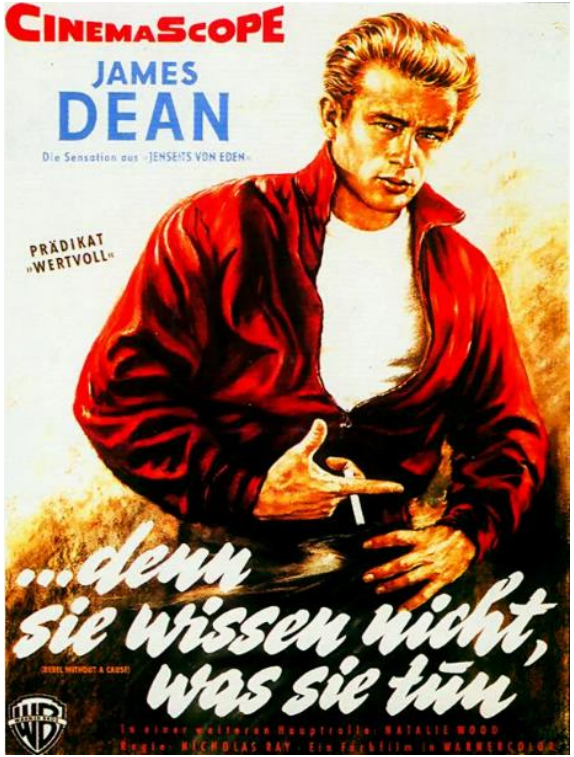
Umsetzung von sicheren OT-Netzen in den Umspannwerken der CKW AG

HSLU Netzwerke und Resilienz, 28. September 2023

CKW.

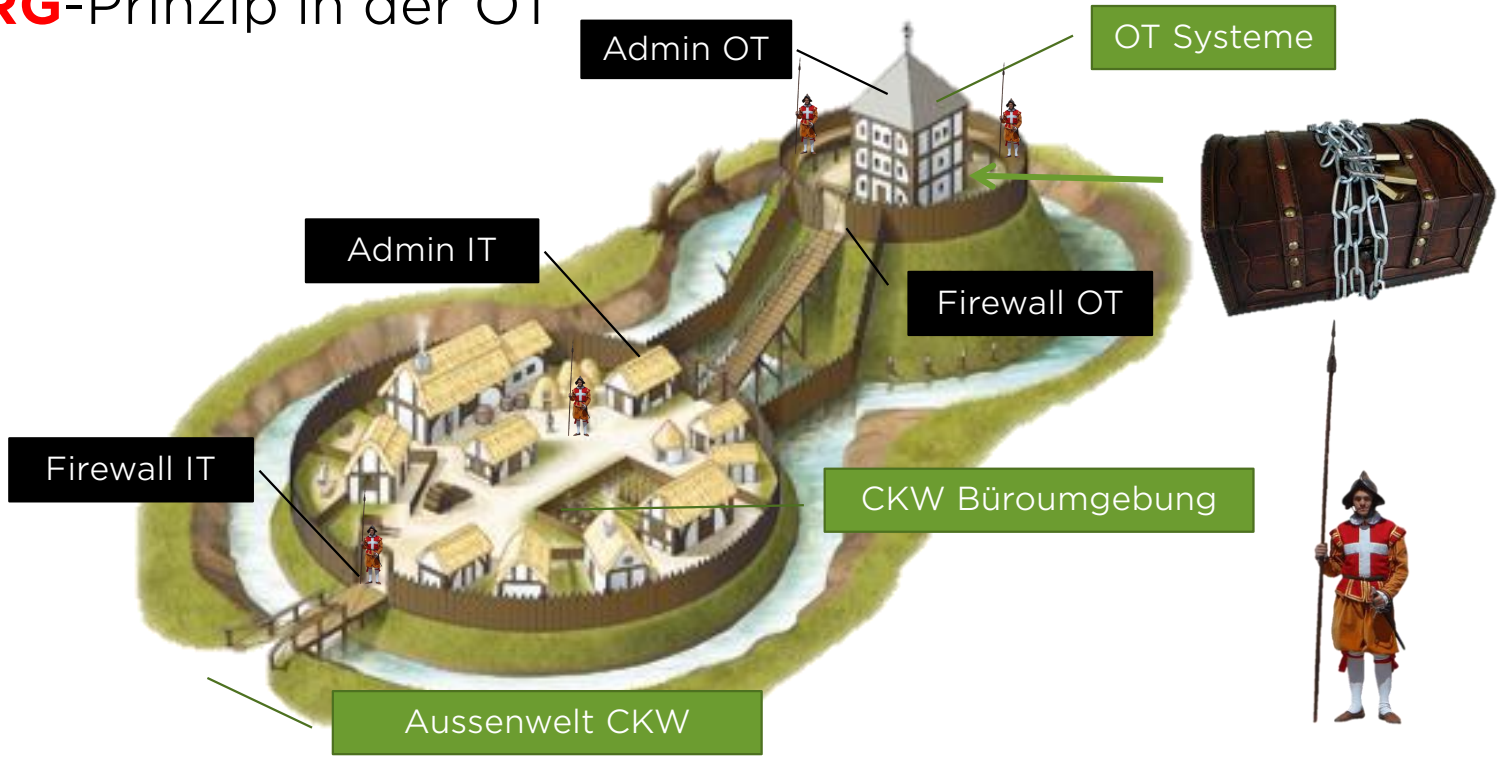
BURG-Prinzip als Beispiel der Unterstation ROTHEN**BURG**

!?!


CINEMASCOPE
JAMES
DEAN
Die Sensation aus »JENSEITS VON EDEN«
PRÄDIKAT
»WERTVOLL«
...denn
sie wissen nicht,
was sie tun

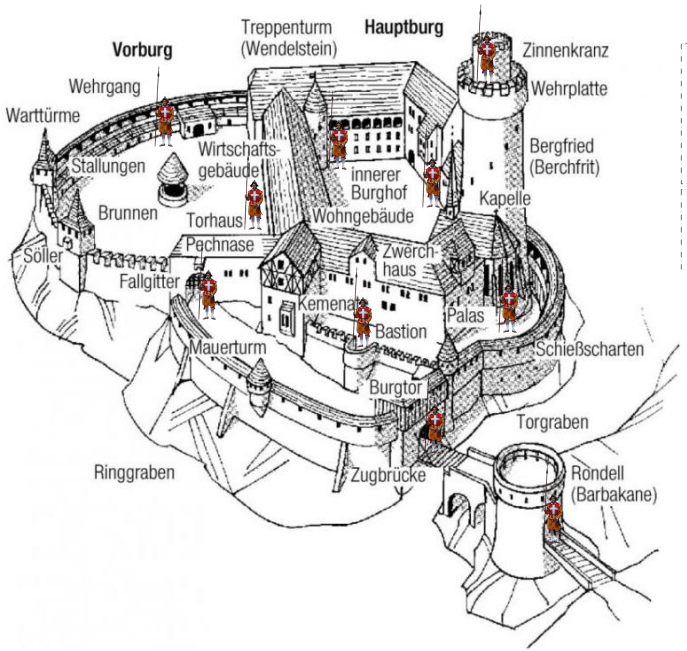
Grundsatz der Cyber Security bei CKW

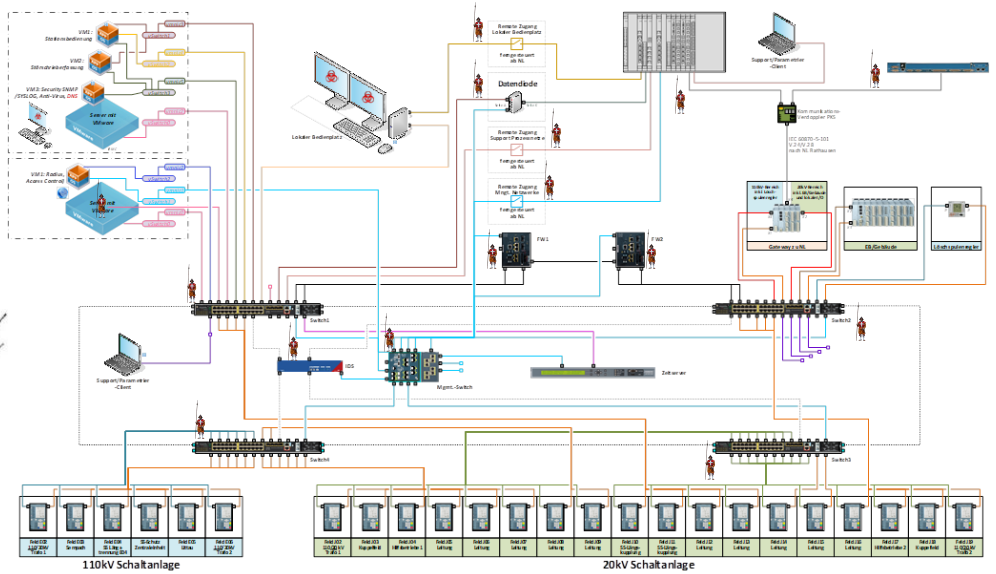
BURG-Prinzip in der OT



Defense-in-Depth in den Umspannwerken von CKW

BURG-Prinzip in der Unterstation ROTHEN**BURG**





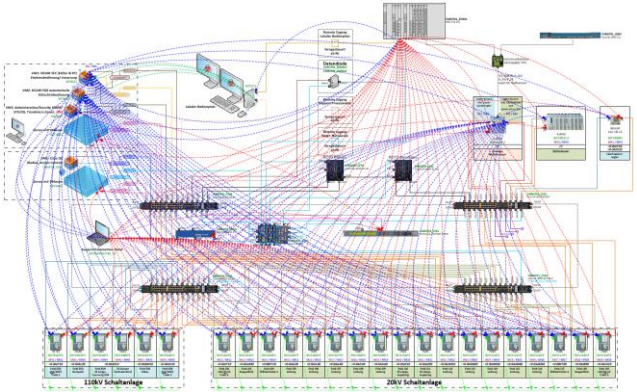
Grundsätze für Defence-in-Depth bei CKW

- Genügende und kontrollierte physische Sicherheit
- "Need to Know" Prinzip
- Keine stehenden Ethernet-Verbindungen zur Anlage (bei Bedarf zuschaltbar)
- Bei Bedarf nur vollverschlüsselte Verbindungen mit Protokollbrüchen
- Konsequente Inventarisierung und Überwachung von Elementen und Verbindungen
- Grösstmögliche Zonierung im Stationsleittechniknetzwerk
- Nur überwachte und gesteuerte Zugänge zum SLT-Netzwerk
- Kontrollierte und überwachte Zonenübergänge im SLT-Netzwerk
- Überwachung und Überprüfung des Contents im SLT-Netzwerk
- Definierte und zugewiesene Benutzerrollen / Anbindung AD
- Konsequentes AAA (Autorisierung, Authentisieren und Accounting)
- Schaffung der Basis für eventuelle forensische Untersuchungen

Physische Sicherheit

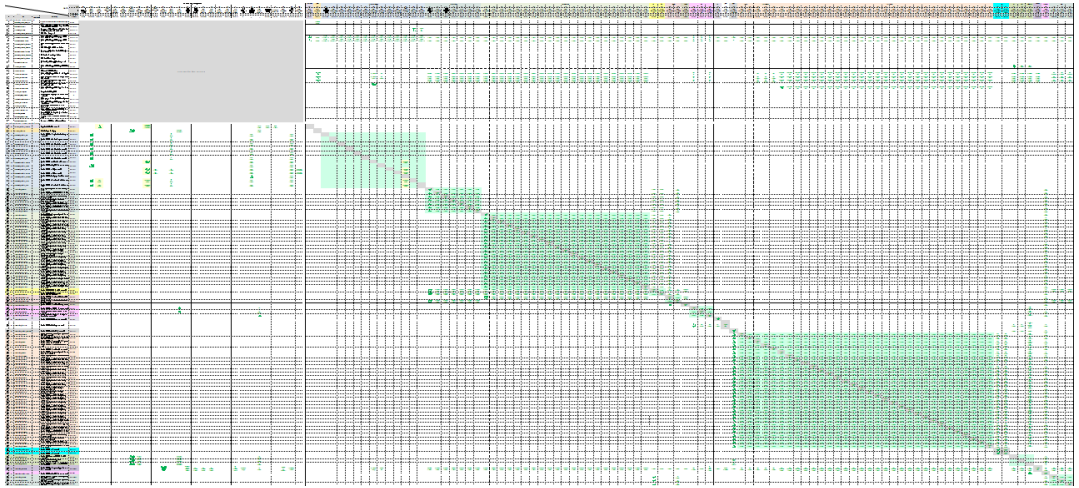
- Mehrere Zonen im Gebäude
- Überwachter Zugang ins Gebäude
- Einbruchmeldeanlage
- Zutrittskontrollsystem
- Zugang in Kernzone nur mit Zweifaktorauthentisierung
- Zentrale Zutrittsüberwachung durch CKW Netzleitstelle (24h)
- An- und Abmeldung bei Betreten der Anlage
- Zugang für Fremdfirmen nur in Begleitung durch autorisiertes CKW-Personal
- Einsatz von Fremdrechnern verboten (keine offenen Zugänge oder Ports)
- Alle nicht benutzten Ports ausgeschaltet oder physisch getrennt

Inventarisierung



- Konsequente Inventarisierung der vorhandenen Hard- und Software
- Konsequente Inventarisierung der nötigen MAC- und IP-Adressen (zukünftig Zertifikate)
- Konsequente Inventarisierung der nötigen Verbindungen bis auf Stufe TCP/IP und UDP
- Konsequente Inventarisierung aller Goose-Domänen, Goose-Message-Verbindungen, SV-Streams (IEC 61850)
- Erstellen und Pflegen von Verbindungsmatrizen und Zugängen
- Inventarisierung der nötigen Rollen für Nutzer und Benutzer
- Inventarisierung der nötigen Nutzer und Benutzer

Verbindungsmatrix mit Ports und Diensten

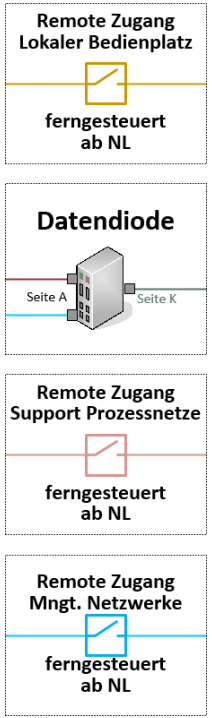


- Verbindungen zwischen >200 Host pro Umspannwerk (Intern und/oder Extern durch Zuschaltung)
- > 90 verschiedene Protokolle und Dienste
- > 100 verschiedene TCP/UDP-Ports

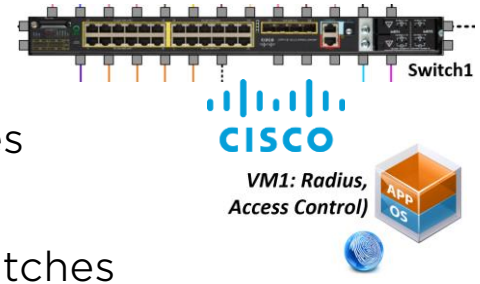
- **> 15'700 mögliche Verbindungen von verschieden Host, auf verschiedenen Host, via verschiedenen TCP/UDP-Port, via verschieden Protokollen --- für ein Umspannwerk**

Keine stehenden Ethernet-Verbindungen

- Kommunikation zum Netzleitsystem mittels IEC 60870-5-101 über eine vollverschlüsselte serielle Verbindung nach dem Gateway – Gateway Prinzip (ALF Application Layer Firewall)
- Schaltbare Remotezugänge für lokalen Bedienplatz, Support-, Prozess- und Management-Netzwerke
- Remote-Zugänge schaltbar über dediziertes System
- Konsequentes Logging der geschalteten Remotezugänge
- Autorisierung der Remotezugänge durch betriebsführende Organisation / Zugriff nur über dedizierte gehärtet Stationen
- Einsatz von Datendiode zur Übermittlung der Log- und Systemmeldungen wie auch der Asset- und Störschreiberdaten
- Protokollbrüche für Remotezugänge (RDP und TeamViewer)
- AAA durch lokale Identity Service Engine



Sichere Netzzugänge



- Statische Abbildung der Netzsegmente auf Stufe Switches
- Keine dynamischen Portzuweisungen auf Netzebene
- Konsequentes MAB (MAC-Adress-Bypassing) auf den Switches
- Vorbereitet für CAC (Certificate based Access Control)
- Periodische Prüfung der Zugänge und Reauthorisierung
- Zentral geführte Angaben der IED's
- Zugangssteuerung auf den Netzzugangsports mittels ACL (Access Control Lists) und Freigaben auf Stufe IP-Adressen und TCP-IP
- Permanente Überwachung der nötigen Netzzugänge auf Stufe Port
- Konsequentes Logging und Alerting

Maximale Segmentierung / Netzübergänge

- Maximale Segmentierung wir durch GOOSE-Domäne beschränkt GOOSE-Domäne pro Spannungsebene
- Funktionale Trennung zwischen Prozesstechnik, Spannungsebene, Gateway, Stationsbedienung und Support
- Netzübergänge an zentrale redundante Firewall
- Prinzip "Whitelisting" nach Vorgaben in Portmatrix
- Überprüfung der Verbindungszuständen (Aufbau, Bestand und Abbau)
- Separates Netzwerk für Überwachung und Steuerung des Prozessnetzwerkes inkl. Firewall und IDS
- Separierte Zugänge zur Datendiode für Leittechnik und Prozessnetzwerke
- Konsequentes Logging und Alerting
- Übermittlung via Datendiode an Splunk / PRTG und SIEM der CKW

Konsequentes AAA

- Das konsequente AAA (Autorisierung, Authentisieren und Accounting) erfolgt über ein zentrales OT-AD (Active Directory) und einen lokalen Radius-Server
- Alle Zugriffe auf Systeme für die Stationsbedienung, den lokalen Bedienplatz und die Störschrieberfassung erfolgen über das zentrales OT-AD und alle Zugriffe auf alle lokalen IED's erfolgen über den lokalen Radius-Server
- Es werden nur Userspezifische bzw. personalisierte Accounts erstellt
- Jedem User wird für jedem Zugriff die nötige Rolle bzw. die nötigen Berechtigungen nach IEC62351-8 erteilt und zugewiesen
- Es erfolgt ein konsequentes Logging und bei zu vielen Fehlversuchen ein Alerting
- Bei nichterreichen der Server sind Notfall-Accounts und Passwörter eingerichtet

Contentüberwachung

- Nach Prinzip "Whitelisting"
- Lokal: Verwendung der SCL-Files mit dezidiertem IDS
- Zentral: Verwendung von Cisco Firepower NGFW
- Implementation der Portmatrix
- Aktive Contentüberwachung / Feststellung von Anomalien
- Nur "Intrusion Detection" nicht "Intrusion Prevention"
- Logging und Alerting / Übermittlung über Datendiode an Splunk
- Verarbeitung der Daten im SIEM der CKW
- Wichtige Basis für eventuelle forensische Untersuchungen

- **> 15'700 mögliche Verbindungen von verschieden Host, auf verschiedenen Host, via verschiedenen TCP/UDP-Port, über verschiedene Protokolle --- pro Umspannwerk**

Cisco-Produkte für sichere OT-Netze bei CKW

- Cisco Industrial Ethernet 4010 Switch -- lokal im Umspannwerk
- Cisco Industrial Ethernet 3300 Switch -- lokal im Umspannwerk
- Cisco Secure Firewall ISA3000 -- lokal im Umspannwerk
- Cisco Identity Services Engine (ISE) -- lokal im Umspannwerk
- Cisco ASA 5500-X mit FirePOWER Services -- Zentral in OT
- Cisco Identity Services Engine (ISE) -- Zentral in OT
- Cisco Secure Network Analytics (SNA) -- Zentral in OT
- Cisco Security Manager (CSM) -- Zentral in OT
- Cisco Secure Firewall Management Center (FMC) -- Zentral in OT

Wieso Cisco-Produkte in Umspannwerken ?

- Lüfterlos, konvektionsgekühlt, ohne bewegliche Teile.
- Erweiterter Betriebstemperaturbereich (-40 bis 75 °C).
- Widerstandsfähig gegen Vibrationen, Stösse, Überspannungen und elektrisches Rauschen
- Entspricht den branchenübergreifenden Spezifikationen für industrielle Automatisierung, ITS und elektrische Umspannwerke.
- Verbessert die Betriebszeit, Leistung und Sicherheit von industriellen Systemen und Geräten = MTBF 415'160h / 47 Jahre
- Weiterleitung mit niedriger Latenzzeit und fortschrittlichen Hardware-Unterstützungsfunktionen (z. B. NAT, IEEE1588)
- Alarm-E/A zur Überwachung und Signalisierung an externe Geräte.

Wieso Cisco-Produkte in Umspannwerken ?

- IEC 61850-3 Kommunikationsnetze für die Automatisierung von Energieversorgungsunternehmen:
  - Manufacturing Message Specification (MMS)
  - GOOSE-Nachrichten
  - Sampled Values (SV)
- IEEE 1588v2 Precision Time Protocol (PTP) Power Profile 2011 und 2017
- Parallel Redundancy Protocol (PRP), PTP over PRP
- **… und natürlich die Netzwerk- und Sicherheitsfunktionen wie wir es in der klassischen OT und IT verwenden**

Einfach:

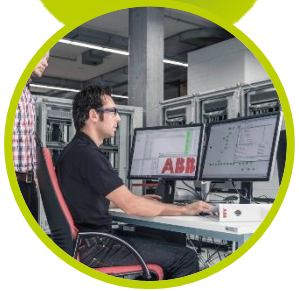
Professional Networking for Substation Automatisation

Sichere Netze im Umspannwerken

Der Schlüssel zum Erfolg bei der Umsetzung

Leittechnik

Schutztechnik



Netzwerk- und Cyber-Security-Technik

Schlüsselfaktoren

- Zusammenarbeit
- Austausch
- Know How
- Innovation
- Erfahrungen

Ganz einfach, oder?
Haben sie noch Fragen?

Danke.

CKW.