

FREQUENTIS

Swiss Federal Railways Talks Punctuality, Digitalisation and Security

With digitalisation the cornerstone of the Swiss Federal Railways innovation strategy we look at how it protects its central rail communication platform with standardised security services that defend the service from cyber-attacks or threats.

The Swiss Federal Railways AG, which also goes by the abbreviation SBB, operates with a punctuality

rate of over 95 percent, making it one of the most reliable train services in Europe. This high reliability is only possible thanks to secure and fast communication between the operations centres and the staff in stations, on trains and on the tracks. And this track record is what makes rail travel in Switzerland the most preferred mode of local transport.

Digitalisation is a cornerstone of SBB's innovation strategy. The Group relies on secure digital networking in order to be able to expand its excellent customer service.

Austrian safety-critical technology supplier Frequentis provides its solution as a core component of the railway providers operational communication environment. This is an essential factor of SBB's reliability, connecting all stakeholders together in real-time, streamlining communication paths.

Within the framework of an almost 20-year co-operation with Frequentis, the operational communication environment of SBB has been continuously expanded and modernised, in order to ensure that employees in the operations centres can communicate quickly



and securely with train drivers, service staff on the trains and with other staff.

As a result of the increasing digitalisation of voice communication, the network infrastructure is under increasing pressure, which brings cyber security requirements to the fore.

IT threat scenarios, and the security requirements derived from them, have changed fundamentally. The topic of security and cyber security has led to a need for much more security in rail traffic itself, to ensure smooth operation continues.

Cyber Security Challenges and Standardised Security Services

In order to meet the many challenges in the area of cyber security, the combined SBB and Frequentis team developed a standardised security service catalogue of responsibilities, not only for systems and components but also for the associated processes. This ensures that SBB is optimally positioned with effective risk management for current security risks in the area of railway communication.

In view of the much-discussed ransomware attacks, SBB, together with Frequentis, has been working on the topic of cyber security even more intensively. The cross-company team has analysed the overall situation and developed a flexible security strategy.

For the systematic assessment of risks and the co-ordination of

suitable measures, SBB uses the Frequentis standardised security service catalogue, choosing services which can be dynamically adapted depending on changing security requirements, and which complement the cyber security requirements of SBB.

Improved Security and More Transparency

SBB benefits from better protection against security threats thanks to this security service catalogue. Together, the team of specialists from SBB and Frequentis have areas of prevention, intrusion and security monitoring, information security management, security risk management and requirements management and a cross-company responsibility matrix was also created, enabling SBB to ensure and optimise process transparency.

During implementation, the standardised security services were tailored to the requirements of SBB and also includes central security monitoring with intrusion detection and proactive early detection of threats. This means that unauthorised access attempts can be detected and managed in real time. This is of utmost importance for reliability, keeping passengers informed and railways moving. A flexible configuration with customer-specific threshold values enables intelligent and automated reactions to suspicious activities.

For prevention purposes, the

Frequentis Security Incident Response Team (SIRT) provides comprehensive information on security threats to the technology stack in use and, if necessary, works with SBB to develop measures to minimise the operational risk.

With the help of this information and processes, SBB can react more quickly to changed cyber security requirements.

Thanks to Frequentis Security Services, SBB can further improve the quality and availability of the railway and optimise operational processes. The services now protect 2,200 users and 650 end devices more effectively against attacks and other threats.

About Frequentis

Frequentis is an international supplier of communication and information systems for control centres with safety-critical tasks, leveraging 75 years of cross-domain experience in aviation, defence and transport. The company also holds the number one market share in GSM-R dispatcher terminal positions; more than 10,000 units have been delivered to customer control centres in over 25 countries. Railway customers include UK Network Rail, German Deutsche Bahn, Austrian ÖBB and Wiener Linien, and Australian Sydney Trains.

For more information visit our website www.frequentis.com.

