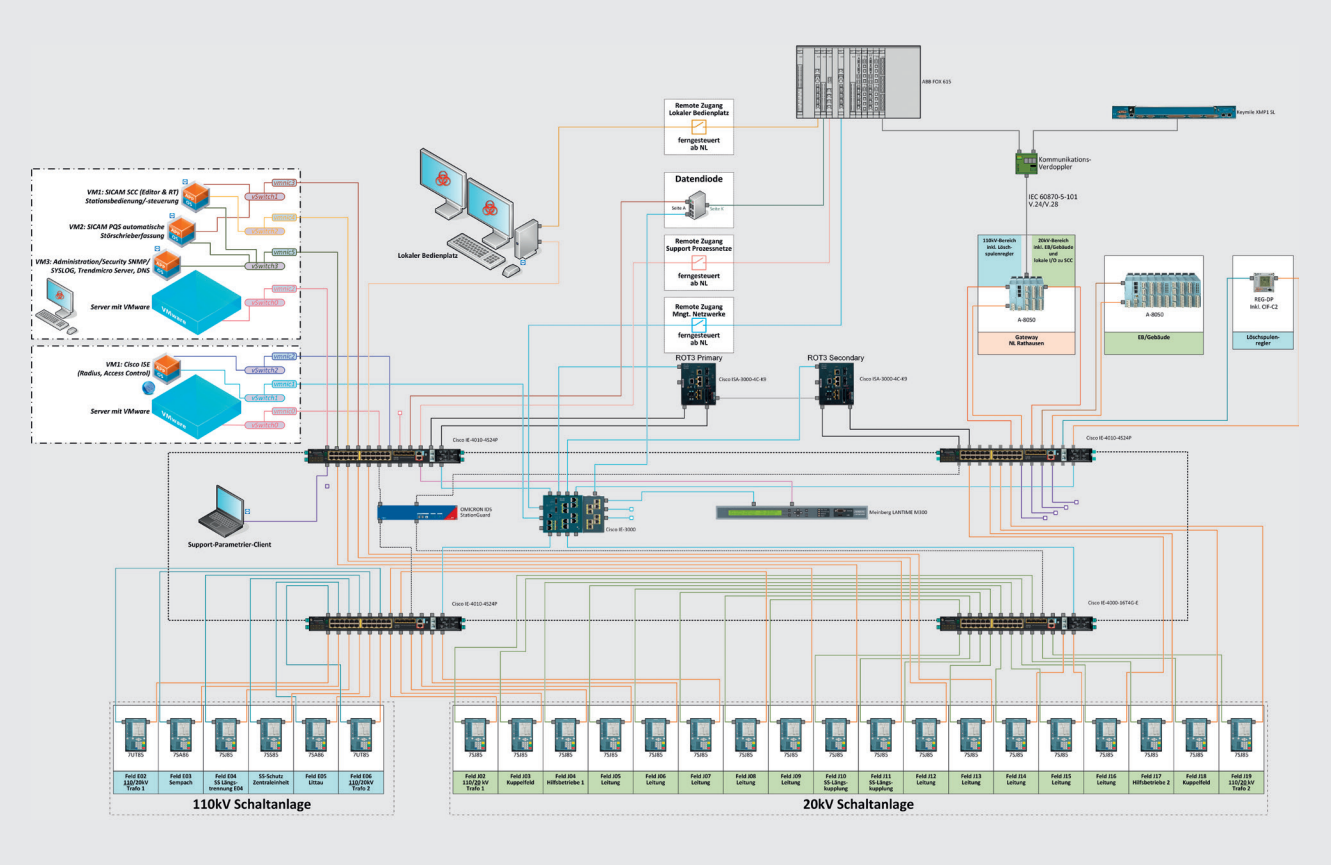

Prozessnetzwerk der Unterstation Rothenburg.

Sichere Leittechnik

Cyber Security in der Unterstation Rothenburg | Damit Schaltanlagen umfassend vor Cyber-Angriffen geschützt sind, muss die Sicherheitsstrategie auf allen Ebenen ansetzen. Sie umfasst die physische und die digitale Zugriffskontrolle und reicht bis zur Überwachung und Erkennung verdächtiger Aktivität im Netzwerk. Dazu braucht es Systeme, die langfristig ein hohes Mass an Sicherheit und Flexibilität bieten.

YANN GOSTELI, ANDREAS KLIEN

In den Jahren 2016/2017 begann das Projektteam der CKW (Centralschweizerische Kraftwerke AG) mit der Planung der neuen Unterstation (US) Rothenburg, die 2020 in Betrieb gehen wird. Hierzu gehörte unter anderem das Erstellen der Ausschreibungsgrundlagen für die Sekundärtechnik. Mit der in den Jahren 2017 und 2018 durchgeführten Ausschreibung definierte CKW diesen neuen Standard für die folgenden Jahre, der auf Schutz- und Leittechnikkomponenten von Siemens setzt. Den Netzwerkteil realisiert CKW selbst. Neben den üblichen Aufgaben für die Entwicklung des Unterstations-Konzepts sollte sich das Projektteam mit der Integration der neuesten Ergebnisse aus dem Bereich Cyber Security, erarbeitet beim VSE (Verband Schweizerischer Elektrizitätsunternehmen), befassen und diese berücksichtigen. Dieser neue Standard führt nun zu einer signifikanten Erhöhung der Operational Technology (OT) Security in den Anlagen und wird im ersten Teil des Artikels beschrieben.

Die Steigerung der OT-Sicherheit wird nicht zuletzt durch eine neue Komponente im Konzept der Stationsleittechnik respektive für die Überwachung der Netzwerke in der US erreicht, einem Intrusion Detection System (IDS). CKW entschied sich zu dessen Einsatz, da sie ihre Erfahrung mit Cyber Security in Stationsnetzwerken für nicht fundiert genug einschätzte, deswegen soll ein IDS eventuell auftretende Unstimmigkeiten im Netzwerkverkehr aufdecken. Ein wesentliches Kriterium bei dessen Auswahl war, dass die Bedienung und alle Meldungen in einer für den klassischen Leittechniker verständlichen Form dargestellt werden. Dazu startete das Projektteam parallel zur Ausschreibung ein Pilotprojekt mit der Firma Omicron, das im zweiten Teil des Artikels beschrieben wird.

Bilder: CKW, Omicron

Sekundärtechnik und Security by Design

Das Thema Sicherheit im Bereich der Stationsleit- und Schutztechnik hat bei CKW in den letzten Jahren stark an Bedeutung gewonnen. Dies ist durch Empfehlungen aus der Branche und vor allen Dingen durch OT-Security Assessments der vergangenen Jahre begründet. Diese Assessments zeigten Schwachstellen sowohl in der Netz- als auch der Stationsleittechnik. Im Bereich der Stationsleittechnik zeigten sich beispielsweise unsichere Zonenübergänge und einige kritische Zugänge zu Stationsleitrechnern oder Netzwerkbereichen. Derzeit besteht noch keine Möglichkeit, im Netzwerk der Stationsleittechnik zu beurteilen, ob aktuell ein Angriff stattfindet, oder ob es dort verdächtige Aktivitäten gibt, die auf einen bevorstehenden Angriff hindeuten könnten. CKW hat es sich aufgrund dieser Erkenntnisse zum Ziel gesetzt, die wesentlichen Schwachstellen zu beseitigen und unter Berücksichtigung des neuen US-Standards die Vorgaben für den sichereren Bau von Netzwerken zu verschärfen.

Neben der Arbeit am US-Konzept 2020 veröffentlichte eine Arbeitsgruppe des VSE als Branchenempfehlung das Handbuch «Grundschutz für ‹Operational Technology› in der Stromversorgung». CKW konnte sich in dieser Arbeitsgruppe engagieren und integrierte die dabei gewonnenen Erkenntnisse und Ansätze kontinuierlich in die eigenen Vorgaben. Das Branchendokument beschreibt einen Defense-In-Depth-Ansatz für die Sicherung der Netze in der OT. Dabei werden Daten-, Informations- und operationale Sicherheit sowohl umfassend als auch in der Tiefe betrachtet. Dazu gehören neben der Erstellung und Einführung von Zonenkonzepten auch deren Überwachung sowie das Erkennen und Reagieren auf bestimmte Ereignisse. Mit der Überwachung und Erkennung wird beabsichtigt, mögliche Auswirkungen, die durch Angriffe entstehen können, in den Anlagen zu minimieren.

Entwurf eines sichereren Netzes für die US Rothenburg

Im Netzwerkentwurf der US Rothenburg werden in jedem Bereich Hürden eingebaut, die einen Angiff auf das Netzwerk erschweren sollen. Das Einstiegsbild zeigt das Prozessnetzwerk der US Rothenburg.

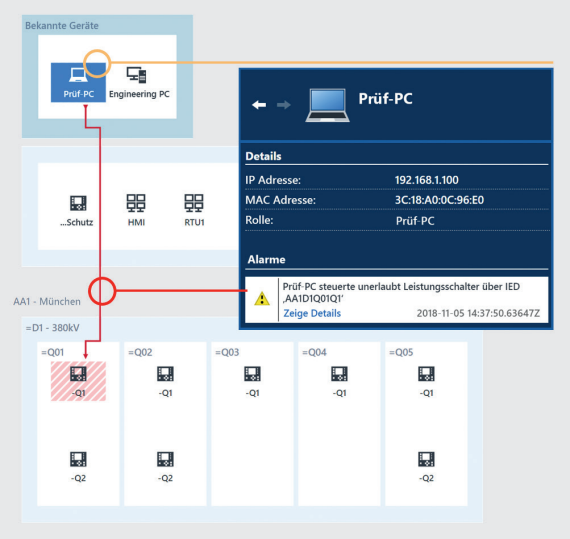

Bild 1 Grafische Alarmanzeige anstelle einer kryptischen Ereignisliste.

In diesem Prozessnetzwerk wurde eine Reihe von Sicherheitsaspekten berücksichtigt. An erster Stelle stehen die IP-Verbindungen der Anlage zur Aussenwelt, die im Normalbetrieb deaktiviert sind. Verbindungen für Remote-Zugänge werden nur bei Bedarf freigeschaltet. Die Kommunikation zum Netzleitsystem erfolgt mit dem Protokoll IEC 60870-5-101. Alle Zugriffe auf die Komponenten für Supportzwecke erfolgen ausschliesslich über spezielle zentrale Arbeitsstationen, welche entsprechend gehärtet sind. Diese Zugänge werden bei Bedarf von fern zugeschaltet.

Die Zugriffsrechte sind dediziert geregelt. Das Scada-System, das Störschreibererfassungssystem sowie das Security-System werden virtualisiert auf einem Server betrieben. Der lokale Bedienplatz greift nur mit Remote-Desktop-Verbindungen über eine lokale Firewall auf diese Systeme zu. Die Benutzer müssen sich auf diesen Arbeitsstationen über ein zentrales Active Directory (AD) anmelden, über welches sie die erforderlichen Rechte und Freigaben zugeteilt erhalten. Der Zugang zum zentralen AD wird bei Bedarf von einer zentralen Stelle freigeschaltet. Zudem müssen sich die Benutzer an jedem IED der Stationsleittechnik mit individuellen Passwörtern anmelden und erhalten vom Access-Control-Server mittels Radius die entsprechenden Rechte zugeteilt. Das gilt sowohl für den Zugriff auf die Geräte mit Parametriertools wie auch bei der Bedienung am Display. Dabei werden keine Standardpasswörter verwendet.

Sämtliche am Netzwerk angeschlossenen Clients werden gehärtet. Das geschieht unter anderem durch den Einsatz der Windows-Firewall mit Berücksichtigung der Kommunikationsmatrix und rollenabhängig durch Sperren nicht erforderlicher Funktionalitäten der Betriebssysteme. Darüber hinaus erfolgt jeder Zugang zum Netzwerk über MAC Authentication Bypass, womit nur registrierte Komponenten mit dem Netzwerk Verbindung aufnehmen können. Dabei müssen auch die Reservegeräte im Störungsfall vom Switch erkannt und akzeptiert werden. Mit Hilfe von Access-Control-Listen wird für jeden Switch-Port festgelegt, welches Gerät mit welchem Protokoll mit anderen Netzwerkteilnehmern kommunizieren darf.

Das Prozessnetzwerk und das Supportnetzwerk sind logisch und physisch getrennt. Die Kommunikation mit dem Protokoll IEC 61850 Ed. 2 wird folglich auf einer anderen Schnittstelle realisiert als der Zugriff zu den Geräten für die Parametrierung oder Wartung. Das gesamte Prozessnetz ist segmentiert, wobei unter anderem die folgenden Segmente gebildet und über eine redundante Firewall getrennt werden:

- 110 kV (Goose und MMS)
- 20 kV (Goose und MMS)
- Kleinleitstelle
- Gateway RTU
- Nebenanlagen
- Support-Netze für IEC und Clients
- Management-Netzwerk, VM, Radius

Die Datentransfers aus der Anlage in übergeordnete Netzwerkbereiche werden über eine Datendiode realisiert.

Diese Datendiode stellt sicher, dass kein Netzwerkverkehr von ausserhalb in die Anlage gelangen kann. Mit einem Whitelisting-Ansatz überwacht zudem ein IDS den ganzen Netzwerkverkehr in der Anlage. Es meldet einerseits via Leittechnik einen Alarm an die Netzleitstelle und stellt andererseits Informationen für übergeordnete Security-Management-Systeme zur Verfügung. Das IDS ist die wesentliche Komponente für das Erkennen von Angriffen oder Auffälligkeiten im Stationsnetz.

Netzwerküberwachung in Schaltanlagen

Das neue US-Konzept 2020 von CKW beruht auf der Einrichtung von Netzwerksegmenten, die jeweils durch eine Firewall getrennt sind. Die Parametrierung der Firewall gibt genau vor, mit welchen Protokollen über die Segmente hinweg kommuniziert werden darf. Allerdings können auch über die von der Firewall erlaubten Protokolle wie beispielsweise Engineering-Protokolle und das in IEC 61850 benutzte MMS- und Goose-Protokoll potenziell Geräte angegriffen und mit Schadsoftware infiziert werden. Genau solche Szenarien will CKW verhindern, indem sie den Netzwerkverkehr mit einem IDS überwachen, um frühzeitig unerlaubte Vorgänge zu erkennen. Omicron forscht seit 2011 an einem Ansatz für Intrusion Detection in IEC 61850-Schaltanlagen und wurde 2017 von Ingenieuren der CKW angesprochen, die auf der Suche nach einem Intrusion-Detection-System für das neue US-Konzept waren. Die Techniker von CKW kannten die Nachteile aktuell verfügbarer IDS-Systeme und eine wichtige Vorgabe war daher, dass das IDS von den verantwortlichen Schutz- und Leittechnikern einfach bedient werden kann. 2018 wurde eine der ersten Proof-of-Concept-Installationen von StationGuard, einem IDS von Omicron, in einer 110-kV-Schaltanlage von CKW in Betrieb genommen. Mittlerweile flossen auch Erfahrungen von anderen Energieversorgern weltweit in die Entwicklung dieses IDS ein.

Die meisten IDS-Systeme für OT verwenden einen «lernbasierten» Ansatz. Dabei wird zunächst über Wochen hinweg der übliche Zustand im Netzwerk erlernt. Anschliessend wird im Normalbetrieb immer dann alarmiert, wenn die Netzwerkkommunikation signifikant vom erlernten Status abweicht. Dies hat zur Folge, dass für alle Vorgänge Fehlalarme ausgelöst werden, die während der Lernphase nicht auftraten. Hierzu gehören beispielsweise Schutzauslösungen, Schalthandlungen oder routinemässige Prüfungen. Da das System die tatsächlichen Ereignisse in der Anlage nicht kennt, beziehen sich die Alarmmeldungen rein auf Protokolldetails. Damit entsteht also eine hohe Anzahl von Fehlalarmen, für deren Überprüfung IT-Spezialisten mit Anlagenkenntnissen erforderlich sind. Ein solcher Aufwand wäre für die meisten EVUs nicht tragbar.

Ansatz in StationGuard

Bei IEC 61850-Anlagen liegt das gesamte Automatisierungssystem mit allen Geräten, den Datenmodellen und den Kommunikationsmustern in einem standardisierten Format vor, der SCL (Substation Configuration Language). Daraus erstellt das IDS ein Systemmodell der Anlage und vergleicht anschliessend jedes Netzwerkpaket mit dem Live-Systemmodell. Dieser Prozess ist ohne Lernphase möglich, allein durch die praktisch automatische Konfiguration über SCL und mit wenigen manuellen Ergänzungen. Aufgrund der kontinuierlichen inhaltlichen Überprüfung des Datenverkehrs werden nicht nur Bedrohungen für die IT-Sicherheit erkannt, wie unzulässige Pakete und Steuervorgänge, sondern auch Kommunikationsfehler und andere Fehlfunktionen in der Anlage. Ein Beispiel: Allein für Goose kennt das IDS aktuell 35 verschiedene Alarmcodes, die auftreten können. Sie reichen von einfachen Sequenznummer-Störungen bis hin zu komplexeren Problemen, wie zu langen Übertragungszeiten.

Neben der Vermeidung von Fehlalarmen ist es entscheidend, dass die angezeigten Alarmmeldungen für die verantwortlichen Leittechniker klar verständlich sind, damit sie besser, einfacher und vor allen Dingen schneller beurteilen können, welche Vorgänge einen Alarm ausgelöst haben. Damit sich die Alarme auch besser den auslösenden Feldern und Geräten zuordnen lassen, werden sie im IDS nicht nur als Alarmliste geführt, wie man das von Firewalls kennt, sondern auch grafisch dargestellt. **Bild 1** zeigt einen Screenshot der grafischen Alarmanzeige des IDS: Der Alarm wird als roter Pfeil zwischen dem Gerät (Prüf-PC), der die verbotene Aktion ausführt, und dem «Opfer» der Aktion angezeigt.

Wartungsmodus

Um Fehlalarme weiter zu reduzieren, berücksichtigt das IDS auch Prüf- und Wartungsvorgänge im Systemmodell der Anlage. Die Prüfausrüstung, einschliesslich der Schutzprüfgeräte, kann der Techniker am IDS vorab bekannt geben und anschliessend das IDS in einen Wartungsmodus schalten, in dem die Prüftechnik verwendet werden darf, ohne einen Alarm auszulösen. Wird der Engineering-PC oder Prüflaptop zu einem anderen Zeitpunkt als der Wartung verwendet, sendet das IDS sofort einen Alarm. Dabei ist zu beachten, dass StationGuard rein passiv agiert: Ist eine Aktion nicht erlaubt, wird ein Alarm ausgelöst, jedoch nicht aktiv in die Anlage eingegriffen. Mit den Binärausgängen des IDS können die Alarme auch unkompliziert über das Gateway an die Leitstelle übermittelt werden. In diesem Fall erfolgt die Meldung ohne Netzwerkkommunikation und die Alarme lassen sich wie jedes andere fest verdrahtete Signal der Anlage in die Leittechnik-Signalliste integrieren. Alternativ ist es auch möglich, Alarme über entsprechende Protokolle an ein Security Incident Event Management System (SIEM) weiterzuleiten.

Fazit

Die hier beschriebenen Massnahmen erfordern ein Umdenken bei allen Beteiligten in der Realisierung von Projekten. Hierzu gehört der Umgang mit neuen Schnittstellen sowie der steigenden Komplexität im System, was vollkommen neue Kompetenzen erfordert. Eine gute Zusammenarbeit der unterschiedlichen Disziplinen wird dadurch immer wichtiger. Während des FAT (Factory Acceptance Test) bei Siemens hat das System seine Feuertaufe bereits bestanden. Ende des Jahres wird es den Betrieb in der Unterstation Rothenburg aufnehmen.

Autoren

Yann Gosteli leitet den Bereich Sekundäranlagen bei der Centralschweizer Kraftwerke AG.
→ CKW AG, 6002 Luzern
→ yann.gosteli@ckw.ch

Andreas Klien leitet den Geschäftsbereich Power Utility Communication (PUC) bei Omicron.
→ Omicron, AT-6833 Klaus
→ andreas.klien@omicronenergy.com