

DATENSICHERHEIT IN DER BAHNTECHNIK

SCHAFFUNG EINES GESICHERTEN STATE-OF-THE-ART-FERNZUGRIFFS IN DER LEITTECHNIK

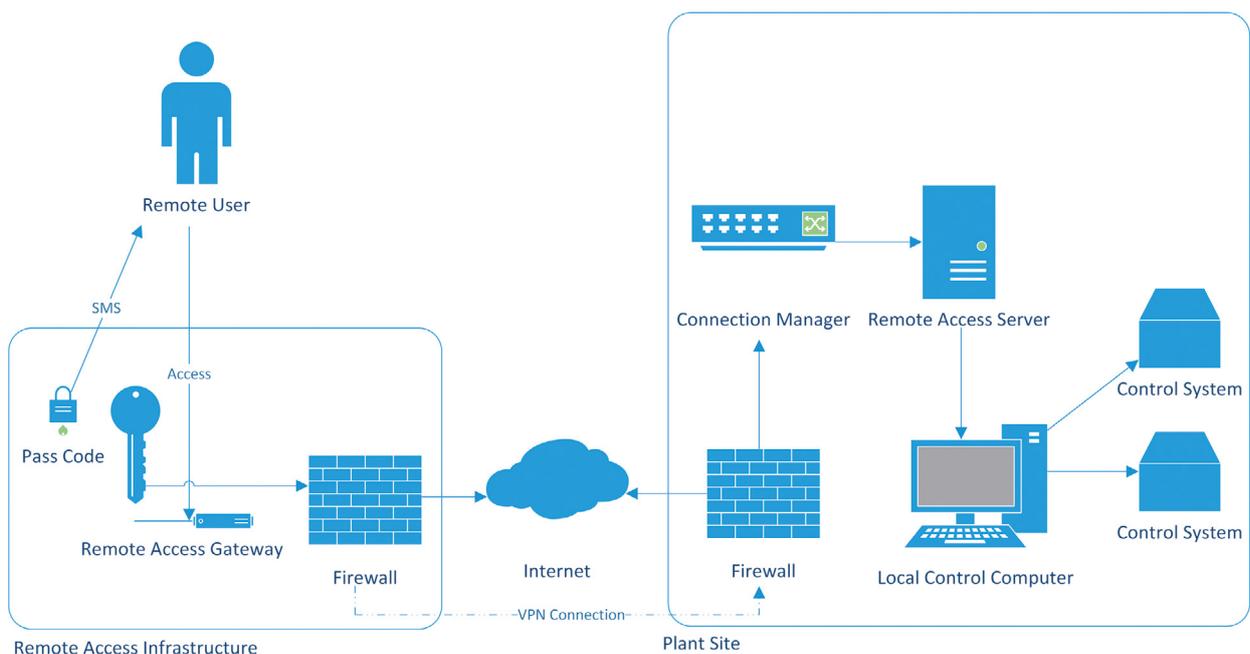
Deutsch

Leittechnik stellt innerhalb der Bahnenergieversorgung einen wichtigen Baustein dar. Wartungs- und Servicearbeiten sind dabei häufig nur innerhalb eines zeitaufwändigen Vor-Ort-Einsatzes möglich. Als Alternative dazu ermöglicht ein Fernzugriff dem Betreiber einer leittechnischen Anlage sowie seinen Service-Partnern eine flexiblere, weniger zeitintensive Möglichkeit den Zustand der Anlage zu prüfen, sowie Arbeiten durchzuführen.

In kritischen Betriebslagen ermöglicht ein Fernzugang die Behebung eines betriebsverhindernden Effekts innerhalb kürzester Zeit. Herausforderung an das Design eines Fern-

zugangs besteht in der Schaffung eines nach dem Stand der Technik gegenüber eines schädlichen Zugriffs Dritter gesicherten Zugangs. Dieser soll gleichzeitig den komfortablen Zugriff von autorisierten Parteien ermöglichen.

Innerhalb der Errichtung des Umrichterwerks Lohsa/West war ein Fernwartungszugang einzurichten, welcher den erforderlichen IT-Sicherheitsanforderungen entspricht sowie die dafür entsprechend notwendige sichere Infrastruktur aufzubauen.



schematisches Diagramm eines Fernzugriffs

Der Fernwartungszugang ermöglicht es Wartungs- und Servicetechnikern aus der Ferne Einblick in Teile der Steuerung des Umrichterwerkes zu nehmen. Falls infolge einer Störung ein Vor-Ort-Einsatz erforderlich wird, kann dieser durch eine Fehlerfernanalyse gezielt vorbereitet werden.

Aufgrund einer Einstufung als sicherheitskritische Infrastruktur waren bei der Gestaltung sowie Umsetzung die Anforderungen des BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ zu berücksichtigen.

Innerhalb dieses Projektes wurde das erste Mal ein derartiger Fernzugriff im Umfeld der Deutschen Bahn AG konzipiert und umgesetzt. Die geschaffene Infrastruktur besteht dabei aus der technischen Lösung (Hard- und Software) sowie den organisatorischen Lösungen (Definition von Verantwortlichkeiten und Prozessen). Der Fernwartungszugriff ist unabhängig von der Betriebsführung und greift nicht in diese ein oder beeinflusst sie.

Als Einstiegspunkt wurde auf Citrix-Basis eine exklusive Infrastruktur an den Rail Power Systems Rechenzentren in München und Offenbach geschaffen. Der Zugriff darauf erfolgt über einen browserbasierten Citrix-Client und wird durch eine Domänen-Anmeldung sowie einem SMS-Session-Pass-Code authentifiziert. Der eigentliche Zugriff auf den Flächenstandort erfolgt über eine VPN-Verbindung, die nach einer personengebundenen Authentifizierung bei der Zentralschaltstelle Leipzig der DB Energie aufgebaut wird.

Am Standort werden die personalisierten Zugriffe auf eine Infrastruktur, bestehend aus einem Verbindungsmanager sowie einer virtualisierten Server-Infrastruktur, geleitet. Von dieser aus sind die Nahsteuerungsrechner von Umrichter und Leittechnik erreichbar. Die Fernzugriff-Infrastruktur ist unter Verwendung von restriktiven Zugriffsregeln, einer Domäne sowie einer gesonderten Schadsoftwareschutzlösung gegen unautorisierte Zugriffe abgesichert. Verschiedene Servicepartner sowie der Betreiber der Leittechnik können logisch voneinander getrennt Tätigkeiten durchführen.

Die geschaffene Lösung ist modular gestaltet und kann in anderen Anlagen ausgerollt werden. Der Vorteil besteht in der flexiblen, rollenbasierten Zugriffsberechtigung sowie der sicheren 3 Faktor-Authentifizierung bei der Anmeldung am Fernmeldungsportal. Über dieses kann nach erfolgter Freischaltung zentral auf verschiedene leittechnische Anlagen zugegriffen werden.

© 2017. Alle Rechte sind der Rail Power Systems GmbH vorbehalten.

Die in diesem Dokument angegebenen Spezifikationen betreffen gängige Anwendungsbeispiele. Sie bilden nicht die Leistungsgrenzen ab. Im konkreten Anwendungsfall können daher abweichende Spezifikationen erreicht werden. Maßgeblich sind allein die im jeweiligen Angebot formulierten oder vertraglich vereinbarten Spezifikationen. Technische Änderungen bleiben vorbehalten. TracFeed® und CATMOS® sind eingetragene Warenzeichen der Rail Power Systems GmbH.