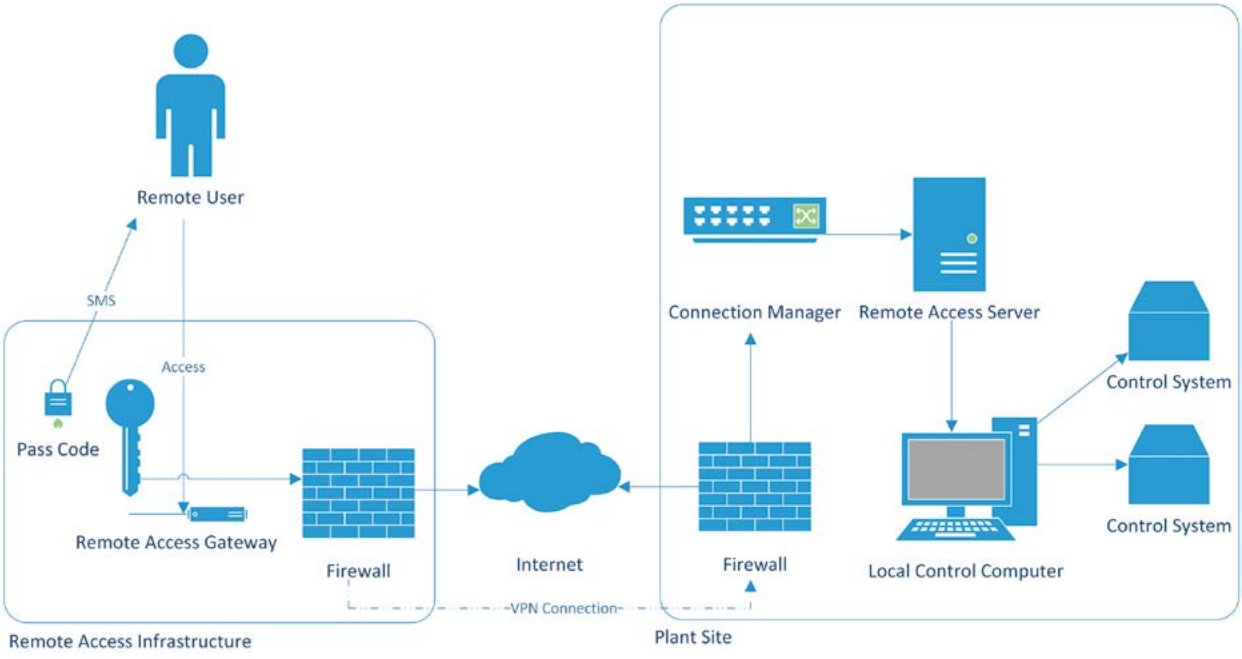
IT SECURITY IN RAILWAY TECHNOLOGY
CREATING A SECURE *STATE-OF-THE-ART* REMOTE ACCESS

English

Control technology within the rail energy supply is an important component. Frequently maintenance and service work are only possible within a time-consuming on-site deployment. A remote access for the operator and its service partners enables a flexible and less time-consuming way to check the condition of the plant and to carry out work. This remote access requires a technical protection against unauthorized access.

In critical operating situations a remote access enables the elimination of an operation impending defect within a short time. The challenge for the design of a remote access is to create a prior art secured access against a malicious third party access. A convenient access should be allowed for authorized parties. During the construction of substations and switching stations for train operators it is now necessary to establish a remote maintenance access which complies with the relevant IT security requirements. Besides pure control technology the necessary secure IT infrastructure is also to be set up.

The remote maintenance access allows maintenance and service technicians to take insight from afar into parts of the control system. If due to a fault an on-site deployment is required it can be selectively prepared by a remote fault analysis or even fixed remotely. Due to classification as a sensitive infrastructure the design and implementation had to consider the requirements of the BDEW whitepaper „Requirements for secure control and telecommunication systems“, which was developed for the general power supply and is updated according to technical progress.



Schematic diagram of the remote access

The created infrastructure consists of the technical solution including hardware and software as well as the organizational solution. These include the definition of responsibilities and processes. The remote maintenance access is independent of the operational management and does not interfere with it. As an entry point, a separate Citrix-based infrastructure was created. It can be accessed via a browser-based client and is authenticated by a domain registration and a SMS-session pass code. The actual access to the control system's location is established via a VPN connection which is permitted by the operator using a person-related authentication. The personalized access the site is passed to an infrastructure consisting of a connection manager and a virtualized server infrastructure.

From this application the local control computers of the control system can be reached. The remote access infrastructure is secure using restrictive access rules, a domain and a separate malware protection solution against unauthorized access. Different service partners and the plant operator can perform logically separated activities.

The established solution has a modular design and can serve as a basis for other facilities. Its advantage is the flexible, role-based access authorization and the secure three-factor authentication when logging on to remote maintenance portal. Using this various process control facilities can be accessed centrally after activation.

Within the project Lohsa/West an equivalent remote solution access has already been designed and implemented.

RAIL POWER SYSTEMS GMBH
Garmischer Straße 35 | 81373 Munich | Germany | T +49 89 41999-0 | F +49 89 41999-270 | info@rail-ps.com | www.rail-ps.com