Audit of the ICT resilience of critical infrastructures – implementation of the minimum standard for railway control systems

Federal Office of Transport, Lausanne-Échallens-Bercher railway, Fribourg transport network, Zentralbahn and Rhaetian Railway

Key facts

Critical infrastructures (CIs) ensure the supply of indispensable goods and services in Switzerland. In order to protect these CIs, it is necessary to keep them functional at all times, insofar as possible. In this context, the resilience of information and communication technology (ICT) and critical infrastructure protection (CIP) against cyberthreats is of great importance. On 8 December 2017, the Federal Council adopted the national CIP strategy (2018–2022), which includes rail transport. The Confederation spends around CHF 4.5 billion annually on preserving value and expanding the railway infrastructure.

As part of a cross-sectional audit, the Swiss Federal Audit Office (SFAO) examined the compliance of four railway companies[1] with minimum requirements for ICT protection against cyberattacks. The minimum standard for improving ICT resilience, as published by the Federal Office for National Economic Supply (FONES), was used. This essentially covers the five topics of "identify", "protect", "detect", "respond" and "recover", and provides a set of concrete measures for implementation. The FONES recommends that CI operators implement the ICT minimum standard.

Major differences in information security

With regard to maturity, which describes the level of protection, the audit revealed a mixed picture, going from "significantly below the recommended minimum value" to "minimum value clearly exceeded". There is still a need for action in the implementation of information security at all audited organisations.

In terms of the organisation of information security, it was already apparent at three of the audited railway companies that the necessary roles were not defined or only insufficiently. The perception of ICT risks also varies greatly among employees.

A full inventory of the information and systems to be protected is the most important basis for implementing ICT security. The railway companies are aware of this and keep an inventory of their assets. In part, these are still in different data sources and are not linked to each other. Various projects should improve this situation in the future.

Access management needs to be improved at three companies. In some respects, there are considerable deficiencies concerning the administration of user accounts and the granting of rights. Clients must be able to control remote access by suppliers and this must be documented in a transparent manner. There is a need for extensive action here on the part of the railway companies concerned.

[1] Lausanne-Échallens-Bercher railway, Fribourg transport network, Zentralbahn and Rhaetian Railway

More attention must be paid to physical and environmental security in general. In one case, access to the control centre was unsecured, with the result that the ICT systems there were not technically protected against unauthorised access. Devices for the maintenance of rolling stock are unlocked and accessible in some cases. In terms of fire protection, widely differing measures have been implemented. While several signal boxes have no fire or smoke detection systems, and lack extinguishing resources for any initial response, the SFAO found redundant automatic extinguishing systems in the critical installations at one railway company.

Half of the railway companies audited have multiple control centres in different locations, which means that services should not be affected in the event of a fault.

The testing of emergency scenarios and recovery procedures should be considered an ongoing process. This ensures that systems and processes will work in the event of an incident. Some railways still need to catch up in order to achieve an adequate level of testing.

Information security requirements are a major challenge for small railway companies

The cross-sectional audit showed that larger companies are better positioned in terms of ICT security than smaller ones, for which it is a major challenge, both financially and in terms of personnel. However, close collaboration with larger railway companies and the procurement of external services can have a positive effect.

This year, the Federal Office of Transport (FOT) revised and adopted the implementing provisions for the Railways Ordinance. These explicitly enshrine information security aspects for the first time. With the entry into force of the regulations on 1 November 2020, all railway companies are obliged to set up and operate an information security management system. However, the FOT has not specified any minimum requirements or any deadline for implementation. By specifying its expectations and providing resources, the FOT could offer significant support to railway companies.

Original text in German