Operational Technology = Technologie opérationnelle

Autor(en): **Mattmann, Stefan / Gosteli, Yann / Niffeler, Remo**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **112 (2021)**

Heft 7-8

PDF erstellt am: **30.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-977585

dossier.

Operational Technology

Wie sich die OT entwickelt | Im Zeitalter der Digitalisierung ist die IT für die administrativen Belange eines EVU unabdingbar. Aber auch in der OT wird zunehmend auf Computer und IT-basierte Systeme gesetzt.

Technologie opérationnelle

Évolution de l'OT | À l'ère de la numérisation, l'IT est indispensable pour répondre aux besoins administratifs d'une EAE. Mais dans l'OT aussi, l'utilisation d'ordinateurs et de systèmes basés sur l'IT prend de plus en plus d'ampleur.

Standort Rathausen
Die CKW-Netzleitstelle befindet sich auf einer Insel an der Reuss beim Kraftwerk Rathausen.

Site de Rathausen
Le centre de contrôle du réseau de CKW est situé sur une île sur la Reuss, près de la centrale de Rathausen.

STEFAN MATTMANN, YANN GOSTELI, REMO NIFFELER

Der Begriff Operational Technology, OT, war bisher im breiten Sprachgebrauch kaum bekannt, obwohl OT-Technologien schon lange eingesetzt werden. Seit etwa 1960 werden Umspann- und Kraftwerke automatisiert und mit Leitstellensystemen (Scada) betrieben. Für die Fernsteuerung und Überwachung eines Umspannwerkes genügte damals ein Datendurchsatz von 50 bit/s. Was heute als OT bezeichnet wird, war unter dem Begriff Fernwirk- oder Leittechnik bekannt. Durch die stetig steigende Leistung der Systeme und die Weiterentwicklung können komplexere, schnellere und intelligentere Anwendungen umgesetzt werden. Wichtig ist bei heutigen OT-Systemen auch eine erhöhte Verfügbarkeit und eine lange Lebensdauer der Geräte.

Bei den Centralschweizerischen Kraftwerken AG, CKW, wurden die ersten Computersysteme in der OT eingesetzt, um Unterstationen fernzusteuern. Erst nach und nach wurden Rechenschieber und Schreibmaschinen durch IT-Systeme abgelöst.

Revolution der IT im Vergleich zur OT

In der IT wurden die Systeme rasch weiterentwickelt und immer breiter eingesetzt. Inzwischen werden IT-Systeme in nahezu allen Lebensbereichen eingesetzt und umfang-

Le terme « technologie opérationnelle », ou Operational Technology (OT), était jusqu'à présent peu connu dans le langage courant, bien que les technologies OT soient utilisées depuis longtemps. Depuis 1960 environ, les sous-stations et les centrales électriques sont automatisées et exploitées avec des systèmes de contrôle-commande (Scada). À l'époque, un débit de données de 50 bit/s était suffisant pour le contrôle et la surveillance à distance d'une sous-station. Ce que l'on appelle aujourd'hui OT était alors connu sous le nom de téléconduite ou contrôle-commande. Grâce à l'augmentation constante des performances des systèmes et à leur évolution, des applications plus complexes, plus rapides et plus intelligentes peuvent être mises en œuvre. Dans les systèmes OT actuels, une disponibilité accrue et une longue durée de vie des appareils sont également importantes.

Chez CKW (Centralschweizerische Kraftwerke AG), les premiers systèmes d'ordinateurs ont été utilisés dans le domaine de l'OT pour contrôler des sous-stations à distance. Ce n'est que progressivement que les règles à calcul et les machines à écrire ont été remplacées par des systèmes informatiques.

Bilder | Figures : CKW, Matthias Weinhold

reich genutzt. Ein Computer deckt heute eine Vielzahl von Funktionen und Anwendungen ab. Es können Dokumente bearbeitet, Videos geschaut oder E-Mails versendet werden. In der OT hingegen wurden Systeme für einen spezifischen Zweck entwickelt. Dies führte zu robusten Systemen mit langen Lebenszyklen. Bei Weiterentwicklungen wurde auf Rückwärtskompatibilität geachtet, um bereits bestehende Anlagen mit neuen Funktionen auszustatten und gleichzeitig bestehende Anlagenteile zu nutzen. Hersteller- oder anwendungsspezifische Protokolle und Architekturen sind weit verbreitet.

Verschmelzung von IT und OT

Auch die OT entdeckte die Vorteile der IT. Es wurde vermehrt versucht, proprietäre Systemumgebungen in standardisierte IT-Umgebungen zu überführen. Da in IT-Umgebungen die Grundsätze der OT wie hohe Stabilität, höchste Verfügbarkeit und lange Lebensdauer nicht zentral sind, entstanden neue Herausforderungen für die OT. Beispielsweise können bestimmte Patches in Betriebssystemen dazu führen, dass einzelne Funktionen verschwinden und auf diese Weise eine Leitsystemapplikation beeinträchtigen. Es kann auch vorkommen, dass ganze Systeme auf eine neue Systemversion migriert werden müssen, da eine bestehende Version nicht mehr unterstützt wird.

Technologien der IT und OT verschmelzen weiter, jedoch nicht in allen Bereichen. Grosse Synergien sind zwar vorhanden, aber die beiden Anwendungsbereiche unterscheiden sich vor allem in den Punkten Datenmenge, Langlebigkeit und Updatezyklen. Updates werden bei OT-Systemen oft auf das Nötigste beschränkt, um eine möglichst hohe Verfügbarkeit der Systeme zu gewährleisten. Durch die Verschmelzung und engere Vernetzung werden OT-Umgebungen näher an das Internet gebracht. Dies kann Systemschwachstellen wie unbefugte Zugriffe oder gar Manipulationen der OT-Systeme schaffen. Durch die langen Updatezyklen und die Nähe zum Internet können Schwachstellen leichter für Cyberangriffe genutzt werden. OT-Systeme, die bisher abgeschottet von der IT betrieben wurden, sind nun mit der IT vernetzt, um Daten aus dem Netzbetrieb direkt in den Business-Prozess weiterzureichen. In der OT besteht daher ein besonderer Bedarf an Sicherheitsvorkehrungen zur Cyber-Abwehr. Netzwerke in der OT werden aufgrund ihrer langen Lebenszyklen meist statisch aufgebaut. Protokolle, Ports und IP-Adressen für die Kommunikation unter den Systemen sind bekannt. Dies ermöglicht eine Kontrolle des Datenverkehrs zum Beispiel durch eine Deep Packet Inspection Firewall.

In einer OT-Umgebung im EVU-Umfeld stehen viele IT-fremde Anforderungen und Funktionen im Vordergrund. Die Anwendung von spezifischen Protokollen, wie z. B. nach den IEC 61850- oder IEC 60870-Standards sind in der OT üblich. Ihre Prüfung und Überwachung ist elementar. Zudem sind die Anforderungen an die Datenübertragung oft völlig unterschiedlich. IT-Umgebungen fordern hohe Bandbreiten für Big-Data-Anwendungen,

Révolution de l'IT par rapport à l'OT

Dans le domaine de l'informatique (IT), les systèmes ont évolué rapidement et sont de plus en plus utilisés. Désormais, des systèmes IT sont installés et amplement exploités dans presque tous les domaines de la vie. Aujourd'hui, un ordinateur couvre un large éventail de fonctions et d'applications. Il est possible de modifier des documents, de regarder des vidéos ou d'envoyer des e-mails. Dans le domaine de l'OT, par contre, les systèmes ont été conçus dans un but précis. Cela a mené à des systèmes robustes avec de longs cycles de vie. Lors des développements ultérieurs, une attention particulière a été portée sur la rétrocompatibilité afin d'équiper les systèmes existants de nouvelles fonctions tout en utilisant les composants existants des installations. Les protocoles et architectures spécifiques aux fabricants ou aux applications sont largement utilisés.

Fusion de l'IT et de l'OT

L'OT a, elle aussi, découvert les avantages de l'IT. Il a été maintes fois tenté de transformer des environnements de systèmes propriétaires en environnements IT standardisés. Étant donné que les principes fondamentaux de l'OT, tels qu'une stabilité élevée, une disponibilité maximale et une longue durée de vie, ne sont pas essentiels dans les environnements IT, l'OT a dû faire face à de nouveaux défis. Par exemple, certains patchs des systèmes d'exploitation peuvent entraîner la disparition de certaines fonctions et ainsi affecter une application du contrôle-commande. Il peut également arriver que des systèmes entiers doivent migrer vers une nouvelle version parce que la version utilisée n'est plus prise en charge.

Les technologies de l'IT et de l'OT continuent de fusionner, mais pas dans tous les domaines. Bien qu'il existe d'importantes synergies, les deux domaines d'application diffèrent principalement en termes de volume de données, de longévité et de cycles de mise à jour. Les mises à jour des systèmes OT sont souvent limitées au strict minimum afin de garantir la plus grande disponibilité possible des systèmes. La fusion et le renforcement de l'interdépendance rapprochent les environnements OT de l'Internet. Cela peut créer des vulnérabilités telles que des accès non autorisés ou même des manipulations des systèmes OT. Les longs cycles de mise à jour et la proximité de l'Internet rendent les failles plus faciles à exploiter pour les cyberattaques. Les systèmes OT qui étaient auparavant exploités de manière isolée, sans avoir recours à l'IT, sont désormais mis en réseau par le biais de l'IT afin de transférer des données relatives à l'exploitation du réseau directement dans le processus opérationnel. Dans le domaine de l'OT, il existe donc un besoin particulier en matière de mesures de sécurité relatives à la cyberdéfense. Dans l'OT, les réseaux ont tendance à être conçus de manière statique en raison de leur long cycle de vie. Les protocoles, les ports et les adresses IP pour la communication entre les systèmes sont connus. Les échanges de données peuvent ainsi être contrôlés, par exemple par un pare-feu DPI (Deep Packet Inspection).

OT-Umgebungen hingegen sind oft mit kleinen Bandbreiten zufrieden, brauchen dafür aber stabile, kurze Laufzeiten. Als Beispiel kann die Übertragung von Schutzsignalen verwendet werden: Hier müssen die Daten über weite Distanzen in wenigen Millisekunden gesichert und redundant übertragen werden. Gängige IT-Übertragungssysteme genügen diesen Anforderungen nicht.

Wo wir heute stehen

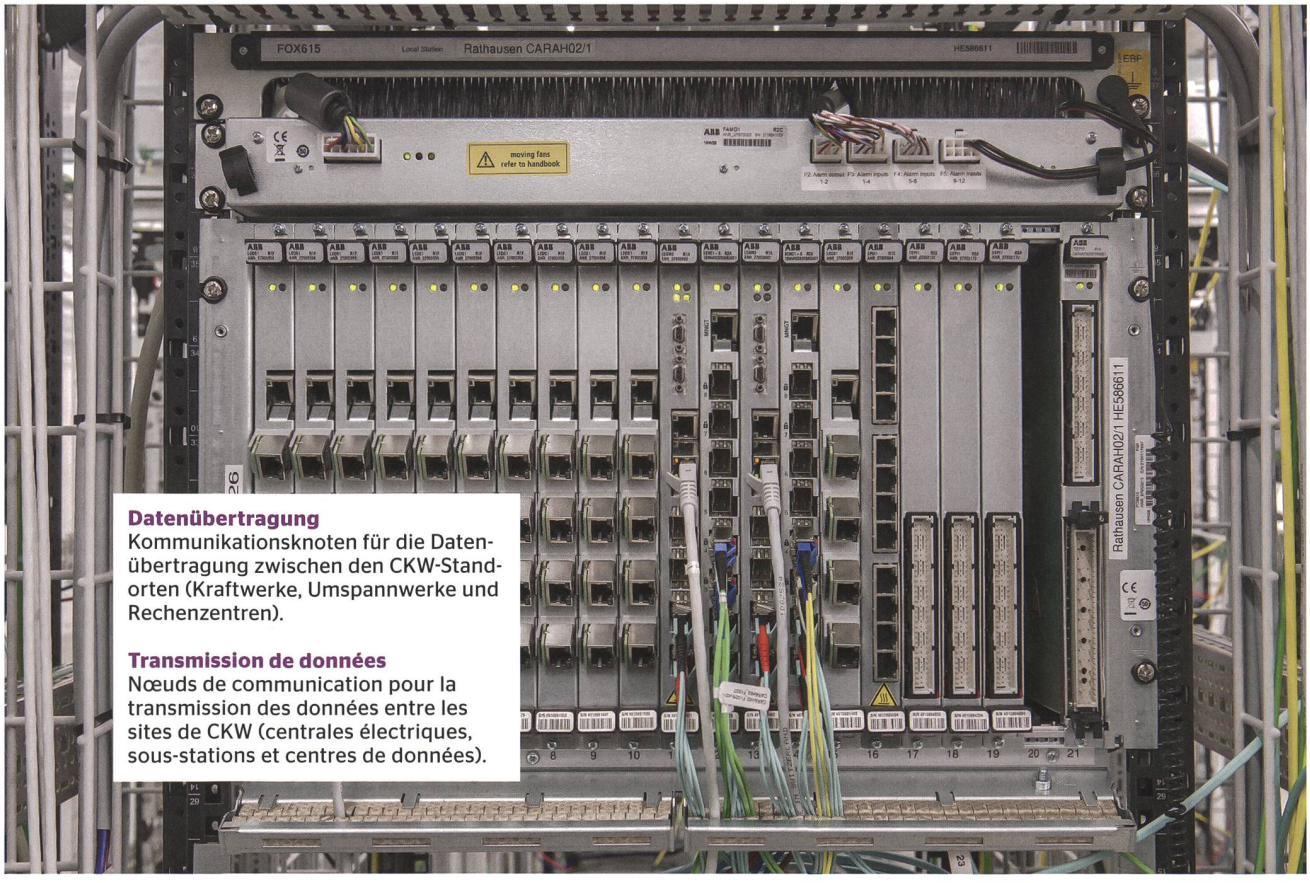
Aus heutiger Sicht ist es sinnvoll, IT- und OT-Systeme getrennt zu betreiben. Systeme für das Business und Systeme mit einem direkten Einfluss auf die Versorgungssicherheit sollten physisch und organisatorisch voneinander getrennt werden. Synergien können genutzt werden, wenn dies sinnvoll ist. Auch bieten heute einige grosse IT-Firmen Elemente wie Windows LTSC an, die besser für die OT geeignet sind. Eine OT-Umgebung muss heute nach einem Zonenmodell aufgesetzt sein (siehe Grundschutz «Operational Technology» in der Stromversorgung, VSE). Durch klar definierte Zonenübergänge wird ein kontrollierbarer Datenfluss sichergestellt und direkte Zugriffe aus dem Internet oder der Business-Umgebung auf die Kernsysteme verhindert. Zonenübergänge vom Business werden, wenn notwendig, zugelassen und mit den nötigen Sicherheitsmassnahmen umgesetzt.

Bei CKW wird das Zonenkonzept schon viele Jahre angewendet. Gleichzeitig wird auf eine starke Segmen-

Dans un environnement OT du secteur des EAE (entreprises d'approvisionnement en énergie), de nombreuses exigences et fonctions ne relevant pas du domaine de l'IT se trouvent au premier plan. L'utilisation de protocoles spécifiques tels que ceux conformes aux normes IEC 61850 ou IEC 60870 est courante dans le domaine de l'OT. Leur contrôle et leur surveillance sont élémentaires. En outre, les exigences en matière de transmission de données sont souvent complètement différentes. Les environnements IT exigent de grandes largeurs de bande pour les applications « big data », tandis que les environnements OT se contentent souvent de petites largeurs de bande, mais ont besoin de temps d'exécution courts et stables. À titre d'exemple, lors de la transmission de signaux de protection, les données doivent être sécurisées et transmises de manière redondante sur de longues distances en quelques millisecondes. Les systèmes de transmission informatiques courants ne répondent pas à ces exigences.

La situation actuelle

À l'heure actuelle, il est logique d'exploiter séparément les systèmes IT et OT. Les systèmes de l'entreprise et les systèmes ayant une influence directe sur la sécurité de l'approvisionnement doivent être séparés les uns des autres aussi bien physiquement que du point de vue organisationnel. Les synergies peuvent être exploitées lors-



Datenübertragung
Kommunikationsknoten für die Datenübertragung zwischen den CKW-Standorten (Kraftwerke, Umspannwerke und Rechenzentren).

Transmission de données
Nœuds de communication pour la transmission des données entre les sites de CKW (centrales électriques, sous-stations et centres de données).

tierung der Netzwerke und die Schaffung von kontrollierbaren Übergängen gesetzt. Durch die Segmentierung wird eine konsequente Überwachung und Kontrolle des Datenverkehrs durch Firewalls ermöglicht. Die Kommunikation in der OT findet grundsätzlich nach dem Whitelisting-Ansatz statt. Vor der Inbetriebnahme von neuen Systemen wird mit einer Portmatrix festgelegt, wie die einzelnen Systemkomponenten untereinander kommunizieren und wer die Verbindung aufbaut. Nur in der Portmatrix definierte Verbindungen (Ports und Protokolle) werden auf der Firewall freigeschaltet. Mit der neusten Generation von Umspannwerken wird dieses Konzept bis auf die Feldebene angewendet. Daten werden ausserhalb der Rechenzentren oder Anlagen grundsätzlich nur verschlüsselt übertragen. Um dem breiten Spektrum an Kommunikationsanforderungen gerecht zu werden, wurde das Datenübertragungssystem auf den neusten Stand der Technik gebracht.

Im Konzept von CKW sind in Umspannwerken stehende Ethernet-Verbindungen nicht erlaubt. Wenn Verbindungen benötigt werden, müssen sie zugeschaltet werden. Bereits 2019 wurde eine IT-unabhängige OT-Client-Umgebung geschaffen, um den sicheren Fernzugriff auf die OT-Systeme zu gewährleisten. Mit der OT-Client-Umgebung werden Service-Notebooks von Lieferanten längerfristig überflüssig. Die permanente Netzwerküberwachung wird durch den Einsatz von Intrusion Detection Systemen (IDS) sichergestellt. Die IDS zeichnen Datenpakete im Netzwerk von der Zentrale bis zur Feldebene auf und senden sie an eine zentrale Stelle (Security Information and Event Management, SIEM). Die OT-Umgebung als Ganzes ist an einen Security Operations Center (SOC) Provider angeschlossen, um allfällige Cyberattacken frühzeitig zu erkennen.

Aber man setzt nicht nur auf technische Massnahmen, um eine sichere und stabile OT-Umgebung zu erreichen, sondern auch auf Massnahmen im Bereich der Mitarbeiterschulung, um das Sicherheitsbewusstsein zu schärfen. Die OT-Umgebung wird bei CKW kontinuierlich nach einem risikobasierten Ansatz analysiert und auf Schwachstellen überprüft. Nötige Verbesserungen werden priorisiert, geplant, umgesetzt und anschliessend geprüft.

Synergien werden genutzt, wo sie sinnvoll sind. Virtuelle Umgebungen ermöglichen hardwareunabhängige Systeme und nutzen Hardware optimal aus. IT-übliche Backupsoftware wird für die Langzeitsicherung der Daten genutzt. Ebenfalls unterstützen Systeme aus der IT bereits heute OT-Systeme bei der Userauthentisierung oder stellen Betriebssystemupdates für den OT-Bereich zur Verfügung. Durch die Kaskadierung von IT und OT nach Zonenkonzept ist eine enge Zusammenarbeit zwischen OT und IT unabdingbar.

Neue Herausforderungen

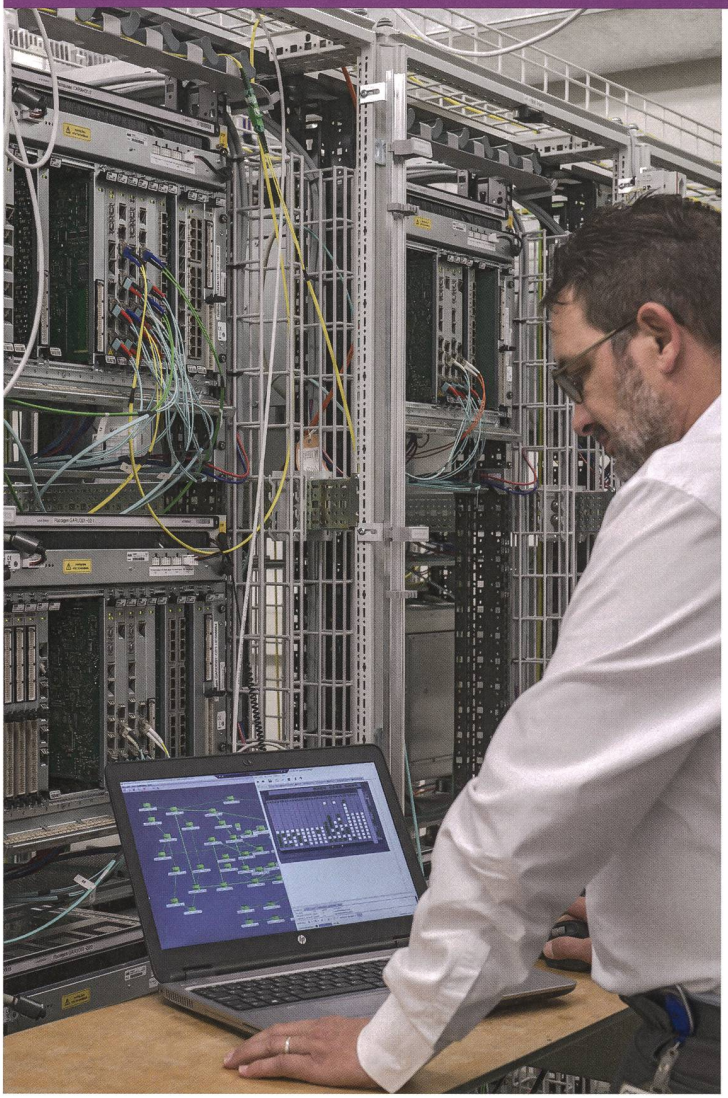
Durch die Digitalisierung werden immer wieder neue Anforderungen an die OT-Systeme gestellt. So müssen beispielsweise Fernzugriffe auf Systeme, Anbindungen an einen SMS-Versanddienst oder direkter Datenaus-

Präzise Zeitreferenz
Zeitquellen für die Synchronisierung des Kommunikationsnetzes, um Daten und Schutzsignale übertragen zu können.

Une référence de temps précise
Sources de temps utilisées pour la synchronisation du réseau de communication afin de pouvoir transmettre des données et des signaux de protection.

qu'il est judicieux de le faire. De plus, certaines grandes entreprises informatiques proposent aujourd'hui des éléments tels que Windows LTSC, qui sont mieux adaptés à l'OT. Aujourd'hui, un environnement OT doit être configuré selon un modèle de zones (voir le manuel de l'AES intitulé Protection de base pour les « technologies opérationnelles » (OT) dans l'approvisionnement en électricité). Des jonctions clairement définies entre les zones garantissent un flux de données contrôlable et empêchent l'accès direct aux systèmes centraux à partir d'Internet ou de l'environnement métier. Si nécessaire, des jonctions entre les zones de l'entreprise sont autorisées et réalisées avec les mesures de sécurité appropriées.

Chez CKW, le concept de zones est utilisé depuis de nombreuses années. Dans le même temps, l'accent est mis sur une forte segmentation du réseau et la création de jonctions contrôlables. La segmentation permet une surveillance et un contrôle conséquents du trafic de données par des pare-feu. La communication dans l'OT se fait essentiellement selon l'approche de la liste blanche (whitelist). Avant la mise en service de nouveaux systèmes, une matrice de ports est utilisée pour définir comment les différents composants du système communiquent entre eux et qui établit la connexion. Seules les connexions (ports et protocoles) définies dans la matrice sont activées sur le pare-feu. Avec la dernière génération de sous-stations, ce concept est appliqué jusqu'au niveau du terrain. Les données ne sont transmises a priori que sous forme cryptée en dehors des centres de données ou des installations. Afin de



OT im Einsatz
Stefan Mattmann arbeitet am GridCom-2020+-Netz: Knotenübersicht der CKW und Knotenkonfiguration.

L'OT en action
Stefan Mattmann travaillant sur le réseau GridCom 2020+ : vue d'ensemble et configuration des nœuds de CKW.

tausch mit Businessanwendungen realisiert, oder ein einfacher Datenaustausch über Filetransfers durch dynamische Datenbankabfragen oder Webschnittstellen ersetzt werden. Innerhalb der OT ist ein breites Spektrum an unterschiedlichen Geräten von diversen Lieferanten vorhanden. Feldgeräte wie Schutz- und Steuergeräte kommunizieren mit lokalen Leitstellensystemen in den Umspannwerken. Diese wiederum sind mit den zentralen Systemen zur Netzsteuerung und Überwachung verbunden. Systeme zur Datenübertragung und Datennetzüberwachung verbinden alles miteinander. All diese Einrichtungen verlangen nach eigenen Parametrierumgebungen und Updatesystemen, und stellen unterschiedliche Anforderungen an die Datenübertragung. So werden innerhalb der Umspannwerke Protokolle wie IEC 61850 eingesetzt, um einen schnellen Austausch von Verriegelungssignalen sicherzustellen, oder Daten werden in der Leitstelle aus dem Langzeitspeicher mit Hilfe einer Rest (https)-Schnittstelle direkt von der Business-IT abgerufen.

répondre au large éventail des exigences en matière de communication, le système de transmission des données a été mis à niveau conformément aux dernières avancées technologiques.

Dans le concept de CKW, les connexions Ethernet continues ne sont pas autorisées dans les sous-stations. Si des connexions sont nécessaires, elles doivent être établies. Un environnement client OT indépendant de l'IT a déjà été créé en 2019 pour garantir un accès à distance sécurisé aux systèmes OT. Avec l'environnement client OT, les carnets de service des fournisseurs deviendront superflus à long terme. La surveillance permanente du réseau est assurée par l'utilisation de systèmes de détection d'intrusion (IDS). Les IDS enregistrent les paquets de données au sein du réseau, de la centrale jusqu'au niveau du terrain, et les envoient à une autorité centrale (Security Information and Event Management, SIEM). L'environnement OT dans son ensemble est connecté à un « Security Operations Center (SOC) provider » afin de détecter toute cyberattaque à un stade précoce.

Cependant, l'entreprise ne s'appuie pas seulement sur des mesures techniques pour atteindre un environnement OT sûr et stable, mais aussi sur des mesures relatives à la formation des employés pour les sensibiliser à la sécurité. L'environnement OT de CKW est continuellement analysé selon une approche basée sur les risques et contrôlé de manière à détecter les failles. Les améliorations nécessaires sont classées par ordre de priorité, planifiées, mises en œuvre et ensuite testées.

Les synergies sont exploitées lorsqu'elles sont judicieuses. Les environnements virtuels permettent de réaliser des systèmes indépendants du matériel et exploitent le hardware de manière optimale. Un logiciel de sauvegarde informatique standard est utilisé pour la sauvegarde à long terme des données. De même, les systèmes IT soutiennent déjà les systèmes OT dans l'authentification des utilisateurs ou fournissent des mises à jour du système d'exploitation pour le domaine de l'OT. Le montage en cascade de l'IT et de l'OT selon le concept de zones rend une coopération étroite entre ces technologies indispensable.

Nouveaux défis

La numérisation impose constamment de nouvelles exigences aux systèmes de technologie opérationnelle. Il faut par exemple mettre en place des accès à distance aux systèmes, des connexions à un service d'envoi de SMS ou un échange direct de données avec des applications métiers, ou encore remplacer un simple échange de données par transferts de fichiers par des requêtes dynamiques de bases de données ou des interfaces Web. L'OT utilise un large éventail de dispositifs différents provenant de divers fournisseurs. Les appareils de terrain tels que les dispositifs de protection et de contrôle communiquent avec les systèmes de contrôle locaux au sein des sous-stations. Ces derniers sont à leur tour connectés aux systèmes centraux pour le contrôle et la surveillance du réseau. Les systèmes de transmission de données et de surveillance des réseaux de données relient le tout.

Wo die Reise noch hingehen wird

Die Verschmelzung von IT und OT wird auch in Zukunft weitergehen. In den einzelnen Bereichen wird es aber stets Spezialdisziplinen geben, die nicht mit einem Standardprodukt abgedeckt werden können. Die Datenbeschaffung über Internet-of-Things-Sensoren wird auch in der OT Einzug halten. Voraussetzung für die Nutzung solcher Sensoren ist ein bewusster Umgang mit der Datenqualität und der Sicherheit solcher Daten in der OT. Für zukünftige OT-Systeme werden auch Teilanwendungen in der Cloud ein Thema werden. So könnten Applikationen ohne direkten Einfluss auf die Versorgungssicherheit in der Cloud gehostet werden, sofern dies sinnvoll ist und im Zonenkonzept abgebildet werden kann. Ähnliche Anforderungen stellt der Einsatz von mobilen Geräten wie Handy oder Tablet. Für künftige Systeme können Applikationen auf solchen Geräten eine wichtige Rolle spielen, um beispielsweise Schaltprogramme oder Anweisungen zu übertragen. Hier müssen allerdings erst die Grundlagen geschaffen werden. Die Systemsicherheit in der OT hängt auch von einem aktuellen Patchlevel ab. Mit umfassenden Testsystemen können Patches oder Softwareanpassungen getestet und anschliessend auf das Livesystem übertragen werden. Dies ermöglicht einen stabilen Betrieb der OT-Umgebung. Im Bereich der Security könnten Systeme zur automatischen Isolierung von potenziell gefährlichen Netzwerkteilnehmern eingesetzt werden. Natürlich stets mit Priorität auf dem Weiterbetrieb der kritischen Infrastruktur.

Kooperation und Kompetenz

Um den heutigen und den künftigen Anforderungen in der OT gerecht zu werden, wird eine enge Zusammenarbeit der einzelnen Teilbereiche innerhalb der OT wie auch der IT vorausgesetzt. Der Einbezug von Lieferanten und die gemeinsame Lösungserarbeitung werden noch weiter an Bedeutung gewinnen. Je früher alle Disziplinen innerhalb der OT integriert werden, desto eher lässt sich eine gute Lösung für die Umsetzung von modernen Systemen finden. Um die Anforderungen der OT umsetzen zu können, sind gut ausgebildete Fach- und Führungskräfte mit einem breiten Wissen über den gesamten OT- und IT-Bereich notwendig.

Autoren | Auteurs
Yann Gosteli ist Leiter Sekundäranlagen bei CKW.
Yann Gosteli est responsable des installations secondaires chez CKW.
→ CKW, 6002 Luzern
→ Yann.Gosteli@ckw.ch

Stefan Mattmann ist Senior System Engineer Grid Communication.
Stefan Mattmann est Senior System Engineer Grid Communication.
→ stefan.mattmann@ckw.ch

Remo Niffeler ist Leiter Grid Communication.
Remo Niffeler est responsable du secteur Grid Communication.
→ remo.niffeler@ckw.ch

Toutes ces installations nécessitent leurs propres environnements de paramétrage et systèmes de mise à jour, et imposent des exigences différentes en matière de transmission de données. Ainsi, des protocoles, par exemple IEC 61850, sont utilisés dans les sous-stations pour assurer un échange rapide des signaux de verrouillage ou, dans le centre de contrôle, des données sont extraites directement de la mémoire à long terme par l'informatique de l'entreprise à l'aide d'une interface Rest (https).

Ce que l'avenir nous réserve

La fusion de l'IT et de l'OT se poursuivra à l'avenir. Dans les différents domaines, cependant, il y aura toujours des disciplines spécifiques qui ne pourront pas être couvertes par un produit standard. L'acquisition de données par le biais de capteurs de l'Internet des objets trouvera également sa place dans l'OT. La condition préalable à l'utilisation de tels capteurs sera une approche consciente de la qualité et de la sécurité de ces données dans le domaine de l'OT. Pour les futurs systèmes OT, il sera également possible d'envisager des applications partielles dans le cloud. Ainsi, les applications qui n'ont pas d'influence directe sur la sécurité de l'approvisionnement pourraient être hébergées dans le cloud, à condition que cela soit judicieux et puisse être représenté dans le concept de zones. L'utilisation d'appareils mobiles tels que les téléphones portables ou les tablettes doit répondre à des exigences similaires. Pour les futurs systèmes, des applications installées sur ces dispositifs pourront jouer un rôle important, par exemple pour transmettre des instructions ou des programmes de commutation. Toutefois, pour cela, les bases devront d'abord être posées. La sécurité des systèmes OT dépend également de la mise à jour des patchs. Les patchs ou les adaptations logicielles peuvent être testés, puis transférés vers le système opérationnel grâce à des systèmes de test complets. Cela permet un fonctionnement stable de l'environnement OT. Dans le domaine de la sécurité, des systèmes pourraient être utilisés pour isoler automatiquement des utilisateurs du réseau potentiellement dangereux. Bien entendu, en priorisant toujours la poursuite du fonctionnement de l'infrastructure critique.

Coopération et compétence

Une coopération étroite entre les différents sous-secteurs de l'OT et de l'IT sera nécessaire pour répondre aux exigences actuelles et futures de l'OT. L'implication des fournisseurs et le développement conjoint de solutions deviendront encore plus importants. Plus vite toutes les disciplines seront intégrées à l'OT, plus rapidement une bonne solution pourra être trouvée pour la mise en œuvre de systèmes modernes. Pour être en mesure de répondre aux exigences de l'OT, des spécialistes et des gestionnaires bien formés, ayant une connaissance approfondie de l'ensemble des domaines de l'OT et de l'IT, sont indispensables.