators in the rail transport system, such as the keeper of the rail network as well as the provider of the state traffic control service, to identify and document the critical parts of the network and the network devices used in them with regard to the dedicated network linked to the public communications network, and asses how it is ensured that the use of network devices will not pose a threat to national security or national defence. The obligation is based on the 5G toolbox[[3]](#footnote-4) of the EU and concern for the information security of 5G networks.

The Rail Transport Act also includes a more general obligation to submit a notification of the information required to form situational awareness. Section 172 of the Act applies to both rail transport operators and keepers of the railway network as well as the company providing traffic control service and the operator in charge of traffic control in the urban rail transport network, which must notify Traficom without delay about events of which they have become aware and that may affect the establishment of situational awareness. Traficom has provided instructions on activities in accordance with the section in 2022 ([Instructions on how to report disturbances in rail transport (Ohje raideliikenteen häiriöiden ilmoittamisesta), in Finnish](https://www.traficom.fi/sites/default/files/media/regulation/H%C3%A4iri%C3%B6ilmoitusohje%20valmis.pdf)). The section can also be considered to include an obligation to submit notifications on cyber security threats and incidents. A low threshold for reporting incidents related to cyber security to Traficom’s National Cyber Security Centre Finland and Rail Transport Service is recommended for all rail transport operators. The simplest way to submit the notification is by using the electronic form: <https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx?langid=en&RetUrl=https%3A//www.traficom.fi/en/services>

In addition to the Rail Transport Act, cyber security is taken into account in the Traficom regulation on drawing up a preparedness plan ([TRAFICOM/308489/03.04.04.00/2019](https://www.traficom.fi/fi/ajankohtaista/uusi-maarays-valmiussuunnittelun-jarjestaminen-liikennejarjestelmassa), in Finnish). Among other things, the regulation requires the keeper of the railway network to describe its cyber operating environment in its preparedness plan. The regulation applies to both the keeper of the state railway network as well as keepers of private sidings. In addition, the keeper of the rail network as well as the provider of traffic control service of the state must take threats and events threatening the cyber operating environment into account when describing the procedures they use to ensure the preparedness of rail transport management at different target levels. The regulation became applicable after a transition period on 1 June 2021. Traficom has also issued instructions on drawing up a preparedness plan concerning the regulation.[[4]](#footnote-5)

### 3.1.2. Future

The regulation, standardisation and instructions of rail transport are developed by several different parties. The most significant of the upcoming EU regulations is the [NIS 2 Directive](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1672915693202&uri=CELEX%3A32022L2555) (EU) 2022/2555 on the cyber security of critical services of society published on 27 December 2022, which specifies the requirements for risk management of the cyber security of critical services of society. The NIS 2 Directive reform also applies to the manufacturing sector of rail transport. The standardisation organisation CENELEC has published the technical specification [TS50701](https://sales.sfs.fi/en/index/tuotteet/SFSsahko/CENELEC/ID5/5/1012872.html.stx) on the cyber security of railways in 2022. Based on the technical specification, the standardisation organisation IEC is developing an international cyber security standard for railways ([IEC project team](https://www.iec.ch/ords/f?p=103:14:319535360914374::::FSP_ORG_ID:28802)). IEC intends to publish a cyber security standard for the railway system on 31 July 2025. Traficom’s National Cyber Security Centre Finland participates in the activities of the European Rail Information Sharing and Analysis Centre [ER-ISAC](https://er.isacs.eu/). Together with the European Union Agency for Cybersecurity (ENISA), ER-ISAC has published instructions on applying the specification TS50701. Traficom participates in ENISA’s Transport Resilience and Security Expert Group (TRANSSEC). ENISA has published studies on the cyber security of the rail transport system annually. In addition, Traficom and the National Police Board of Finland are involved in the Expert Group on Land Transport Security (Landsec) and Rail Passenger Security Platform (Railsec) operating under the European Commission that share information on the cyber security of rail transport and draw up recommendations. All rail transport operators have an opportunity to influence the development of cyber security in the sector. The Finnish Transport Infrastructure Agency is a member of the International Union of Railways (UIC), and UIC’s cyber security group is intended to activate at the end of 2022. UIC participated in the CYRAIL project that published a [cyber security recommendation](https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf) concerning control and signalling in 2018. The Finnish Transport Infrastructure Agency also participates in the cyber security group of European Rail Infrastructure Managers (EIM) and the cyber security working group of the European Railway Traffic Management System (ERTMS) Users Group (EUG). For instance, EUG investigates the management of certificates in the ERTMS online key management system. In addition, the Finnish Government resolution on improving information security and data protection in the critical sectors of society must be taken into account; when realised, its measures would oblige parties to specify critical information and telecommunications functions and use ISO 27001 certification, among other things.[[5]](#footnote-6)

The European Union Agency for Railways has also initiated measures needed to regulate cyber security in the railway sector. The work will focus first on developing the third level (L3) of the European Rail Traffic Management System (ERTMS). The work will also take the results gained from the projects of the Shift2Rail consortium into account. The European Union Agency for Railways intends to include cyber security more comprehensively in the framework of European rail transport regulations in the future and take account of CENELEC’s TS 50701 railway applications - cybersecurity, among other things, in the work.

The importance of cyber security being highlighted in the EU regulations on rail transport is likely to influence the processing of cyber security issues related to the railway system in the next few years. In contrast, no similar changes are to be expected for urban rail transport, and therefore the discussion of cyber security issues related to urban rail transport systems will most likely remain within the scope of national guidance in the future, too.

## 3.2. Cyber security threats and risks in rail transport

The most important part of cyber security is managing cyber security risks. Vulnerabilities and their impact can be managed and mitigated by identifying and repairing them. However, the existence of a vulnerability does not automatically lead to damage; instead, damage only occurs when a threat exploiting the vulnerability is realised. If no threat of exploitation is related to the vulnerability, it may not necessarily require implementing a management measure, but it should still be identified and its situation monitored in case of potential changes. A threat refers to the cause of a potential unwanted and harmful event, and threats can be managed by assessing the risks they cause. In contrast, risks can be processed by using risk management methods.

In fact, cyber risk management refers to the identification and assessment of risks as well as the selection, development and implementation of options carried out for the processing of risks. Risk management applies to all potential risks that may affect the organisation and reacting to them. Cyber security risks are a part of risk management. As a whole, risk management is a systematic and continuous thought process that reflects the values of the organisation and, in addition to identification, processing and assessment, consists of continuous coordination, studying the development of risks, reassessment of risks, corrective measures, communication as well as reporting. Not being linked to time or space and the difficulty of calculating damages are highlighted in cyber risks from the perspective of risk management in particular.

Cyber risks can be divided into four main categories, which are human activity, system failures and technical malfunctions, failed internal processes and external events. As for the main categories, they can be divided into subcategories that illustrate the operational activities that create risks. For cyber risks as a whole, it is important to take into account that cyber risks often correlate with each other, and if realised, one risk can cause a chain of events that triggers several risks.[[6]](#footnote-7)

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Human activity | 2. System failures and malfunctions | 3. Failed internal functions | 4. External events |
| 1.1 Lack of intentAccidentsErrorsNeglect | 2.1. DevicesCapacityPerformanceMaintenanceObsolescence | 3.1. Design and implementation of the functionProgress of the functionDocumentation of the functionRoles and responsibilitiesNotifications and alarmsFlow of informationGrowth of problemsService-level agreementsTransfer of tasks | 4.1. DisastersWeather phenomenaFiresFloodsEarthquakesCivil unrestAccidentsPandemics |
| 1.2. IntentFraudsSabotageTheftsVandalism | 2.2. SoftwareCompatibilityConfiguration managementChange management Security settingProgramming practicesTesting | 3.2. Monitoring the activitiesMonitoring the operating environmentIndicatorsRegular self-monitoringOwnership of the activity | 4.2. Legal problemsCompliance with regulationsFunctionality of the regulationsTrials |
| 1.3 InactionSkillsKnowledgeGuidanceAvailability | 2.3. SystemsDesignTechnical requirementsIntegrationComplexity | 3.3. Support functionsHuman resources managementFinancingDevelopment and training activitiesProcurement | 4.3. Business problemsDisturbances due to a subcontractorMarket conditionsFinancial situation |
|  |  |  | 4.4. DependenciesElectricity, water and telecommunications networksRescue servicesReserve powerTransport |

*Table 2. Division of the cyber risks of rail transport into main categories. Based on the work by Cebula & Young, 2010.*

Cyber risks can be seen from a wider perspective as operational risks concerning information and technology that affect the confidentiality, availability or integrity of the information or system. In fact, a cyber risk is considered to cover all of the risks that lead to financial loss, interruption of the activity or damage to the organisation’s reputation or the concrete activities of the organisation. If a cyber risk is realised, in the worst case the damage may be considerable from the financial and human perspectives.

For both the railway system as well as urban rail transport, the cyber operating environment of rail transport consists of two separate parts: information systems and operational systems. Information systems and operational systems are increasingly often linked to each other, which creates new requirements for the management of cyber risks. Traditionally, cyber security has been taken into account more comprehensively in information systems, and with regard to operational systems, interest in cyber security issues has only started to grow in the last few years. Today, the technical solutions of OT systems are also starting to approach the technical solutions of IT systems.

A feature characteristic of rail transport is the long life of the systems used and partially also the ageing of the systems. Some of the systems have been used for decades and their parts have been improved along the way, which makes them both challenging and vulnerable with regard to cyber security. The slow increase in taking cyber security into account on the operational side as well as the geographic dispersal make rail transport more vulnerable to cyber threats. A key factor of cyber risk management is developing the cooperation between the operators of information systems and operational systems. It is also important to pay attention to protecting systems, protecting the information and data in the systems and ensuring the safety of telecommunications both within and between the systems.

Because the number of cyber security risks grows as the functions and systems of rail transport develop and become digitalised and the risks become more diverse, the management of cyber security risks is challenging. However, securing the digital world completely is impossible, and as a result, attention should also be paid to matters such as the maturity of the organisation in detecting cyber security threats.

Attention should be paid to identifying and combating cyber threats both when updating existing systems as well as in new systems all the way from the design phase. The client and operator organisations have a major responsibility in implementing cyber security, and especially before the deployment of changed or new systems, it is important to verify that the systems are cyber secure and their users have procedures for taking care of cyber security throughout the life cycle of the systems. Because many supply agreements in rail transport are long and several of them have been drawn up during a time when cyber security issues were not central, it is also important to agree on cyber security requirements when updating or renewing existing contracts.

## 3.3. Examples of cyber security threats and their management methods

The following table describes different kinds of cyber risks that may target rail transport and that should be taken into account in the risk management of rail transport operators. However, the cyber risks mentioned in the table are only examples, and every rail transport operator must independently assess the cyber risks that are related specifically to their own activities as well as the critical systems that must be taken into account in developing cyber security.

|  |  |  |
| --- | --- | --- |
| **Cyber risk** | **Examples (threat)** | **Targeted operators** |
| **Risks related to computer-based interlocking equipment** | The data transfer from traffic control breaks and the commands are not transmitted to computer-based interlocking (CBI) equipment as intended due to a broken cable caused by track work, for example. | Traffic control, keeper of the rail network, rail transport operators  |
| **Interface risks between traffic control systems and signal devices** | An outage or disruption in data transfer between computers and the relay signal devices controlled by them. | Traffic control, keeper of the rail network, rail transport operators |
| **Interface risks between traffic control systems and computer-based interlocking equipment** | The commands used by the remote control system of the traffic controller are not transmitted correctly to the computer-based interlocking device. | Traffic control, keeper of the rail network, rail transport operators |
| **Risks related to the integrity and reliability of the data in traffic control systems.** | The data content used crumbles due to the actions of a hacker, for instance, so that the data in the systems cannot be trusted or utilised. | Traffic control, keeper of the rail network, rail transport operators |
| **Risks related to traffic control systems based on a source code** | Malicious code is inserted into the source code, and it enters the traffic control system and is activated in the system in connection with updating it, for example. | Traffic control, keeper of the rail network, rail transport operators |
| **Risks related to traffic control systems connecting to the public network** | Unwanted updates or configuration changes are made intentionally to systems via the public network, or the connection to the public network breaks. | Traffic control, keeper of the rail network, rail transport operators |
| **Interface risks related to linking the IT and OT systems together and connecting them to the public network** | The IT and OT systems are connected to each other as well as the public network, which means that the integrity of the OT systems may be at risk. | Traffic control, keeper of the rail network and rail transport operators |
| **Risks related to ensuring the power supply** | There is a malfunction in the main grid that prevents the electricity from being transferred to high-voltage substations or from the substation to the rail network, or an unauthorised party can hack the monitoring systems of electrified railways. | Keepers of the rail network, traffic control. |
| **Risks related to the telematic systems**  | Someone is able to intentionally disrupt passenger announcements or information displays. | Keepers of the rail network, rail transport operators |
| **Risks related to components** | A factor that also causes disturbances outside the component is intentionally included in a component (e.g. microchips and phones). | Traffic control, rail transport operators (rolling stock) |
| **Risks related to the interoperability of devices** | The compatibility of access control devices is disrupted by software updates or poorly planned development projects, among other things. | Traffic control, keeper of the rail network, rail transport operators |
| **Cyber risks related to the rolling stock**  | The access control or other functions of the rolling stock is disrupted so that it is not safe to use the stock. | Rail transport operators, parties maintaining the rolling stock |
| **Hijacking the systems** | Due to the hijacking, the operation of the systems is disrupted or has to be stopped to ensure safety | All rail transport operators |
| **Risks due to the personnel** | The personnel, or a former member of the personnel, causes disturbances in the system either intentionally or due to a lack of competence. High-risk duty combinations in particular. | All rail transport operators |
| **Risks due to subcontractors** | As above, but the actor is a subcontractor. | All rail transport operators that use subcontracting |
| **Risks due to the users of services** | As above, but the actor is a service user. | All rail transport operators that provide services |

*Table 3. Examples of cyber threats in rail transport*

The bowtie model, for instance, can be used for a detailed review and analysis of cyber security scenarios.[[7]](#footnote-8) The following table shows examples of individual cyber security events processed by using the bowtie model. At the same time, the tables act as examples of functions that can cause a cyber security events, how it is possible to protect against events already in advance, and if an event occurs despite the precautions, what are the protections that restore it as well as the consequences.

The examples have been drawn up in a rail transport cyber security workshop arranged by Traficom on 11 March 2020 in order to test whether the bowtie model could be useful for a more detailed review of cyber security events and understanding all of the dependencies that may be linked to an individual event.

|  |
| --- |
| **TRAIN OPERATION** |
| **Function** | **Initiating factor** | **Event/dangerous situation** | **Preventive protection** | **Restorative protection** | **Consequence of the event** |
| Physical protection | Breaking into the safety equipment room | Remote control is paralysed | Exercises, training, audits | Relying on a backup system, stopping or restricting traffic | Train operation is prevented |
| Protection | Hacking over the network |
| Protection | Malware | Accident |
| Backup system | Backup system crashing |

*Table 4. Examples of reviewing cyber security events related to train operation*

|  |
| --- |
| **MAINTENANCE** |
| **Function** | **Initiating factor** | **Event/dangerous situation** | **Preventive protection** | **Restorative protection** | **Consequence of the event** |
| Problem with the agreement | Deficiencies in the subcontracting agreement | The subcontractor affects the system in connection with maintenance | Good preparation of the agreement and updating it, if necessary; skilled agreement negotiators | Removing and isolating the cause and the party that caused the damage, backup systems are in order, responsibilities and working instructions are in order, reacting quickly to the error, communication skills are in order | The system is paralysed |
| Problem with the agreement | Breach of agreement | Consequences related to the agreement are in order, monitoring, confidentiality agreements |
| Bad intentions | Intent of the party carrying out the work | Investigating the background of the service provider, previous references, specifications of the agreement, service descriptions are in order, regular reviews | Accident or dangerous situation |
| Deficiencies in the monitoring | Subcontracting is not monitored, the monitoring does not work | Assignment of responsibilities for monitoring | Damage to reputation |

*Table 5. Examples of reviewing cyber security events related to maintenance*

# **4. Recommendations for developing the cyber security of rail transport**

The recommendations of the Finnish Transport and Communications Agency for developing cyber security have been compiled in this section. The recommendations are also presented as a table in a separate appendix. The kind of measures each operator should take to respond to the recommendations issued depends on the type and scope of the operations of the rail transport operator.

The Finnish Transport and Communications Agency recommends that in the operational technology (OT) sections of the new rail transport system, the technical specification TS50701 Railway Applications - Cybersecurity should be used in addition to a standard that will be developed based on the technical specification. It is recommended that the existing OT systems should continue to comply with the IEC 62443 series designed for the safety of industrial automation, if the systems have been developed based on them.

It is recommended that all operators in the rail transport system should assess and measure the cyber security level of their organisation. For existing administrative IT systems, the use of the standard ISO/IEC 27001:2022[[8]](#footnote-9) for cyber security management systems is recommended. An ISO/IEC 27001 information security management system can be used to manage an OT environment, where the standards applicable to an OT environment mentioned above are also applied.[[9]](#footnote-10) Other alternative frameworks may include, for instance, the free [Kybermittari (Cybermeter)](https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter)[[10]](#footnote-11) tool, available in Finnish, maintained by the National Cyber Security Centre Finland. When Kybermittari is used as the framework, it is recommended that all rail transport operators exceed target level 1. The recommendation for providers of critical services for the rail transport system (NIS operators) is to exceed the target level 2. The Kybermittari\_V2 assessment tool is attached to this recommendation; cross-references to the recommendations of chapters 4.1–4.11 are recorded in it.

Applying the frameworks mentioned above, the recommendations in chapters 4.1–4.11 can be replaced insofar as the requirements according to the framework selected are at least as strict. Chapter 4.12 of these recommendations applies to increasing cooperation in the rail transport system. The Kybermittari target level 1 has been applied during the compilation of chapters 4.1–4.11, but some of the items in the recommendation are placed higher than target level 1. Kybermittari is based on the NIST Cybersecurity Framework and Cybersecurity Capability Maturity Model (C2M2), on which the previous recommendation on promoting cyber security in rail transport, updated with this recommendation, was based. The Architectural Framework for Digital Security ([DTARK](https://wiki.dvv.fi/display/DTARK/)), published by the Digital and Population Data Services Agency, is also based on the NIST Cybersecurity Framework. DTARK is well suited to designing cyber security, but it is not primarily intended for assessing and measuring the level of cyber security.

## 4.1. Cyber security as a part of safety management and safety culture

The Finnish Transport and Communications Agency recommends that rail transport operators include cyber security management as a part of their safety management system, or if they do not have one, as a part of their general management system. Cyber security is promoted as far as possible by taking account of the operating models that are an integral part of developing the rest of the operations (risk assessment, self-monitoring, etc.) For the purpose, the operators should:

* Define a cyber security strategy as a part of the safety management system, for example, and secure the support of the management and board or executive group of the organisation in order to implement the goals in accordance with the cyber security strategy.
	+ The cyber security strategy must include at least a list of the cyber security goals and a plan for implementing them.
	+ Document a cyber security strategy and goals. The strategy and goals must be in line with the general goals of the organisation as well as the risks focusing on critical infrastructure.
* Take cyber security into account in plans related to the continuity of the operations and ensure that the cyber security strategy and plans related to the continuity of the operations have been coordinated with each other.
* Allocate the resources (personnel, financing and tools) for establishing cyber security management.
* Define and document the responsibilities and cooperation models concerning cyber security that cover the organisation as well as the other operators related to the operations, taking account of the fact that in the rail transport system, cyber security is an end-to-end chain that passes through the infrastructure owned by several different operators.

## 4.2. Protecting critical services

The Finnish Transport and Communications Agency recommends that rail transport operators should recognise their role as a part of the logistics chain that is a critical service of society and manage the risks accordingly. The critical services and their dependencies must be identified and managed and the impact of cyber incidents must be minimised. For the purpose, the operators should:

* Define and document the services critical to the continuity and safety of rail transport.
* Define and document the data needed to provide the services critical to the continuity and safety of rail transport.
* Define and document the processes critical to the continuity and safety of rail transport.
* Define and document targets to be protected, i.e. the information systems, operational systems and data critical to the continuity and safety of rail transport, such as traffic control systems and their different functions.
* Define and document the systems and functions essential to monitoring the situational awareness as well as the critical systems, services and equipment.
* Bring all resources (data, processes, facilities, equipment, supply chains) needed to provide the services critical to the continuity and safety of rail transport within the scope of the organisation’s security management and policies.
* Bring all resources (data, processes, facilities, equipment, supply chains) needed to provide the services critical to the continuity and safety of rail transport within the scope of the organisation’s risk management policies.
* Draw up a cyber event and incident response plan that covers all services critical to the continuity and safety of rail transport.
	+ The response plan covers the likely impact of known attacks comprehensively.
	+ The personnel participating in the management of cyber events and incidents and disruptions internalises and understands the management plan.
	+ The reponse plan is documented and distributed to the relevant interest groups.

## 4.3. Asset, change and configuration management

The Finnish Transport and Communications Agency recommends that rail transport operators manage their IT and OT assets. Assets refer to the equipment, software and information essential to the functions. For the purpose, the operators should:

* Establish an inventory of the software and equipment important to the continuity and safety of rail transport.
* Establish an inventory of the information assets important to the continuity and safety of rail transport, such as the capacity management and customer information within the operator’s sector as well as the basic settings of the software and equipment.
* Establish configuration baselines for the configurations of equipment, software and information assets.
* Assess the changes made to the inventoried devices, software and information assets and have them approved before implementing them.
	+ Keep a log of the changes made to the inventoried devices, software and information assets.
* Create methods for keeping the firmware up to date (e.g. firmware updates)
* Create methods for the remote monitoring, management and updates of critical equipment.

## 4.4. Threat and vulnerability management

The Finnish Transport and Communications Agency recommends that rail transport operators define procedures for detecting, identifying, analysing, managing and responding to cyber security threats and vulnerabilities, taking account of the threats against the continuity and safety of rail transport. For the purpose, the operators should:

* Identify suitable sources of information to identify vulnerabilities.
	+ Collect and interpret vulnerability information for their operations.
	+ Carry out vulnerability assessments.
	+ Address vulnerabilities relevant to their activities by e.g. increasing monitoring or installing an update to correct the issue.
	+ By taking advantage of vulnerability assessments, determine the parts of the systems they use that are exposed to cyber security attacks, taking account of system interfaces and dependencies, among other things.
* Identify suitable sources of information for identifying threats.
	+ Collect and interpret threat information for their operations.
	+ Address threats relevant to their activities by e.g. increasing monitoring or following the development of threats.
		- Follow and monitor cyber security threats and their management in a timely, risk-based manner in operational and information systems, so that it is possible to react to them as early as possible.
	+ Take care of protecting the parts of procedures, systems and people exposed to cyber security threats throughout their life cycle.
	+ Take account of the cyber security threats detected starting from setting requirements during the system procurement planning stage throughout the life cycle of the systems.

## 4.5. Risk management

The Finnish Transport and Communications Agency recommends that rail transport operators define an organisation-wide risk management system to enable the identification, analysis and mitigation of cyber security risks and risk monitoring, taking account of the business units, subsidiaries, infrastructures connected together and other interest groups in relation to the risks against the safety and continuity of rail transport. For the purpose, the operators should:

* Guide cyber security risk management systematically.
* Identify cyber risks by mapping the risks to their procedures, systems and people and take advantage of continuous risk assessment
* Prioritise cyber risks based on their estimated impact.
* React to cyber risks and cyber risk categories by e.g. mitigating, accepting, avoiding or transferring them.
* Agree on acceptable risk levels and specify what measures are used to protect the organisation and what measures will be taken in a potential attack situation to detect the attack, analyse it, respond to attacks and recover from them.
* Take cyber security risks into account when making decisions.
	+ Take account of the cyber security risks detected starting from setting requirements during the system procurement planning stage throughout the life cycle of the systems.
	+ Plan the life cycle management of systems as a whole and ensure that accepting the potential residual risks is done in a controlled and conscious manner.

## 4.6. Identity and access management

The Finnish Transport and Communications Agency recommends that rail transport operators define procedures for the access right management and access control of physical premises, information systems and operational systems, taking account of not only the internal and external persons, but also other parties (devices, systems, software processes), and paying special attention to remote connections. For the purpose, the operators should:

* Allocate separate identities to employees and other units (such as processes and devices that need access to the devices, software and data resources that belong to the functions), and assess the necessity of shared identities.
	+ Distribute access right credentials such as passwords, smart cards or keys to employees and other units.
	+ Remove the identities when they are no longer needed.
* Implement logical access controls (information systems).
	+ Revoke access rights when they are no longer needed.
* Implement physical access controls (such as fences, locks or signage).
	+ Revoke access rights when they are no longer needed.
	+ Maintain a log of access rights.
* A stronger or multi-factor authentication is required for rights of use or access with a higher related risk (such as administrator and maintenance IDs, shared IDs, remote connections).

## 4.7. Situational awareness

The Finnish Transport and Communications Agency recommends that rail transport operators define the functions and technologies to be used for collecting and analysing operational and cyber security information, raising alarms, and presenting and utilising the information to establish situational awareness on the functioning of the organisation and the level of cyber security. For the purpose, the operator should:

* Collect log data on devices, software and information assets important to the continuity and safety of rail transport.
* Monitor and analyse the data collected via logs and other sources.
	+ Monitor IT and OT environments in case of anomalous activity and potential cyber events.
* Define procedures for creating and maintaining situational awareness of cyber security as well as communications that are updated regularly.
	+ Compile monitoring data for the operational situational awareness of the operator.
	+ Enhance situational awareness with other applicable data of the organisation, such as visual observations.

## 4.8. Event and incident response, continuity of operations

The Finnish Transport and Communications Agency recommends that rail transport operators define plans, processes and technologies to be used to detect and analyse events and incidents related to cyber security, respond to them and recover from them in relation to the risks to the continuity and safety of rail transport. For the purpose, the operators should:

* Define procedures for reporting cyber security events and incidents to predetermined persons or roles and maintain a log about them.
* Draw up criteria for defining cyber incidents.
	+ Analyse cyber events in a way that supports determining potential cyber incidents.
* Identify suitable employees and assign them roles for cyber security event and incident response.
	+ Respond to cyber events and incidents by limiting their impact on the function and restoring the operation to normal.
	+ Cyber incidents are reported to the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency as well as the L-ISAC group, for example.
	+ Information security breaches and their attempts are reported to the police, if an offence is suspected.
* Draw up a system recovery plan and a continuity plan for the function concerning their own operations, which takes account of the organisation’s ways of continuing the operation during disruptions and opportunities to ensure that services critical to the continuity and safety of rail transport are provided.
	+ Back up data and test the backups.
	+ Identify the IT and OT devices that need spare parts and are critical to the continuity and safety of rail transport.
* Train both within their own organisation as well as together with the other operators of the transport system to test the continuity plans, respond to cyber security events and incidents and map vulnerabilities.

## 4.9. Third-party risk management

The Finnish Transport and Communications Agency recommends that rail transport operators define procedures for the management of the supply chain and external dependencies used to manage the cyber security risks of services and targets to be protected that are dependent on external parties in relation to the risks to the continuity and safety of rail transport. For the purpose, the operators should:

* Identify significant IT and OT dependencies in the partner network, including partners responsible for operating the functions.
	+ Identify the operators in the partner network that own, manage or are otherwise able to access devices, software or information assets important to the function.
* Take the estimate of the cyber security qualifications of suppliers and other operators in the partner network into account as a part of their selection.
* When selecting products and services, take the assessment of their cyber capabilities into account.
	+ Ensure the safety of the systems to be acquired by setting the necessary cyber security requirements during the procurement phase on both the system to be acquired as well as the cyber security level of the supplier.
* Through agreements, ensure that the cyber security measures of the operators in the partner network are sufficient and that they are adjusted to the organisation’s own cyber security operating models.
* As a part of acceptance testing, the most critical devices, data resources and systems to be procured are confirmed to be safe with safety testing before their deployment.

## 4.10. Workforce management

The Finnish Transport and Communications Agency recommends that rail transport operators define and maintain plans, processes, technology and controls to establish a cyber security culture for the operator and guarantee that there are suitable and skilled personnel in relation to the risks to the continuity and safety of rail transport and the operator’s own goals. For the purpose, the operators should:

* Identify the responsibilities related to cyber security and appoint a person or persons in charge for the organisation.
* By offering cyber security training to the persons in charge, ensure that the organisation has sufficient cyber security competence in relation to the nature and scope of its activities, and that it is maintained and developed.
* Ensure that the persons in charge are familiar with the operator’s functional and transport operation systems, understand the cyber security risks focused on them and work to minimise them. The persons in charge are familiar with the standards and legislation on cyber security and are able to ensure that they are sufficiently taken into account and complied with in the organisation.
* Identify cyber security knowledge, skill and ability requirements and any related gaps , taking both current and future needs into account.
* Also train the rest of the personnel and, if necessary, also the subcontractors with regard to cyber security issues and take care of raising the cyber security awareness of the organisation.
* Define procedures for carrying out background checks of employees and suppliers and appointing them to duties with access to protected targets related to the provision of services critical to the continuity and safety of rail transport.
	+ The procedures related to the end of an employment relationship take cyber security into account.

## 4.11. Cyber security architecture

The Finnish Transport and Communications Agency recommends that rail transport operators create and maintain structures they use to manage and guide the cyber security controls, processes and other cyber security activities of organisations in relation to both the risks to the organisation’s assets as well as the goals set by the organisation. For the purpose, the operators should:

* Define a cyber security architecture strategy around the integrity and availability of critical systems as well as the information to be protected, paying special attention to the design and operating principles of safety equipment and the physical protection and monitoring of equipment facilities.
* Separate the organisation’s IT networks from its OT networks by implementing network segmentation, for example, and assess the need for network duplication and implement the necessary network duplications.
* Implement cyber security protection mechanisms on devices, connections, software and data resources important for the operation.
* Ensure the safety of internally developed software and third party solutions in high priority devices and software throughout the life cycle of the software from their procurement to decommissioning, ensuring especially that the principles of secure software development are followed.
	+ Take the principles of secure safe software development into account in systems other than the high priority ones, too.
* Implement protection of sensitive data based on identifying and classifying the data being processed.
	+ For certain file types, also take account of protecting all other data.
	+ For certain file types, also take account of protecting all data in transit.

## 4.12. Increasing cooperation

The Finnish Transport and Communications Agency recommends that rail transport operators cooperate in order to raise the overall protection level of the rail transport system. For the purpose, the operators should:

* For their own organisation, define procedures for cooperation to develop cyber security and promote cyber security risk management with authorities and other operators in the field.
* Ensure cyber security in cooperation with the other operators in the field and aim to harmonise the procedures and level of protection among parties using the same system or a joint interface, for example.
* Transmit information on cyber security threats, risks and attacks to other rail transport operators and cooperation networks to create and share common situational awareness.
* Disseminate their good practices to develop cyber security.
* Influence the good development of cyber security regulations in the technical specifications of interoperability, among other things.
* Ensure that cyber security issues are brought up in agreements between organisations and in various highly visible places.

# **Appendices, further information and sources of information**

Appendix 1: Cyber security management methods presented in the recommendation as a table

Appendix 2: The Kybermittari (Cybermeter) tool by the National Cyber Security Centre Finland, which includes a reference to this recommendation

Regulations

* NIS1 Directive ([https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&amp;amp;from=EN))
* NIS2 Directive ([https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1672915693202&uri=CELEX%3A32022L2555](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1672915693202&amp;amp;uri=CELEX%3A32022L2555))
* Rail Transport Act, section 169, in Finnish (<https://finlex.fi/fi/laki/ajantasa/2018/20181302#L22P169>)
* Act on Electronic Communications Services, section 244a ([https://www.finlex.fi/en/laki/kaannokset/2014/20140917](https://www.finlex.fi/en/laki/kaannokset/2014/20140917#O9L29P244a))

National authorities

* Traficom: Regulation on arranging preparedness planning (<https://www.traficom.fi/fi/ajankohtaista/uusi-maarays-valmiussuunnittelun-jarjestaminen-liikennejarjestelmassa>, in Finnish)
* Traficom: instructions on how to report disturbances in rail transport, in Finnish (<https://www.traficom.fi/sites/default/files/media/regulation/H%C3%A4iri%C3%B6ilmoitusohje%20valmis.pdf>)
* Website of the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency (<https://www.kyberturvallisuuskeskus.fi/en>)
	+ Instructions and guides (<https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides>)
	+ Kybermittari - Cybermeter (<https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter>)
	+ NIS notification form (Notification of an information security incident) (<https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx?langid=en&RetUrl=https%3A//www.traficom.fi/en/services>)
* Finnish Government resolution on improving information security and data protection in the critical sectors of society (<https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80732d82>, in Finnish)
* The Architectural Framework for Digital Security (DTARK) of the Digital and Population Data Services Agency (<https://wiki.dvv.fi/display/DTARK/>, in Finnish)

Standardisation

* IEC standardisation of the cyber security of the railway system (<https://www.iec.ch/ords/f?p=103:14:319535360914374::::FSP_ORG_ID:28802>)
* ISA 62443, Security for Industrial Automation and Control Systems
* CENELEC (<https://www.cenelec.eu/>)
	+ CLC/TS 50701:2021:en Railway applications - Cybersecurity (<https://sales.sfs.fi/en/index/tuotteet/SFSsahko/CENELEC/ID5/5/1012872.html.stx>)
* NIST Cyber Security Framework (<https://www.nist.gov/cyberframework>)
* NIST 800-82r2, Guide to Industrial Control Systems (ICS) Security (<https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final>)
* ISO/IEC 27001:2022:fi Information security, cybersecurity and privacy protection. Information security management systems. Requirements. ([https://online.sfs.fi/fi/index/tuotteet/SFS/ISO/ID5/2/1155761.html.stxISO/IEC 27002](https://online.sfs.fi/fi/index/tuotteet/SFS/ISO/ID5/2/1155761.html.stxISO/IEC%2027002))
* SFS-EN ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection. Information security controls. (<https://online.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/2/1172534.html.stx>)
* ISO/IEC 27005, Guidance on managing information security risks. (<https://sales.sfs.fi/en/index/tuotteet/SFS/ISO/ID2/2/738504.html.stx>)
* Cybersecurity Capability Maturity Model (C2M2) (<https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>)

Other

* Vocabulary of Cyber Security (<https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/>)
* Website of the EU Agency for Cybersecurity (<https://www.enisa.europa.eu/>)
	+ Cyber security threat landscape (<https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends>)
* European Commission publication: Cybersecurity Toolkit for transport <https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en>
* EU 5G toolbox (<https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security>)
* Information exchange group on the cyber security of European railways (ER-ISAC) (<https://er.isacs.eu/>)
* CYRail (<https://cyrail.eu/>) See also: CYRail Recommendations on cybersecurity of rail signalling and communication systems (<https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf>)
* UK Rail Cyber Security Strategy ([https://www.raildeliverygroup.com/component/arkhive/?task=file.download&id=469772253](https://www.raildeliverygroup.com/component/arkhive/?task=file.download&amp;amp;id=469772253))
* An example of bowtie analysis ([https://www.traficom.fi/sites/default/files/media/file/Guidance for FSTD operators.pdf](https://www.traficom.fi/sites/default/files/media/file/Guidance%20for%20FSTD%20operators.pdf))
* Cebula, James J. & Young, Lisa R. 2010. A Taxonomy of Operational Cyber Security Risks. Carnegie Mellon University

Approved on 30 January 2023

Kaisa Sainio
Head of Rail Transport Services

Ville Lahti

Senior Specialist

1. The definitions in Table 1 are mainly based on the Vocabulary of Cyber Security by the Security Committee, but some of them have been supplemented with the definitions used in the UK Rail Cyber Security Strategy and adapted to fit rail transport better (see Chapter 5. Further information and sources of information) [↑](#footnote-ref-2)
2. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN [↑](#footnote-ref-3)
3. <https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security> [↑](#footnote-ref-4)
4. <https://www.traficom.fi/fi/saadokset/ohje-valmiussuunnitelman-laatimiseksi-raideliikenteessa> [↑](#footnote-ref-5)
5. <https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80732d82> [↑](#footnote-ref-6)
6. The table is based on the table of operational cyber risks by Cebula & Young (2010). [↑](#footnote-ref-7)
7. Example: IEC 31010:2019 Risk management. Risk assessment techniques. B.4.2 Bowtie analysis, and p. 22 <https://www.traficom.fi/sites/default/files/media/file/Guidance%20for%20FSTD%20operators.pdf> [↑](#footnote-ref-8)
8. <https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID5/2/1155761.html.stx> [↑](#footnote-ref-9)
9. Traficom does not have the competence to demand an ISO/IEC 27001 certification from operators, even though in Denmark, for instance, the certification requirement is valid. Traficom monitors operators based on risk, and obtaining the certificate would reduce Traficom’s need for monitoring. [↑](#footnote-ref-10)
10. <https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter> [↑](#footnote-ref-11)