Erkennen von Cyberangriffen in digitalen Schaltanlagen – ein neuer Ansatz

Andreas Klien, OMICRON electronics GmbH, Klaus, Österreich
andreas.klien@omicronenergy.com

1 Zusammenfassung

Um die Cybersicherheit von digitalen Schaltanlagen sicherzustellen, sind Überlegungen auf mehreren Ebenen erforderlich. Mit Verschlüsselungsverfahren können zwar Geräte authentifiziert werden, allerdings verhindern diese Maßnahmen nicht alle Angriffe. Firewalls und „Air Gaps“ lassen sich mit vorhandenen Remote-Access-Tunneln oder durch Wartungscomputer, die direkt an die IEDs oder den Anlagenbus angeschlossen sind, umgehen. Deshalb erfordert es Maßnahmen für das Erkennen von Angriffen, die schnelle Reaktionszeiten sicherstellen und die Folgen auf ein Minimum reduzieren.
Seit mehreren Jahren kommen zu diesem Zweck sogenannte „Intrusion Detection Systems“ (IDS) zum Einsatz. Dabei handelt es sich um Systeme die das unberechtigte Eindringen in Netzwerke erkennen lassen. Da aber nur eine kleine Anzahl von Cyberangriffen auf Anlagen bekannt ist und selbst ein erstmaliger Angriff schwerwiegende Folgen haben kann, muss das IDS in der Lage sein, Angriffe auch ohne das Vorliegen entsprechender Signaturen erkennen zu können.
Bei einigen Herangehensweisen versucht man unbekannte Angriffe durch „Lernen“ zu erkennen, das heißt, das System lernt, wie häufig bestimmte Protokollmarker auftreten. Dies führt in vielen Fällen dazu, dass ein falscher Alarm ausgelöst wird, wenn ein selten vorkommendes, aber legitimes Ereignis eintritt.
In diesem Artikel wird eine neue Herangehensweise für das Erkennen von Angriffen in digitalen Schaltanlagen vorgestellt. Dabei wird zur Unterscheidung zwischen legitimen und böswilligen Aktivitäten ein Systemmodell des IEC-61850-Stationsautomatisierungssystems und der Schaltanlage genutzt. Da die gesamte Kommunikation verifiziert wird, lassen sich nicht nur sicherheitsrelevante Angriffe erkennen, sondern auch Kommunikationsfehler und Ausfälle von Betriebsmitteln. Die Konfiguration wird automatisch aus der SCD-Datei der IEC-61850-Anlagen abgerufen, sodass das System ohne Lernphase einsatzbereit ist.
Im Anschluss an die Vorstellung der Software- und Hardwarevoraussetzungen für ein Schaltanlagen-IDS wird die Herangehensweise ausführlich erklärt, die in StationGuard von OMICRON Verwendung findet. Der Artikel schließt mit einem Praxisbeispiel für die Umsetzung dieser Herangehensweise.

2 Angriffsvektoren bei Anlagen

Für diesen Artikel definieren wir den Cyberangriff auf eine Anlage als ein Ereignis, bei dem ein Angreifer einen Dienst von mindestens einem Gerät für den Schutz, die Automatisierung oder die Steuerung in der Anlage verändert, deaktiviert oder dessen Funktion beeinträchtigt. Eine typische Anlage kann über alle in Abbildung 1 dargestellten und nummerierten Pfade angegriffen werden. Ein Angreifer könnte über die Verbindung zur Leitstelle (1) eindringen, wie es bei einem der Cyberangriffe in der Ukraine geschah, bei dem die Firmware von Gateway-Geräten verändert wurde was zu deren Zerstörung führte. Einen weiteren Eintrittspunkt stellen Wartungs-PCs (2) dar, die an die Anlagenausrüstung angeschlossen sind. Verbindet ein Schutztechniker seinen Computer mit einem Relais, um die (Schutz-)Einstellungen zu ändern, könnte Malware auf dem PC wiederum Malware auf dem Relais installieren, ähnlich wie es etwa beim Cyberangriff Stuxnet mit den PLCs geschehen ist. Bei der Prüfung von IEC-61850-Systemen werden die verwendeten Laptops oft unmittelbar an den Anlagenbus angeschlossen und können so potenziell IEDs (3) infizieren. Aus diesem Grund gibt es neue IEC-61850-Prüflösungen, die eine gegen Cybergefahren sichere Trennung zwischen dem Prüfcomputer und dem Anlagennetzwerk sicherstellen. Somit bleibt nur noch das Prüfgerät (4) als potenzieller Eintrittspfad. Deshalb müssen Hersteller von Prüfgeräten in die Härtung ihrer Geräte investieren, um zu verhindern, dass dieser Eintrittspfad nicht durch einen Angreifer ausgenutzt werden kann.
Die Speicherung von Einstellungen (2a) und von Prüfdokumenten (3a) kann ebenfalls eine Quelle sein. Dieser Storage Server ist somit ebenfalls für die Perimeter-Sicherheit entscheidend. Aus diesem Grund ist es sinnvoll, für diese Daten eine getrennte, isolierte und geschützte Datenmanagement-Lösung einzuführen.

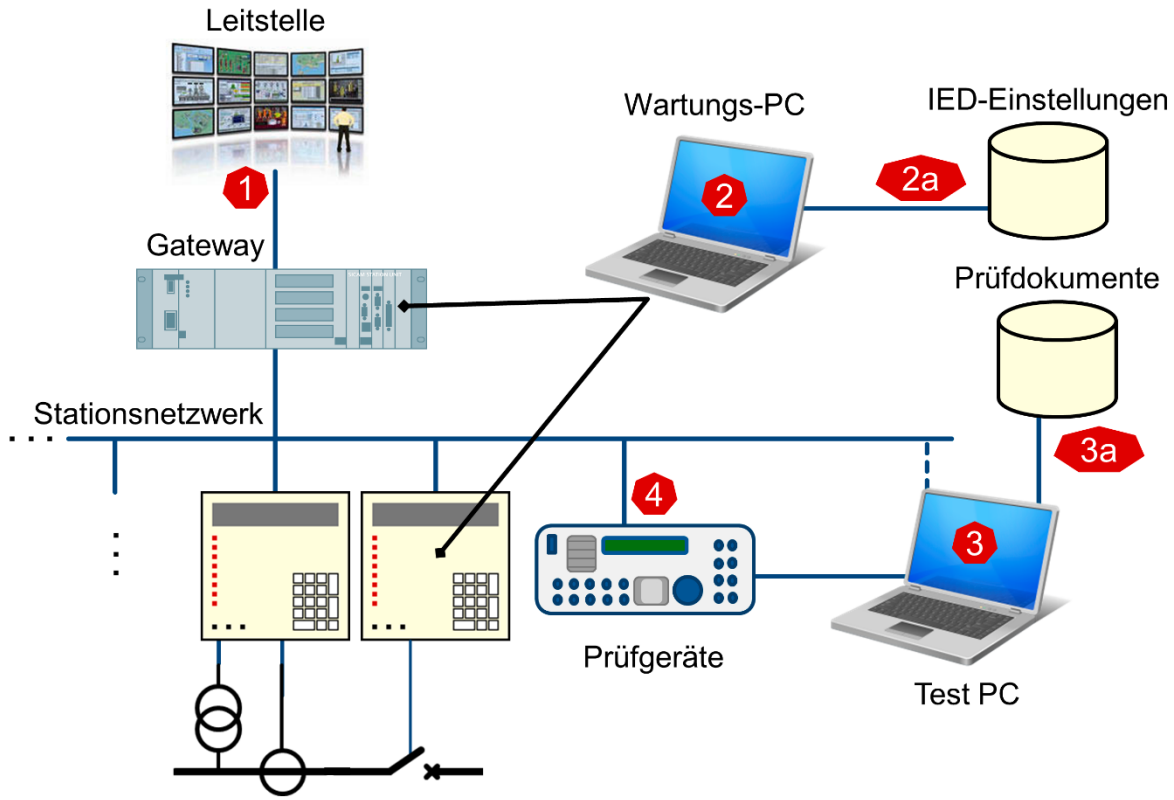

Abbildung 1 Angriffsvektoren einer Anlage

3 Sicherheit in IEC-61850-Anlagen

Eine häufig gestellte Frage zur Cybersicherheit in IEC-61850-Anlagen lautet: *„Wie kann ich verhindern, dass ein Angreifer eine Trip-GOOSE in den Anlagenbus einspeist?“* Für diese Frage sollten wir uns nicht auf den Fall beschränken, in dem der Angreifer einen physischen Zugang zum Anlagennetzwerk hat. Eine solche Situation kann auch aufgrund anderer Umstände eintreten: ein infizierter Wartungs- oder Prüf-PC, der an den Anlagenbus angeschlossen wird, oder sogar über ein infiziertes IED, das eine GOOSE einspeist. In diesem Zusammenhang werden die Status- und Sequenznummern in der GOOSE-Nachricht sehr oft als „GOOSE-Sicherheitsmechanismen“ bezeichnet. Allerdings sollten solche Maßnahmen heute nur mehr als Schutz gegen versehentliches einspeisen bezeichnet werden, da Angreifer natürlich die aktuelle Status- und Sequenznummer abhören und geeignete Werte fälschen können. Darüber hinaus lässt sich die MAC-Adresse des Absenders des GOOSE-Pakets problemlos vom Angreifer manipulieren. Das IED, das die GOOSE empfängt, hat keine andere Wahl, als auf die erste empfangene GOOSE mit der korrekten MAC-Quelladresse und der korrekten Status-/Sequenznummer zu reagieren. Dasselbe gilt natürlich auch für den Zähler des Abtastwerts in den Sampled Values. Die einzig wirksame Maßnahme, solchen Einspeiseangriffen zu begegnen, besteht darin, die Authentizität und Integrität der Nachricht durch Authentifizierungscodes am Ende der GOOSE-Nachricht gemäß IEC 62351-6 sicherzustellen. Mit dieser Maßnahme wird das sendende IED eindeutig identifiziert. Eine Manipulation des Inhalts der GOOSE-Nachricht ist somit unmöglich. Dafür ist es übrigens nicht erforderlich, die Nachricht zu verschlüsseln. Für die Bereitstellung und Wartung dieser Authentifizierungsschlüssel je IED wird allerdings eine Infrastruktur für die Verwaltung der Schlüssel innerhalb der Anlage benötigt. Aus diesem Grund finden diese GOOSE-Sicherheitsmechanismen bisher noch keine breite Anwendung, ihre Einführung ist jedoch nur eine Frage der Zeit. Gleiches gilt für MMS und die rollenbasierte Zugriffskontrolle.

Verschlüsselung

Die Verschlüsselung wurde hier nicht explizit erwähnt, obwohl sie oft als Patentlösung in der IT-Sicherheit gilt. Die Norm IEC 62351 regelt auch die Verschlüsselung für GOOSE und MMS. In der Anlagenumgebung gibt es jedoch nur wenige Anwendungen, bei denen die Vertraulichkeit von Nachrichten eine wichtige Rolle spielt. Wenn Nachrichten nicht manipuliert werden können (Integrität) und der Absender verifiziert werden kann (Authentifizierung) – was durch die Verwendung von

Authentifizierung in GOOSE und MMS erfüllt wird – muss die Nachricht auch nicht noch zusätzlich verschlüsselt werden. Ein Beispiel, bei dem eine Verschlüsselung notwendig sein könnte, ist die Übertragung von routbaren GOOSE (R-GOOSE) über einen unverschlüsselten Kommunikationsweg. Die Verschlüsselung führt nur zu einer zusätzlichen CPU-Last auf den IEDs, erhöht die Übertragungszeit der GOOSE und erschwert Prüfszenarien, ohne in den meisten Fällen zusätzliche Sicherheit zur bereits vorhandenen Authentifizierung zu bieten. Eine Verschlüsselung erschwert auch eine spätere Analyse des aufgezeichneten Datenverkehrs und behindert Überwachungsansätze wie die nachfolgend beschriebenen.

Defense in Depth

Die meisten bis heute gebauten IEC-61850-Anlagen haben IEC 62351 noch nicht implementiert. Selbst in Anlagen, in denen GOOSE und MMS mit Authentifizierungscodes verwendet werden, können infizierte Geräte im Netzwerk weiterhin andere Geräte infizieren oder die Verfügbarkeit durch eine Störung des Kommunikationssystems beeinträchtigen. Daher empfehlen die meisten Sicherheits-Frameworks die Verwendung eines „Intrusion Detection Systems“ (IDS) – einem Einbruchserkennungssystem, ein bekannter Begriff in der klassischen IT – um Bedrohungen und bösartige Aktivitäten im Netzwerk zu erkennen. Diese IDS werden heute immer häufiger im Bereich der Stromversorgung eingesetzt.

4 Anforderungen an ein IDS für digitale Schaltanlagen

In einer IEC-61850-Anlage würde ein IDS wie in Abbildung 2 gezeigt angeschlossen. Mirror Ports an allen relevanten Switches leiten eine Kopie des gesamten Netzwerkverkehrs an das IDS weiter. Das IDS überprüft den gesamten über diese Switches übertragenen Netzwerkverkehr. Für eine Analyse des wichtigsten Datenverkehrs zwischen dem Gateway und den IEDs sollte das IDS mindestens mit dem Switch neben dem Gateway und allen anderen kritischen Eintrittspunkten im Netzwerk verbunden werden. Die Switches auf Feldebene müssen in der Regel nicht geschützt werden, da von dort typischerweise nur Multicast-Verkehr (GOOSE, Sampled Values) kommt. Um sicherzustellen, dass auch der gesamte Unicast-Verkehr in allen Netzwerkzweigen analysiert wird, müssten auch die Switches auf der Feldebene über Mirror Ports zum IDS gespiegelt werden.

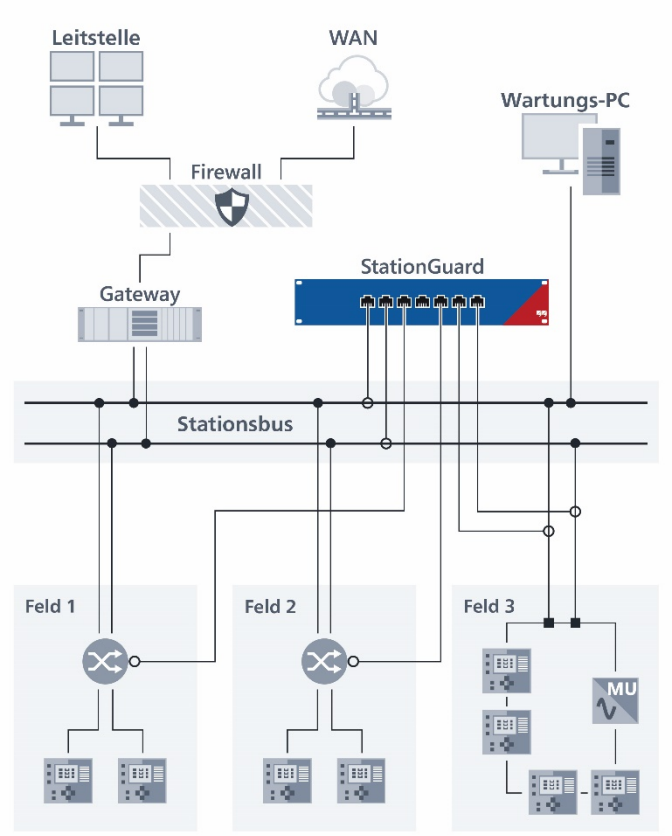

Abbildung 2 Möglichkeiten für den Anschluss des IDS an das Anlagennetzwerk

IDS aus der klassischen IT sind für den Einsatz in einer Anlagenumgebung nicht geeignet. Während sich die klassische IT-Sicherheit mit Hochleistungsservern und deren unzähligen simultanen Verbindungen beschäftigt, befasst sich die IT-Sicherheit in Schaltanlagen mit Geräten, die begrenzte Ressourcen aufweisen, proprietären Betriebssystemen, Echtzeit-Anforderungen und speziellen Redundanzprotokollen. So müssen beispielsweise für einen „Denial-of-Service“-Angriff auf den Kommunikationsdienst eines IEDs oft nur zehn Verbindungen, das heißt zehn Ethernet-Pakete, verwendet werden, um erfolgreich zu sein. Der Grund ist einfach: „Denial-of-Service“-Szenarien wurden zu den Zeiten, als diese Geräte und Protokolle entwickelt wurden, nicht berücksichtigt. Weiterhin gibt es nur eine kleine Anzahl bekannter Cyberangriffe auf Anlagen, aber bereits das erste Auftreten eines neuen Angriffs könnte schwerwiegende Folgen haben. Deshalb muss das IDS einer Anlage Angriffe ohne Vorkenntnisse darüber, wie der Angriff aussehen könnte, erkennen können und das ist genau was der StationGuard von OMICRON tut. Es handelt sich also um einen ganz anderen Ansatz als bei einem Virenscanner, der seine Suche anhand einer Liste von Virensignaturen durchführt.

5 Lernbasierte Systeme

Um ihre Systeme in die Lage zu versetzen, unbekannte Angriffe zu erkennen, verwenden viele Anbieter eine „Lernphase“ bei ihren Lösungen. Diese Systeme beobachten die Häufigkeit und den Zeitpunkt bestimmter Protokollmarker. Damit soll das übliche Verhalten des Systems erlernt werden. Nach der Lernphase wird immer dann ein Alarm ausgelöst, wenn einer der Marker deutlich außerhalb des erwarteten Bereichs liegt. Dies hat zur Folge, dass Fehlalarme für alle Ereignisse ausgelöst werden, die während der Lernzeit nicht aufgetreten sind. Dabei handelt es sich beispielsweise um Schutzereignisse, Schalt- oder Automatisierungsaktionen, oder die routinemäßige Instandhaltung und Prüfung.
Ein weiteres Problem ist, dass die Alarmmeldungen in Form von technischen Protokolldetails ausgedrückt werden, weil diese IDS die Vorgänge in der Anlage nicht kennen. Somit können Alarme nur von einem Ingenieur geprüft werden, der mit den Einzelheiten des IEC-61850-Protokolls und mit der IT-Netzwerksicherheit vertraut ist. Dieser Ingenieur muss darüber hinaus die Betriebssituation kennen, um beurteilen zu können, ob bestimmte Ereignisse des IEC-61850-Protokolls dem gültigen Verhalten entsprechen. Deshalb tritt bei jeder Anlage eine Vielzahl von Fehlalarmen auf, die eine Überprüfung durch hochqualifiziertes Personal erfordern. Dies führt nicht selten dazu, dass Alarme ignoriert oder verworfen werden, ohne dass die notwendige Prüfung erfolgt, und das IDS schließlich abgeschaltet wird.

6 Der StationGuard-Ansatz

Für IEC-61850-Anlagen wird das gesamte Stationsautomatisierungssystem mit allen Geräten, den Datenmodellen und den Kommunikationsmustern in einem standardisierten Format, der SCL (Substation Configuration Language), beschrieben. SCD-Dateien (System Configuration Description) enthalten in der Regel auch Informationen über primäre Betriebsmittel. Für eine stetig wachsende Anzahl von Anlagen ist sogar schon das Prinzipschaltbild in der SCD enthalten.

Mit diesen Informationen lässt sich ein anderer Ansatz für die Erkennung von Angriffen verwenden: Das Monitoring-System kann ein vollständiges Systemmodell des Stationsautomatisierungssystems sowie der Schaltanlage erstellen und jedes einzelne Paket im Netzwerk mit dem Live-Systemmodell vergleichen. Auch die in den kommunizierten Nachrichten (GOOSE, MMS, SV) enthaltenen Variablen lassen sich anhand der aus dem Systemmodell abgeleiteten Erwartungen bewerten. Dieser Prozess ist ohne Lernphase und allein durch die Konfiguration des IDS mit der SCL möglich. Im neuen funktionalen Sicherheitsüberwachungssystem StationGuard wird genau dieser Ansatz umgesetzt.

Funktionale Sicherheitsüberwachung

Im Wesentlichen wird eine sehr detaillierte Funktionsüberwachung erstellt, um Cyber-Bedrohungen im Netzwerk zu erkennen. Aufgrund der detaillierten Überprüfung werden nicht nur Bedrohungen für die Cybersicherheit, wie manipulierte Pakete oder unzulässige Steuervorgänge, erkannt, sondern auch Kommunikationsfehler, Probleme mit der Zeitsynchronisation und damit auch möglicherweise bevorstehende Geräteausfälle. Kennt das System das Prinzipschaltbild und können die Messwerte über die MMS-Kommunikation (oder auch mit den Sampled Values) beobachtet werden, sind der Überprüfung keine Grenzen gesetzt.
Beispiel: Allein für GOOSE gibt es 35 mögliche Alarmcodes. Sie reichen von einfachen stNum-/sqNum-Störungen (wie oben erläutert) bis hin zu komplexeren Problemen, wie beispielsweise zu langen Übertragungszeiten. Letzteres wird durch das genaue Messen der Differenz zwischen dem EntryTime-

Zeitstempel in der Nachricht und der Ankunftszeit bei StationGuard erkannt. Ist die Übertragungszeit des Netzwerks für eine „Schutz“-GOOSE (gemäß IEC 61850-5) deutlich länger als 3 ms, dann deutet dies auf ein Problem im Netzwerk oder bei der Zeitsynchronisation hin.

Was wird bei der MMS-Kommunikation getan? Aus dem Systemmodell (in der SCL) ist bekannt, welche logischen Knoten welche primären Betriebsmittel steuern. Somit kann zwischen korrekten/nicht korrekten beziehungsweise kritischen/nicht kritischen Aktionen unterschieden werden. Das Schalten eines Leistungsschalters und das Schalten des Prüfmodus gemäß IEC 61850 nutzen dieselbe Reihenfolge im MMS-Protokoll (Select-before-Operate), doch die Auswirkung in der Anlage ist jeweils eine ganz andere. Wenn also der Prüfcomputer aus Abbildung 1 den Prüfmodus auf einem Relais umschaltet, kann dies eine legitime Aktion während der Instandhaltung sein, sehr wahrscheinlich ist es aber nicht legitim, wenn dieser Prüfcomputer einen Leistungsschalter betätigt. In den folgenden Abschnitten wird auf dieses Beispiel näher eingegangen.

Mit Schutz- und Leittechnikern entwickelt

Die Forschung zu diesem Ansatz begann 2011. Spin-offs dieses Konzepts – die 24/7-Funktionsüberwachung von SV, GOOSE und die PTP-Uhrzeitsynchronisation – sind seit 2015 in einem dezentralen und hybriden Analysegerät (DANEO 400 von OMICRON) verfügbar. Aufgrund dieser Tatsache wurden wir vom Schweizer Energiedienstleister CKW (Centralschweizer Kraftwerke AG) angesprochen. Ihnen waren die Nachteile kommerziell verfügbarer IDS-Systeme bekannt, weshalb sie nach einer passenderen Lösung für Anlagen suchten, die für Schutz-, Automatisierungs- und Steuerungstechniker einfacher zu bedienen war. Dies führte zu einer Zusammenarbeit zwischen den Leittechnikern der CKW und dem Entwicklungsteam von StationGuard. Es war beeindruckend zu hören, wie die CKW die Einbruchserkennung bereits als Teil der Cybersicherheit ihrer zukünftigen Anlage planten. In dieser Phase erhielten wir zudem Rückmeldungen von vielen anderen Energieversorgern weltweit, welche gemeinsam mit den Erkenntnissen aus einigen Proof-of-Concept-Installationen in unsere Entwicklung einflossen.
2018 wurde eine der ersten Proof-of-Concept-Installationen in einem 110-kV-Umspannwerk der CKW installiert und in Betrieb genommen. Abbildung 3 zeigt unten die Installation mit der mobilen Plattform MBX1. In dieser Konfiguration wurde der gesamte Datenverkehr des „Core“-Switches auf StationGuard gespiegelt. Dadurch wird sichergestellt, dass die gesamte Kommunikation vom Gateway zu und von allen IEDs sichtbar ist. Da über diesen Switch auch Verbindungen für die ferngesteuerte Instandhaltung laufen, kann der gesamte Verkehr von StationGuard eingesehen werden. Da es sich bei GOOSE-Kommunikation um Multicast handelt und die Netzwerkkonfiguration es zulässt, sind für StationGuard alle GOOSE sichtbar, die die IEDs in den jeweiligen Anlagenfeldern senden.

Abbildung 3 Installation mit der mobilen Plattform MBX1 von StationGuard in der 110-kV-Anlage der CKW

Alarmanzeige

Für die Ingenieure, die für den Betrieb der Schaltanlage mit deren Schutz-, Automatisierungs- und Netzwerksystemen verantwortlich sind, ist es nicht nur von entscheidender Bedeutung, dass Fehlalarme vermieden werden, sondern auch, dass die Alarmmeldungen allgemein verständlich sind. Das ermöglicht schnellere Reaktionszeiten, da die Alarme oft von Prüfern ausgelöst werden, die gerade in der Anlage (oder per Fernzugriff) arbeiten. Eine leichte Verständlichkeit erlaubt zudem die Zusammenarbeit der Sicherheits- und PAC-Ingenieure bei der Analyse von Ereignissen in der Anlage.
Abbildung 4 zeigt einen Screenshot der grafischen Alarmanzeige: Der Alarm wird als Pfeil vom aktiven Teilnehmer (Prüfcomputer), der die verbotene Aktion durchführt, und vom „Opfer“ der Aktion, einem Feldleitgerät im Feld Q01, dargestellt. Abbildung 5 zeigt die Details dieses Alarms: Es wurde ein Leistungsschalter betätigt (mit einer MMS-Steuersequenz), was für einen Prüfcomputer nicht erlaubt ist.

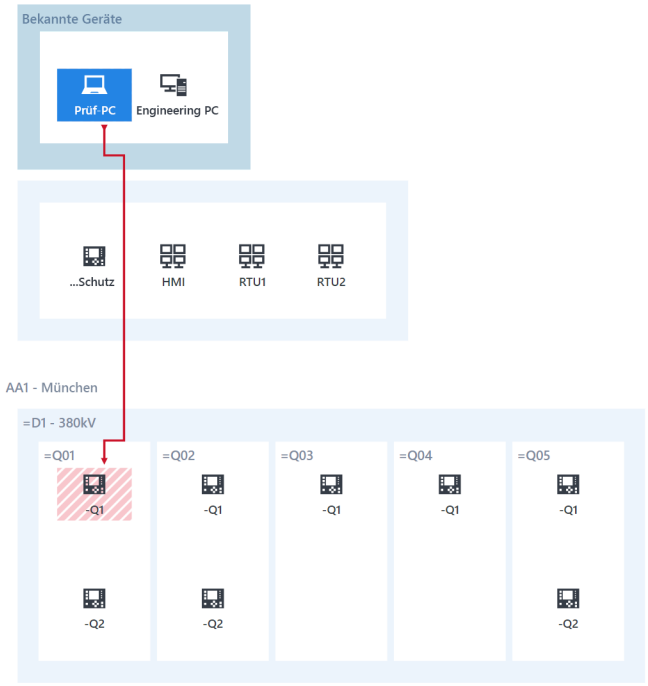

Abbildung 4 Grafische Alarmdarstellung anstelle einer Ereignisliste

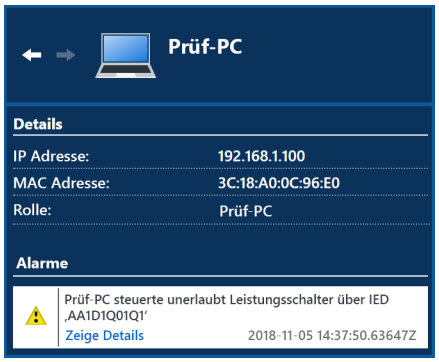

Abbildung 5 (Details für Abb. 4) Der Prüfcomputer versucht, den Leistungsschalter unbefugt zu steuern

Instandhaltungsmodus

Um Fehlalarme zu vermeiden, müssen routinemäßige Prüf- und Instandhaltungsbedingungen in das Systemmodell der Anlage aufgenommen werden. StationGuard ermöglicht es deshalb, dass die Prüf- und Wartungsausrüstung, einschließlich der Schutzprüfgeräte, in das System einbezogen werden. In Abbildung 6 sehen wir, dass die Instandhaltung für Feld Q01 aktiviert wurde. In diesem Modus sind dem Prüfcomputer aus dem obigen Beispiel mehr Aktionen erlaubt als zuvor. Es wird kein Alarm ausgegeben, wenn der Prüfcomputer den Prüf- oder Simulationsmodus des IED-Q1 in diesem Feld gemäß IEC 61850 steuert. Ein Alarm wird allerdings dann ausgelöst, wenn der Prüfcomputer einen Leistungsschalter in diesem Feld betätigt. Dies wäre eine kritische Aktionen, die für einen Prüfcomputer unzulässig ist. Natürlich können diese Regeln von den Verantwortlichen geändert werden, wenn die Richtlinien des Unternehmens solche Aktionen erlauben.

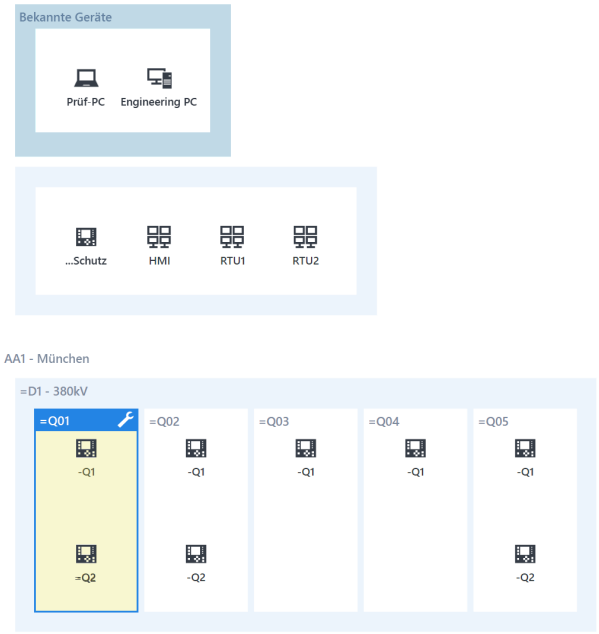

Abbildung 6 Feld Q01 mit aktiviertem Instandhaltungsmodus

Konfiguration

Wie bereits erwähnt, erfordert StationGuard keine Lernphase. Das Erkennen des Systems beginnt sofort mit dem Einschalten des Geräts und kann aus Sicherheitsgründen auch nicht beendet werden. Bis die SCD-Datei der Anlage geladen ist, werden alle erkannten IEDs als unbekannte Geräte dargestellt. Nach dem Laden der SCD-Datei zeigt StationGuard die IEDs als bekannte Geräte an und die Anlagenstruktur wird in einer sogenannten „ZeroLine“ zusammengefasst, so wie es mit StationScout eingeführt wurde. Die Konfiguration kann auch zunächst im Büro vorbereitet und anschließend in jeder einzelnen Anlage per Schnellinbetriebnahme installiert werden. Wurden nicht alle IEDs in einer Datei zusammengefasst , lassen sich zusätzliche IEDs auch einzeln importieren. Nach dem Importieren kann der Techniker den noch verbleibenden unbekannten Geräten Rollen wie „Prüfcomputer“, „Engineering-PC“ usw. zuordnen.

Was passiert bei einem Alarm?

StationGuard agiert rein passiv: Ist eine Aktion „nicht erlaubt“, wird ein Alarm ausgelöst. Dieser Alarm kann an das Gateway/die RTU und die Leitstelle oder an ein separates Security Incident Event Management System (SIEM) übermittelt werden, das die Sicherheitswarnungen sammelt. StationGuard reagiert nicht aktiv auf einen Angriff, in dem Sinne, dass es ihn stört oder unterbindet. Er ermöglicht aber eine schnelle Reaktion, beispielsweise die Isolierung des betroffenen Geräts vom Netzwerk, bevor ein Schaden entstehen kann. Je nach gewählter Hardwarevariante stehen auch Binärausgänge zur Verfügung, die direkt an die RTU angeschlossen werden können. In diesem Fall erfolgt die Alarmmeldung ohne Netzwerkkommunikation und die Alarme können wie jedes andere fest verdrahtete Signal der Anlage in die normale SCADA-Signalliste integriert werden.

7 Cybersicherheit von StationGuard

Wie wir es aus Hollywood-Filmen kennen, greifen Einbrecher immer zuerst die Alarmanlage an. Wie steht es also um die Sicherheit von StationGuard? Um diese Sicherheit zu gewährleisten, verwendet StationGuard eine eigenständige und sichere Hardware, nicht eine virtuelle Maschine. Beide Hardwarevarianten von StationGuard, sowohl die mobile (MBX1) wie auch die 19-Zoll-Variante für die Installation in Schaltanlagen (RBX1), verwenden dieselbe Plattformhärtung. Beide verfügen über einen sicheren Kryptoprozessorchip nach ISO/IEC 11889. Dadurch wird sichergestellt, dass kryptografische Schlüssel nicht auf dem Flash-Speicher, sondern auf einem separaten Chip gespeichert werden, der vor Manipulationen geschützt ist. Durch die Installation der Zertifikate von OMICRON auf diesem Chip, die bereits während der Produktion erfolgt, entsteht eine sichere, kontrollierte Bootkette. Das bedeutet, dass jeder Schritt im Boot-up-Prozess der Firmware die Signaturen des nächsten zu ladenden Moduls oder Treibers überprüft. So wird sichergestellt, dass nur Software mit einer Signatur von OMICRON ausgeführt

werden kann. Der Speicher der Geräte wird mit einem für diese Hardware eindeutigen Schlüssel verschlüsselt, welcher wiederum im Kryptochip geschützt ist. Da niemand, auch nicht OMICRON, diesen Schlüssel kennt, gehen beim Austausch der Hardware im Rahmen einer Reparatur alle Daten auf dem Gerät verloren. Viele weitere Mechanismen sorgen dafür, dass die Prozesse auf dem Gerät nicht angegriffen oder missbraucht werden können. Deshalb wirkt der „Defense-in-Depth“-Ansatz auch tief in die auf dem Gerät laufende Software. Die Erläuterung all dieser Mechanismen würde allerdings den Rahmen dieses Artikels sprengen.

8 Fazit

Jede Anlage bietet potenzielle Vektoren für Cyberangriffe. Sobald es für einen Angreifer möglich wird, eine oder mehrere Anlagen zu beeinflussen, kann dies unter Umständen schwerwiegende Folgen für das gesamte Energienetz haben. Deshalb müssen effektive Maßnahmen zur Abwehr von Cyberangriffen nicht nur in den Leitstellen umgesetzt werden, sondern auch in den Schaltanlagen selbst. Für IEC-61850-Anlagen existiert ein Ansatz zur Einbruchserkennung, der wenige Fehlalarme und einen, aufgrund der Nutzung der SCL, sehr geringen Konfigurationsaufwand bietet. Dieses System erkennt neben Sicherheitsbedrohungen auch funktionale Probleme der IEC-61850-Kommunikation sowie der IEDs, was auch in der FAT (Factory Acceptance Test)- und SAT (Site Acceptance Test)-Phase hilfreich ist. Durch die Darstellung der erkannten Ereignisse in der Sprache der Schutz- und Leittechniker bieten diese Einbruchserkennungssyteme den Vorteil, dass Schutz- und Leittechniker, sowie IT-Security-Verantwortliche bei der Suche nach der Alarmursache und deren Behebung zusammenarbeiten können.

OMICRON ist ein weltweit tätiges Unternehmen, das innovative Prüf- und Diagnoselösungen für die elektrische Energieversorgung entwickelt und vertreibt. Der Einsatz von OMICRON-Produkten bietet höchste Zuverlässigkeit bei der Zustandsbeurteilung von primär- und sekundärtechnischen Betriebsmitteln. Umfassende Dienstleistungen in den Bereichen Beratung, Inbetriebnahme, Prüfung, Diagnose und Schulung runden das Leistungsangebot ab.

Kunden in mehr als 160 Ländern profitieren von der Fähigkeit des Unternehmens, neueste Technologien in Produkte mit überragender Qualität umzusetzen. Servicezentren auf allen Kontinenten bieten zudem ein breites Anwendungswissen und erstklassigen Kundensupport. All dies, zusammen mit einem starken Netz von Vertriebspartnern, ließ OMICRON zu einem Marktführer der elektrischen Energiewirtschaft werden.

Mehr Informationen, eine Übersicht der verfügbaren Literatur und detaillierte Kontaktinformationen unserer weltweiten Niederlassungen finden Sie auf unserer Website.

www.omicronenergy.com