Bild: TheDigitalArtist/pixabay

Smart Grid? Aber sicher!

IEC-61850-Standard | Beschränkte sich der Einsatz des Kommunikationsprotokolls IEC 61850 bislang vor allem auf den Umspannbereich, gehen aktuelle Versionen weit darüber hinaus und umfassen grundsätzlich sämtliche Netzkomponenten. Aus Sicht der IT-Security gibt es aber einiges zu beachten.

UDO SCHNEIDER

Beim Thema «smarte» Stromversorgung denken viele vermutlich an Themen wie Smart Metering sowie die lokale Steuerung und Einspeisung von Photovoltaik- oder Windkraftanlagen. Von vielen unbeachtet werden aber auch die Kernnetze beziehungsweise deren Komponenten immer «smarter». Sehr deutlich lässt sich dies zum Beispiel in Umspannwerken sehen: Dort sind Lösungen auf Basis von IEC 61850 immer mehr auf dem Vormarsch und lösen damit immer häufiger elektromechanische «festverdrahtete» Implementierungen ab.

Während der ursprüngliche Einsatzbereich von IEC 61580 ausschliesslich die Kommunikation im Umspannwerk umfasste, gehen aktuelle Versionen deutlich darüber hinaus und umfassen grundsätzlich alle Netzkomponenten inklusive verschiedenster lokaler Anlagen wie Wasser- und Windenergieanlagen bis hin zu intelligenten Ladestationen für Autos. Diese Breite an Einsatzmöglichkeiten ist nicht zuletzt auch dem Austausch von festverdrahteter Kommunikation durch flexible, netzwerkbasierte Kommunikation zu verdanken. Aus (IT-)Security-Sicht ergeben sich aber genau hier auch potenzielle Gefahren, die es zu betrachten gilt:

Leitwarte

Die Zeiten, in denen Umspannwerke über serielle Leitungen mit der Leitwarte verbunden waren, waren auch schon vor IEC 61580 lange vorbei. Die heute vorherrschende Anbindung an Umspannwerke und auch die Verbindung der Systeme untereinander erfolgt inzwischen fast ausschliesslich über normale Netzwerktechnik aus der «Office-IT», inklusive der Nutzung von TCP/IP und darauf aufbauenden Diensten. Damit einher geht auch die Nutzung von normaler Office-IT-Hard- und Software.

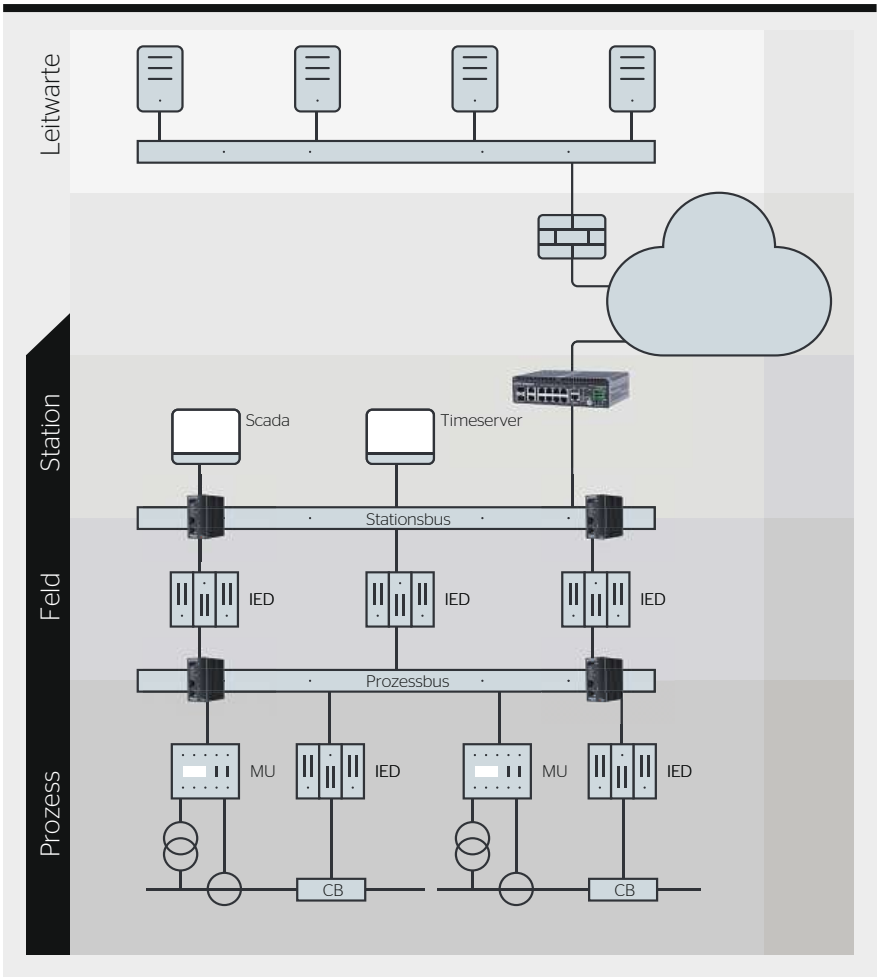
Das hat Folgen für die IT-Sicherheit: Das Risiko unterscheidet sich kaum noch von normalen Office-IT-Szenarien. Positiv ist manchmal anzumerken, dass einige Leitwarten keinen direkten Internetzugang besitzen, wobei diese Trennung in der Praxis leider immer weniger eingehalten wird. Wie andere industrielle Umgebungen, leidet jedoch auch die Leitwarten-IT unter dem Konzept des «never touch a running system». Das bedeutet, einmal eingesetzte Systeme (Hard- und Software) werden über lange Zeiträume ohne Updates betrieben. Kombiniert mit der immer grösseren Anzahl von Sicherheitslücken ist es für einen potenziellen Angreifer, der es in das Leitwarten-Netz geschafft hat, in der Regel sehr einfach, dort erheblichen Schaden anzurichten. Bilder von Leitwarten, bei denen die Ransomware-Meldungen dem Betrachter auf riesigen Displays entgegenspringen, sind leider keine Seltenheit.

Sicherheit bedeutet deshalb nicht nur Unfallvermeidung (Safety), sondern vielmehr auch die Abwehr von Cyber-Gefahren (Security). Dementsprechend sollte auch das Risiko von Cyber-Angriffen mit in die Risikobetrachtung einbezogen werden – nicht nur initial beim Aufbau der Leitwarte, sondern kontinuierlich. Hier empfiehlt sich insbesondere der Einsatz eines ISMS (Information Security Management System), um das Risiko besser einschätzen zu können. Erst dann lohnt es sich, in technische Netzwerksicherheits-Massnahmen wie Firewalls, IDS-/IPS-Systeme, (virtuelles) Patch-Management und ähnliche Lösungen zu investieren. Aber auch der Einsatz von Application-Safelisting- beziehungsweise Lockdown-Systemen oder installationslosen Antiviruslösungen ist sinnvoll.

Stationsebene/Stationsbus

Die Stationsebene unterscheidet sich, bis auf die für IEC 61580 überlebenswichtige Zeitsynchronisation, kaum von den Steuerebenen in anderen Branchen. Auch hier ist der Einsatz von ICS-/Scada-Lösungen auf Standard-Hard- und -Software an der Tagesordnung. Interessant ist aber ein Blick auf den Stationsbus zur Feldebene (Bay-Level), insbesondere im Hinblick auf Netzwerktopologie und Protokolle. In anderen Branchen übliche Feldnetzprotokolle wie Modbus, S7Comm oder OPC(-UA) über UDP oder TCP sucht man in IEC-61580-Umgebungen vergebens. Vielmehr ist hier MMS (Manufacturing Message Specification) in Kombination mit redundanten Netztopologien, zum Beispiel HSR (High-availability Seamless Redundancy) und RSTP (Rapid Spanning Tree Protocol), zur Kommunikation mit IEDs (Intelligent Electronic Device) an der Tagesordnung. Auch werden verschiedene Protokolle über die jeweiligen Switche in separaten VLANs mit entsprechenden QoS-Parametern (Quality of Service) transportiert.

Aus Sicht der IT-Security ergibt sich auf der Stationsebene ein zweischneidiges Schwert: Auf der einen Seite finden sich die normalen ICS-/Scada-Komponenten. Diese machen es einem Angreifer oft leicht, da er sich auf gewohntem Terrain bewegt. Werden diese aus Verfügbarkeitsgründen («never touch a running system», siehe oben) nicht mit aktuellen Patches versorgt, macht es das dem Angreifer sogar noch einfacher.



Schematische Netzstruktur nach IEC 61580.

Auf der anderen Seite kommt mit MMS und der ungewohnten Netztopologie aber Neuland auf viele Angreifer zu. Doch auch hier ist deswegen nicht alles automatisch sicher. MMS als Protokoll setzt auf TCP/IP auf und ist daher für Angreifer gut zu untersuchen. Die Tatsache, dass MMS-Payloads standardmässig weder verschlüsselt noch signiert sind, macht es einem Angreifer auch sehr leicht, diese zu fälschen und damit falsche Anzeigen zu provozieren. Und auch die «seltsame» Netztopologie erlaubt trotzdem oft via TCP/IP einen Durchgriff über den Stationsbus auf IEDs.

Hier gilt es also (zusätzlich zu den oben aufgeführten Schutzmassnahmen für Standard-Hard- und -Software) besondere Vorsicht in Bezug auf unbekannte Geräte und anomale Netzwerkkommunikation walten zu lassen. Die Kommunikation bedarf deshalb einer kontinuierlichen Überwachung im Hinblick auf Endpunkte und Kommunikationsinhalte. Diese darf jedoch auf keinen Fall die Funktionalität und Verfügbarkeit kompromittieren. Der Einsatz von Office-IT-Komponenten wie Firewalls oder IDS/IPS-Systemen ist aufgrund der fehlenden Kompatibilität mit Netzwerktopologien und Protokollen wie MMS jedoch wenig sinnvoll. Hier sind spezielle Lösungen gefragt, die mit den jeweiligen Anforderungen der Umgebung auch vertraut sind.

Feldebene/Prozessbus

Auf Höhe der Feldebene beziehungsweise auf dem Prozessbus verlässt man endgültig die vertraute Office-IT-Umgebung. Die auf dieser Ebene ansässigen IEDs kommunizieren zum Beispiel via Goose und SMV mit nachgelagerten Leistungsschaltern (Circuit Breaker, CB) oder Strom- beziehungsweise Spannungswandlern (Current Transformer, CT respektive Voltage Transformer, VT). Auch hier ist die eingesetzte Netzwerktopologie mit PRP (Parallel Redundancy Protocol) weitab vom bekannten Terrain.

Bild: Trend Micro

Leider ist aber auch hier nicht alles Gold, was glänzt. Goose und SMV setzen zwar nicht auf TCP/IP auf, sondern werden als eigener Ethernet-Typ direkt versendet, sind aber leider wie MMS auch weder verschlüsselt noch signiert. Im Gegensatz zu MMS sind Angriffe zudem direkt sicherheitsrelevant, sei es, da falsche Sensorwerte von Prozesskomponenten gemeldet werden (SMV) oder – noch schlimmer – Kommandos und Alarmierungen verändert und unterdrückt werden können (Goose).

Aus Sicht der IT-Security ist auf Feldebene einiges einfacher und anderes deutlich schwieriger: Die Aufgabe einfacher macht die Tatsache, dass auf Feldebene keine Office-IT-Komponenten zum Einsatz kommen. Das bedeutet, es sind «nur» noch Angriffe auf IEDs zu erkennen und abzuwehren. Auf der anderen Seite ist die Absicherung der Netztopologie und der genutzten Protokolle sogar noch herausfordernder als bei MMS. Zusätzlich zum Wissen über die Protokollinhalte gibt es hier harte Vorgaben bei Verarbeitungszeiten. Bei einer Gesamtlatenz von <4 ms (zum Beispiel für Leistungsschalter) muss eine eventuelle Sicherheitslösung entsprechend kleine Durchlaufzeiten garantieren.

Ein möglicher Ansatz ist das passive Betreiben von Sicherheitskomponenten. Anstatt diese aktiv in die Kommunikation einzusetzen, werden diese an den Switches passiv angeschlossen und hören nur mit. Dies hat zwar den Nachteil, dass Angriffe nicht direkt unterbunden werden können, bietet jedoch den unschätzbaren Vorteil, dass diese nicht in sicherheitsrelevante Kommunikation eingebunden sind.

Arbeitsgruppen diskutieren Sicherheitsaspekte

Die «schöne neue Welt» der IEC 61580 hat viele Vorteile. Abgesehen von der deutlich einfacheren Verkabelung auf Prozess-, Feld- und Stationsebene erlaubt die Einführung einer einheitlichen Netzwerk- und Kommunikationsinfrastruktur die einfache Ausbreitung in viele Bereiche. Gleichzeitig stellt aber genau diese einheitliche Infrastruktur auch eine potenzielle Gefahr dar. Hacker, die sich bisher in normalen Office-IT-Umgebungen ausgetobt haben, finden unter Umständen ein neues Spielfeld, auf dem sie mit ihnen bekannten Werkzeugen und Erfahrungen für Schaden sorgen können. Dabei geht die Gefahr nicht nur von politisch motivierten Angreifern aus – selbst das völlig branchenunspezifische und rein finanziell motivierte Einbringen von Verschlüsselungstrojanern («Ransomware») kann den Betrieb nachhaltig stören.

Die gute Nachricht ist aber, dass Betreiber zur Sicherung eben jener Office-IT-Komponenten auch durchaus auf entsprechende Sicherheitslösungen «von der Stange» zurückgreifen können. Je näher man der Feld- oder Prozessebene kommt, desto stärker unterscheidet sich die Umgebung von der Office-IT und umso spezialisierter müssen auch die Sicherheitslösungen werden. Auf reine «Sicherheit durch Unwissen» können sich Betreiber jedenfalls nicht verlassen, da es doch noch immer gewisse Gemeinsamkeiten gibt. Völlig ausser Frage steht aber, dass die Netzwerktopologie und Protokolle bei IEC 61580 einen gewichtigen Sicherheitsaspekt darstellen. Das Wissen um diese ist für Betreiber dementsprechend essenziell.

Letztendlich ist man aber auch hier nicht allein. Die fehlende Sicherheit, beispielsweise von Protokollen wie MMS, Goose und SMV, wird in Arbeitsgruppen diskutiert und im Rahmen von Standards wie IEC 62351 auch spezifiziert (IEC 62351-4 für MNS, IEC 62351-6 für MNS und Goose). Die IEC 61580 wird also erhalten bleiben – dafür bietet sie einfach zu viele Vorteile. Eine wichtige Aufgabe ist deshalb, diese sicher betreibbar zu machen. Mit Best Practices aus der Office-IT (wo möglich), spezialisierten Lösungen für die Feld- und Prozessebene und Ergebnissen aus sicherheitsrelevanten Standards wie IEC 62351 ist man damit auf einem guten Weg.

Autor
Udo Schneider ist IoT Security Evangelist bei Trend Micro.
→ Trend Micro Deutschland GmbH, D-85748 Garching bei München.
→ udo_schneider@trendmicro.com

RÉSUMÉ

Smart Grid ? La sécurité sinon rien !

Standard CEI 61850

Si, jusqu'à présent, l'utilisation de la norme de communication CEI 61850 se limitait surtout au domaine de la transformation, les versions actuelles vont bien au-delà et comprennent l'ensemble des composantes de réseau. Du point de vue de la sécurité informatique, il faut néanmoins tenir compte d'un certain nombre de choses.

Dans le monde nouveau de la norme CEI 61580, on trouve de nombreux avantages. Hormis le câblage fortement simplifié au niveau du processus, du terrain et de la station, l'introduction d'une infrastructure homogène de réseau et de communication permet de l'étendre simplement à de nombreux domaines. Parallèlement, c'est précisément cette infrastructure homogène qui représente un risque potentiel. Les hackers, qui se défoulaient jusqu'à maintenant dans les environnements d'informatique de bureau « normaux », pourraient trouver un nouveau terrain de jeu où utiliser les outils et expériences dont ils disposent pour engendrer des dommages. Le danger ne vient pas uniquement d'agresseurs aux motivations politiques : même l'implantation de rançongiciels (ou « ransomwares »), sans aucune spécificité de branche et motivée uniquement par l'appât du gain, peut perturber durablement l'exploitation.

Toutefois, il y a une bonne nouvelle : pour assurer la sécurité de ces composantes d'informatique de bureau, les exploitants peuvent tout à fait recourir à des solutions « prêtes à l'emploi ». Plus on s'approche du niveau du terrain ou du processus, plus l'environnement se distingue de l'informatique de bureau et plus les solutions pour la sécurité doivent être spécialisées. En tout cas, les exploitants ne peuvent pas se fier à une simple « sécurité basée sur l'ignorance », puisqu'il existe toujours certains points communs. Néanmoins, il n'y a absolument aucun doute sur le fait que la topologie du réseau et les protocoles selon le standard CEI 61580 représentent un aspect sécuritaire important. Pour les exploitants, il est donc essentiel de les connaître. MR