



Funktionale Prüfung von Stationsautomatisierungssystemen

1 Einführung

Wenn es um die Prüfung der Sekundärtechnik für Umspannwerke geht, ist das standardisierte und automatisierte Prüfen der Schutzgeräte und -systeme bewährte Praxis. Für die Prüfung der Schutzeinstellungen und -funktionen stehen entsprechende Prüfinstrumente und -methoden zur Verfügung. Für spezifische Schutzrelais-typen können Prüfpläne erstellt werden, die in bestimmten Phasen eines Projekts wiederverwendet werden können, beispielsweise bei der Werksabnahme (Factory Acceptance Test - FAT), der Inbetriebnahme, der Anlagen-übernahme (Site Acceptance Test - SAT) und der laufenden Wartung im Betrieb.

Andererseits erfolgt die Prüfung des Stationsautomatisierungssystems (SAS) mit seinen vielen Automatisierungs-, Steuerungs- und Leittechnikfunktionen in der Regel manuell. Derzeit ist es so, dass das Prüfen des Automatisierungs- und Kommunikationssystems meist länger dauert als das Prüfen der Schutzfunktionen. Automatisierungssysteme werden immer komplexer und der Aufwand für das Prüfen der Kommunikation und der Verriegelungslogik sowie der ordnungsgemäßen Übertragung der notwendigen Signale an die Leitstellen ist enorm gestiegen.

In Schaltanlagen müssen im Rahmen der FAT und SAT alle Schnittstellen zwischen den Feldgeräten (Intelligent Electronic Device – IED) und der Primärtechnik geprüft werden. Diese Prüfungen erfolgen zum Beispiel bei fest

verdrahteten Schnittstellen üblicherweise so, dass jedes einzelne Signal in ausgedruckten Funktionsdiagrammen und Schaltplänen per Hand „grün markiert“ wird. Zum Prüfen der implementierten Logikfunktionen, wie z. B. der Befehlsverriegelungen, müssen viele physische Eingänge gleichzeitig gesetzt werden und die Logik muss durch Ausführen der entsprechenden Steuerbefehle verifiziert werden. Zum Prüfen der Signalübertragung zu den Leitstellen wird eine Ende-zu-Ende-Prüfung durchgeführt. Dazu werden die Signale direkt auf Betriebsmittelebene in der Schaltanlage oder durch Simulation an den Eingängen der IEDs stimuliert. In der Regel sind zusätzliche Unterlagen erforderlich, wie beispielsweise eine Liste der Fernwirksignale und deren Adress- und Funktionszuordnungen.

Dieser Prozess, der vorzugsweise im Zuge der Werksabnahme vor der eigentlichen Montage durchgeführt wird, dauert bei einer typischen Schaltanlage mehrere Wochen und erfordert die Einbeziehung mehrerer erfahrener Leittechnik- und Schutzspezialisten. Für die Systemprüfung im Werk sollte idealerweise Folgendes vorhanden sein:

- im Idealfall das gesamte SAS mit allen Feldgeräten, der gesamten Netzwerktechnik, den Fernwirk-Gateways, den Nahsteuerplätzen, usw.
- ein mit den Feldgeräten fest verdrahteter Schaltanlagensimulator (sowohl einfache Schalter und LED-Anzeigen als auch anspruchsvolle SPS-basierte Simulatoren sind möglich),

- ein Leitstellensimulator mit Unterstützung für das verwendete Leitstellenprotokoll (z. B. IEC 60870-5-104, DNP3)
- Werkzeuge für die Netzwerkprüfung und die IED-spezifischen Wartungstools
- umfangreiches Wissen über die verwendeten Produkte, die Norm IEC 61850 und Ethernet-Netzwerke ganz allgemein
- sorgfältig ausgearbeitete Prüfpläne und Unterlagen (Signalübersicht, Verriegelungslogiken und andere Prüfverfahren).

In der Regel sind aber nicht alle Komponenten des SAS im Werk verfügbar. Dies ist beispielsweise dann der Fall, wenn die IEDs als Teil der Schaltanlagenlieferung direkt an den Standort des Umspannwerkes gesendet werden, ohne dass zuvor eine komplette Systemprüfung stattfindet. In diesen Fällen muss die Prüfung vollständig vor Ort erfolgen, was sich auf den Aufwand und die Kosten auswirkt.

Erfahrungen aus der Praxis zeigen: Je besser das System im Werk geprüft wird, desto weniger Probleme treten bei der Inbetriebnahme und bei der Abnahme auf und desto effizienter und reibungsloser läuft das Projekt.

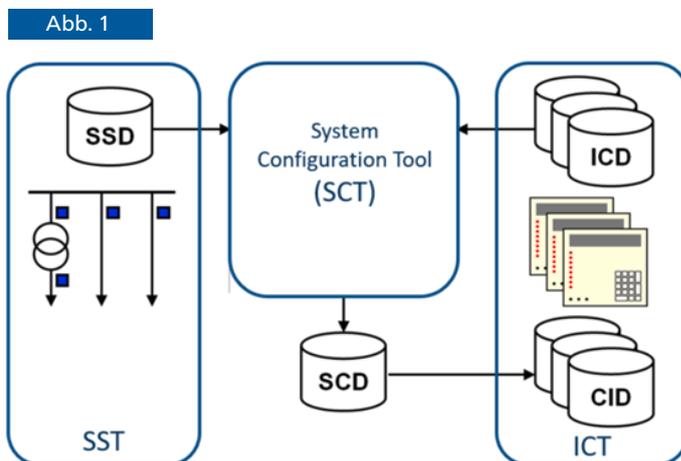
Im Zuge der Prüfung werden Fehler in den Geräteparametern und manchmal auch in der Gerätefirmware erkannt und behoben. Aber jede Firmwareaktualisierung und auch jede Änderung der Geräteeinstellungen macht zumindest eine erneute Prüfung der betroffenen Funktion und idealerweise sogar des gesamten Systems erforderlich. Erfolgt diese Prüfung manuell, ist der Prozess nicht effizient. Daher wird dringend eine stärker automatisierte und effizientere Systemprüfung gefordert. Eine solche Lösung, die auf dem SCL-Konzept basiert, das wiederum Teil der Norm IEC 61850 ist, ist heute bereits verfügbar.

2 IEC 61850 und das SCL-Konzept

IEC 61850 ist die internationale Norm für die Automatisierung in der Energieversorgung und definiert neben Kommunikationsprotokollen auch die verwendeten Datenmodelle. Darüber hinaus ist in der Norm auch ein allgemeines, herstellerunabhängiges Konfigurationskonzept definiert. In diesem Prozess werden maschinenlesbare Konfigurationsinformationen verwendet, die in einem XML-basierten standardisierten Format namens SCL (System Configuration Language) gespeichert sind.

2.1 Engineeringprozess mit SCL

Das SCL-Konzept ist im Teil 6 der IEC 61850 definiert. Der Hauptzweck der SCL besteht darin, den kompatiblen Austausch von Konfigurationsdaten zwischen den



SCL-Konzept

Konfigurations- und Prüfwerkzeugen verschiedener Hersteller zu ermöglichen.

In Abb. 1 ist das allgemeine Konzept des Engineeringprozesses eines SAS unter Verwendung des Datenaustauschformats SCL dargestellt.

Für den Austausch von Informationen sind die folgenden Arten von SCL-Dateien spezifiziert (mit jeweils eigener Dateinamenerweiterung):

- **SSD (System Specification Description):** Dieser Dateityp wird zur Beschreibung des einpoligen Schaltbildes der Anlage, der Spannungsebenen, der Primärausrüstung und der erforderlichen logischen Knoten (logical nodes - LN) für die Implementierung der Funktionen zur Anlagenautomatisierung verwendet. Die SSD-Datei wird von einem SST (System Specification Tool) generiert.
- **ICD (IED Capability Description):** Dieser Dateityp dient zur Beschreibung der Funktionsmerkmale eines IED-Typs. Für jeden IED-Typ gibt es eine zugehörige ICD-Datei. Sie enthält Angaben zu den logischen Knoten, Daten und unterstützten Diensten für das IED und wird vom herstellereigenen ICT (IED Configuration Tool) generiert.
- **SCD (System Configuration Description):** Dieser Dateityp enthält alle konfigurierten IEDs, die Kommunikationskonfiguration und alle IEC-61850-Aspekte für das jeweilige System. Diese Datei wird vom SCT (System Configuration Tool) generiert.
- **CID (Configured IED Description):** Dateien dieses Typs enthalten einen Teil der SCD-Datei mit allen Informationen für ein konkretes IED. Private Erweiterungen sind zulässig.

Prinzipiell kommen drei Arten von Engineering-Tools zum Einsatz: SST (System Specification Tool), SCT (System Configuration Tool) und ICT (IED Configuration Tool). Bei Systemen, die vollständig nur von einem Hersteller

stammen, wird in der Praxis häufig ein All-in-One-Tool und keine SSD-Datei verwendet. Bei SAS mit Komponenten verschiedener Hersteller und herstellerspezifischen ICTs kommt in der Regel ein herstellernerutrales SCT zum Einsatz. Zunehmend setzen die Netzbetreiber auf eine weitgehende Standardisierung der Anlagen und spezifizieren daher das Datenmodell und die Kommunikationsdienste ihrer SAS mittels eines SST Werkzeuges schon vor Beginn der eigentlichen Systemparametrierung.

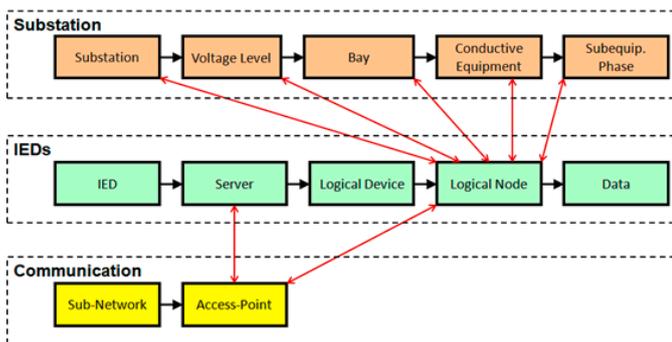
Mit dem SCT wird der systemweite Datenfluss der Anlage konfiguriert. Dazu können ICD-Dateien aus allen IEDs sowie die SSD-Datei in das SCT importiert werden. Das SCT Tool unterstützt sowohl die Parametrierung der horizontalen (GOOSE und Sampled Values) und vertikalen Kommunikationsverbindungen (Client/Server-Reports). Durch die Nutzung von Daten aus der SSD-Datei oder die direkte Eingabe lassen sich IED-Funktionen (logische Knoten) mit der Primärtechnik und deren Funktionen verknüpfen. Am Ende generiert das SCT die SCD-Datei, die das vollständige System dokumentiert.

2.2 SCL-Inhalt

Die SCL in ihrer Gesamtheit ermöglicht die Beschreibung eines aus drei Grundbausteinen bestehenden Modells der Anlage:

- Substation/Station: Beschreibt das einpolige Schaltbild der Anlage, die Primärtechnik und die Funktionen; wie ist die Primärtechnik, z. B. der Leistungsschalter, mit den virtuellen logischen Knoten im IED „verbunden“.
- IED: Beschreibt alle Hardwaregeräte (IEDs), die im SAS verwendet werden. In diesem Teil wird das im IED implementierte Datenmodell einschließlich seiner logischen Geräte und logischen Knoten beschrieben. Die Verbindung zwischen IEDs und Kommunikationssystem wird über dessen Zugangspunkte hergestellt.
- Communication/Kommunikation: Beschreibt die logisch möglichen Verbindungen zwischen den IEDs in Teilnetzwerken über Zugangspunkte (Kommunikationsports).

Abb. 2



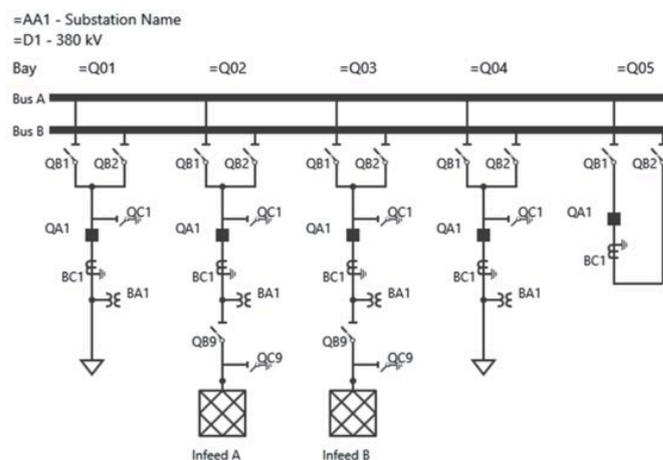
SCL-Inhalt

Eine vollständige SCD-Datei besteht aus diesen drei Teilen und einem Abschnitt mit Datentypvorlagen zur Beschreibung der von den IEDs verwendeten Daten und Attribute.

2.3 Schaltanlage und funktionale Adressierung

Dieser Teil der SCL spiegelt die Primärtechnik wider und beschreibt, welche Schaltgeräte verwendet werden und wie die Ausrüstung verbunden ist. Die Objekte in diesem Abschnitt sind hierarchisch geordnet und gemäß IEC 81346 benannt. Abb. 3 zeigt ein Beispiel für ein einpoliges Schaltbild einer Schaltanlage, bei dem die Benennungen hinsichtlich Aufbau und Ausrüstung, z. B. hinsichtlich der Trenn- und Leistungsschalter, der Norm IEC 81346 folgen.

Abb. 3



Beispiel für eine Anlagentopologie

Der Hauptzweck dieses Abschnitts ist die Ableitung einer eindeutigen Funktionsbezeichnung für die abstrakten logischen Knoten, die in den IEDs implementiert sind. Andernfalls ist es für den Systemprüfer schwierig herauszufinden, welche konkrete LN-Instanz im IED mit welchem Primärelement in der Schaltanlage „verbunden“ ist.

2.4 Inhalt und Verwendung von SCD-Dateien

Wie oben erläutert ist die SCD-Datei das Endergebnis aus einem vollständigen Systementwurf gemäß IEC 61850. Die SCD-Datei wird nicht nur von Engineering-Werkzeugen und zu Dokumentationszwecken sondern auch für die Anlagenprüfung verwendet. Prüfwerkzeuge helfen dabei, Prüfungen effizienter zu machen, indem sie die Informationen in der SCD-Datei für die Prüfung der Anlage verwenden.

Die Norm gibt zwar ein klares Konzept für den Engineeringprozess vor, sie enthält aber keinerlei Mindestanforderungen an den Inhalt der SCD-Datei. So ist beispielsweise die Bereitstellung von Topologieinformationen im Abschnitt <Substation> optional. Die Informationen im IED-Abschnitt sind von den Merkmalen der konkreten im Projekt verwendeten IED-Produkte abhängig. Den Anlagenverantwortlichen wird daher dringend empfohlen, in die SAS-Spezifikationen, die für Projektausschreibungen

und Serviceverträge verwendet werden, die Mindestanforderungen an die SCD-Datei aufzunehmen, wie z. B. folgende:

- Der Abschnitt <Substation> muss alle Spannungsebenen, Felder und Leistungs-/Trennschalter mit ihren LN-Referenzen (XCBR/XSWI, CSWI und CILO) enthalten
- Datenobjekte müssen „desc“-Beschreibungsattribute mit dem vom Eigentümer vorgegebenen Signaltexten enthalten
- GOOSE-Subskriptionen müssen im <GSEControl>-Element <IEDName>-Elemente sowie <Inputs><ExtRef type="GOOSE">-Elemente verwenden
- Alle Clients wie die Fernwirk-Gateways oder Human-Machine-Interfaces (HMIs) müssen definiert sein und die Report Control Blocks im IED müssen reserviert und im <ReportControl>-Element mit <ClientLN> angegeben sein.
- Alle in Reports verwendeten Datensätze müssen statisch sein (da dynamische Datensätze nicht in der SCD-Datei dokumentiert werden)

Je besser die Qualität und der Inhalt der SCD-Datei der Anlage ist, desto effizienter wird die Systemprüfung ablaufen. Eine konforme SCD-Datei ist außerdem bei späteren Erweiterungen der Anlage äußerst hilfreich, dazu aber später.

3 Neuer Ansatz für die Prüfung eines SAS unter Verwendung der SCD-Datei

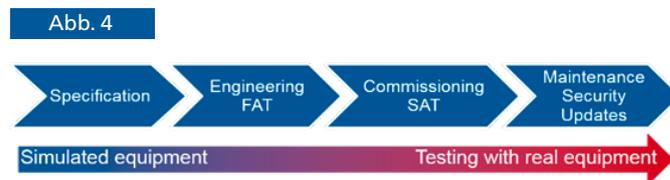
3.1 Prüfansatz

Wie bereits erwähnt, werden Prüfungen der Automatisierungs- und Leittechnikfunktionen normalerweise manuell durchgeführt. Es gibt seit vielen Jahren Tools die das manuelle Prüfen und Simulieren einzelner IEDs ermöglichen.

Die hier vorgestellte Methode erlaubt zusätzlich zum Prüfen und Simulieren einzelner IEDs auf das Prüfen des gesamten SAS. Die Prüfung basiert vollständig auf der SCD-Konfigurationsdatei. Durch Importieren der SCD-Datei kann das gesamte System visualisiert werden und alle in der SCD-Datei enthaltenen Informationen werden genutzt. Die Informationen im Abschnitt <Substation> werden genutzt, um die IEDs und die Schaltanlagenausstattung in ihrer jeweiligen Spannungsebene graphisch zu visualisieren. Wie in Abb. 5 zu sehen, wird das System in Anlehnung an das vertraute einpoligen Schaltbild der Anlage dargestellt.

Die vorgeschlagene Methode eignet sich zum Prüfen des SAS während des gesamten Lebenszyklus. Die Projektphasen werden in IEC 61850 4 beschrieben und in Abb. 4

dargestellt. Das Werkzeug, das diese Methode verwendet, unterstützt sowohl die Überwachung und Fehlersuche als auch das Simulieren des Systems. Während einer Prüfung hat das Prüfgerät Zugriff auf den GOOSE-Netzwerkverkehr und ist auch direkt mit den IEDs verbunden.



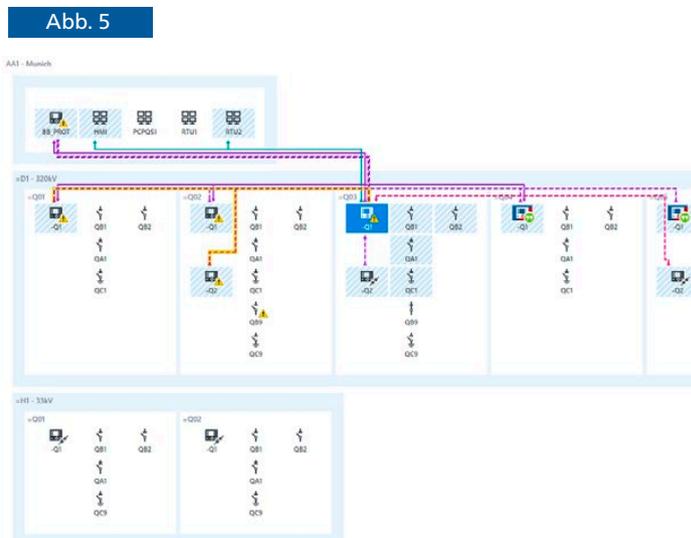
SAS-Lebenszyklus

Bereits in der Spezifikationsphase des Projektes können die SCD-Datei, die Signale und die Kommunikationsdienste ohne physisch vorhandene Geräte validiert werden. Später lassen sich die Fernwirk-Gateways und HMIs durch Simulieren des Kommunikationsverhaltens und der Signale aller IEDs prüfen – auch hier wieder ohne das eigentliche IED. Während der Werksabnahme können die nicht vorhandenen IEDs simuliert werden, um eine Prüfung der bereits verfügbaren IEDs zu ermöglichen. Bei der Inbetriebnahme wird schlussendlich die komplette Anlage mit den realen IEDs geprüft.

Einer der entscheidenden Faktoren für einen effizienten Ansatz ist die Möglichkeit, Prüfpläne zu erstellen. Es ist somit möglich, ein Prüfverfahren zu dokumentieren und dieses während des gesamten Lebenszyklus des SAS wiederzuverwenden. Prüfsequenzen können automatisch ausgeführt und bewertet werden.

3.2 SAS-Funktionsprüfung mit StationScout

StationScout ist eine innovative Prüflösung für IEC-61850-Anlagen, die alle der oben beschriebenen erforderlichen Prüffunktionen bietet. StationScout vereinfacht Prüfungen von SAS und reduziert den erforderlichen Prüfaufwand erheblich. Es wird mit einer robusten und leistungsstarken



Beispiel SCL, in StationScout

Hardware geliefert, die es Benutzern ermöglicht, viele IEDs mit IT-sicherer Verbindung zum SAS-Netzwerk gleichzeitig zu simulieren. Mit der benutzerfreundlichen Software wird die SCL-Datei der Anlage ohne zusätzlichen Konfigurationsaufwand visualisiert und einzelne Signale können live verfolgt werden.

In den folgenden Abschnitten werden einige Anwendungsfälle aus der Praxis beschrieben, in denen StationScout zur Fehlersuche und zur Prüfung des SAS eingesetzt wurde.

3.3 Verifizierung der Kommunikationsverbindungen

Wenn die SCD-Datei geladen wird und Zugriff auf den Netzwerkverkehr und die MMS-Verbindung zu den IEDs besteht, kann StationScout alle GOOSE-, SV- und Report-Kommunikationsverbindungen automatisch validieren.

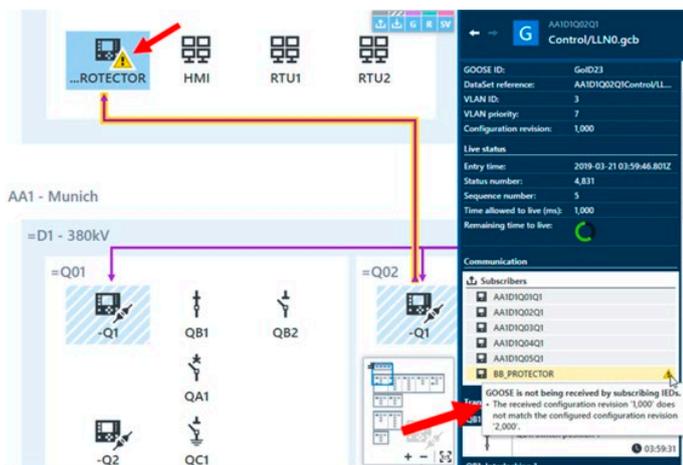
Das Prüfgerät kann Attribute in den IEDs abfragen und diese anhand des SCD-Modells validieren. Der Benutzer kann beispielsweise prüfen, welche Reports gerade aktiviert sind und ob die Report-Owner die in der SCD-Datei angegebenen Clients sind.

GOOSE-Kommunikationsverbindungen werden automatisch auf folgende Kriterien geprüft:

- GOOSE-Diskrepanz auf Senderseite: durch Prüfen der Control-Block-Einstellungen
- GOOSE-Publishing-Fehler: durch mitlesen der GOOSE am Netzwerk und Vergleichen mit der SCD
- GOOSE-Subskriptions-Fehler: durch Prüfen der LGOS-Zustände in allen IEDs.

Abb. 6 zeigt ein Beispiel, bei dem die von einem IED publizierte GOOSE im Netzwerk geprüft wird und StationScout aufgrund einer Diskrepanz in der Konfigurationsrevision ein Problem bei einem der Subscriber feststellt. Das Problem wird dargestellt, indem die entsprechende Verbindung gelb hervorgehoben wird und Warnsymbole angezeigt werden.

Abb. 6



Prüfung von GOOSE-Publisher-Subscriber-Verbindungen

3.4 Prüfen von Verriegelungslogiken

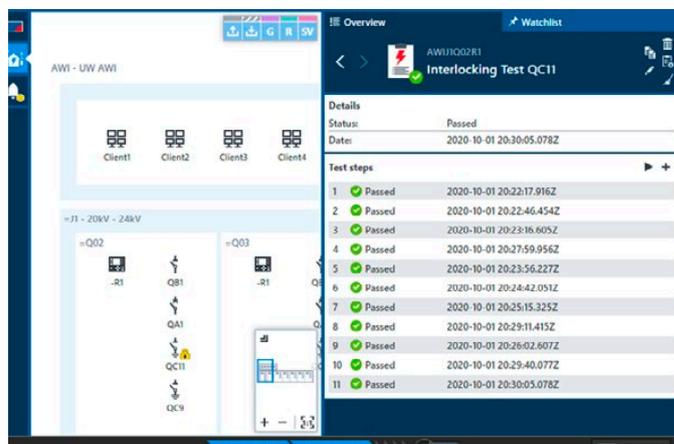
Die meisten IEDs enthalten Steuerungs- und Automatisierungsfunktionen in SPS-Logik. Sie können automatisch geprüft werden, indem die Eingänge der Logikfunktionen entweder über IED-Simulation oder mittels Hardware-Simulator simuliert und die Ergebnisse der Logikberechnungen mit StationScout ausgewertet werden. Ein Anwendungsbeispiel ist die Verwendung der Logiken für Verriegelungsschemas, um den ordnungsgemäßen Betrieb von Trenn- und Erdungsschaltern sicherzustellen. Zur Darstellung des Ergebnisses von Verriegelungslogikbedingungen definiert die IEC 61850 den Status der Freigabe im logischen Knoten „CILO“. Zu Prüfzwecken können einige oder idealerweise alle möglichen Eingabekombinationen vorgegeben werden, wobei zur Auswertung der Logik automatisch die CILO-Statuswerte eingelesen werden.

Abb. 7

Signal	Logics	IEC Reference / Step in Testcase	1	3	4	5	6	7	8	9	10	11
8811 No-Voltage		11Q00R1100/MVGPAC2.ind.sVal	TRUE	FALSE								
Q02-QB1 OPEN		11Q03R1CTRL/DCKSW1.Pos.sVal	OPEN	CLOSE								
Q03-QB1 OPEN		11Q03R1CTRL/DCKSW1.Pos.sVal	OPEN	CLOSE								
Q06-QB1 OPEN		11Q03R1CTRL/DCKSW1.Pos.sVal	OPEN	CLOSE								
Q10-QB1 OPEN		11Q03R1CTRL/DCKSW1.Pos.sVal	OPEN	CLOSE								
Q09-QB1 OPEN		11Q03R1CTRL/DCKSW1.Pos.sVal	OPEN	CLOSE								
Q07-QB1 OPEN		11Q03R1CTRL/DCKSW1.Pos.sVal	OPEN	CLOSE								
SG11 Enable Close		11Q03R1CTRL/ESCLO2.EnaCl.sVal	TRUE									

Prüfen von Verriegelungsschemas: Verriegelungslogiken und Definition von Prüfschritten in einer Kalkulationstabelle

Abb. 8

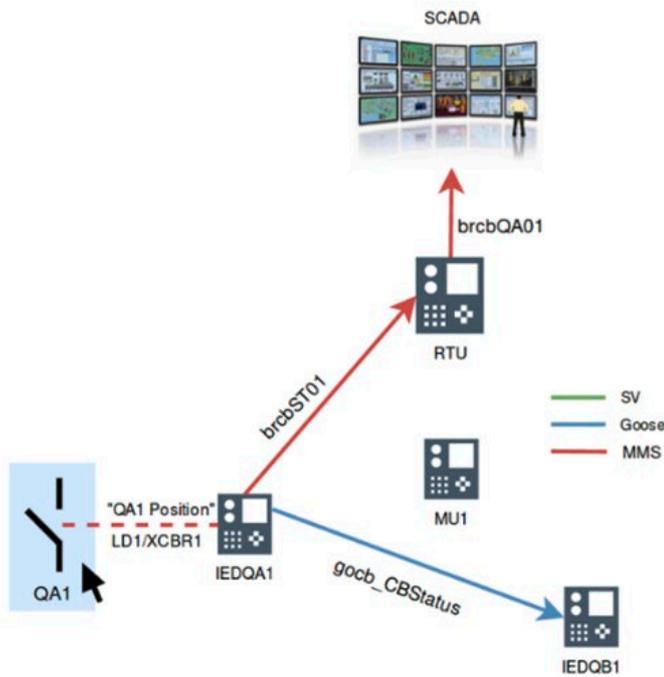


Ergebnisse der Verriegelungsprüfung nach Ausführung mit StationScout

3.5 Fehlersuche durch das Verfolgen von Signalen

In einem SAS finden viele Signalübertragungen zwischen den einzelnen Gräten statt. Ein Signal durchläuft mehrere Schritte, bis es in den jeweiligen Zielen z. B. in der Leitstelle eintrifft. Wenn bei dieser Kommunikation ein Fehler auftritt, muss der Inbetriebsetzer das Signal auf seinem Weg durch das SAS verfolgen. Das Aufspüren solcher Signalfehler kann recht zeitaufwendig sein. Mit StationScout lässt sich einfach verfolgen, wie sich die Signale durch das SAS ausbreiten.

Abb. 9



Übertragung der Position des Leistungsschalters innerhalb des SAS

3.6 Prüfen der Fernwirk-Gateway- und der lokalen HMI-Konfiguration

Fernwirk-Gateways und das lokale HMI kommunizieren normalerweise mit fast allen IEDs im System – hauptsächlich über sog. Reports, aber auch über GOOSE. In der Regel müssen pro Anlage mehrere tausend Signale geprüft werden. Bei der Inbetriebnahme werden zumindest die wichtigsten Signale über die gesamte Übertragungsstrecke hinweg geprüft, wobei das Signal in der Schaltanlage stimuliert wird. Alle anderen Signale können durch StationScout simuliert werden. Zur Beschleunigung der Prüfung bietet StationScout die Möglichkeit, einen Prüfplan zu erstellen, der die Simulation aller IEDs und Signale der Anlage vorsieht. So wird überprüft ob die Gateways korrekt konfiguriert sind.

Fernwirk-Gateways, HMIs und aber auch IEDs erhalten während ihrer Lebenszeit im Allgemeinen mehrere Firmwareaktualisierungen und Sicherheitspatches. Nach einer Aktualisierung können die Geräte ganz einfach neu geprüft werden („Sanity Check“), indem der für das betreffende Gerät bereits erstellte Prüfplan ausgeführt wird, bevor das Gerät wieder in Betrieb geht. Solche Prüfungen können in der Anlage stattfinden, wobei alle anderen IEDs durch StationScout simuliert werden, ohne dass die in Betrieb befindlichen Geräte beeinträchtigt werden.

4 Anwendungsfall aus der Praxis: Erweiterung einer vorhandenen Anlage

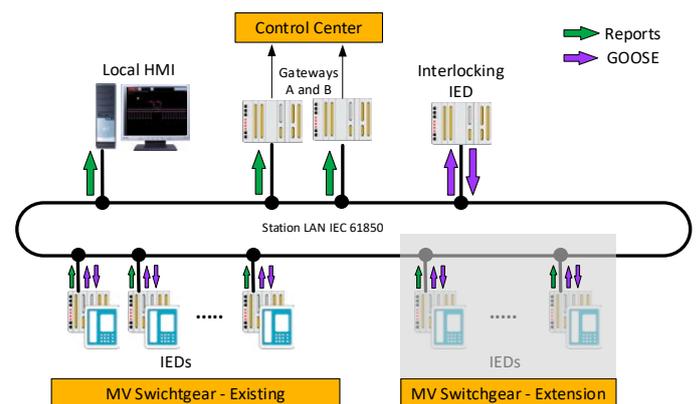
Der Betreiber einer wichtigen 20-kV-Innenraum-Anlage mit 3 Sammelschienen, 30 Abgängen und 2 Sammelschienenabschnitten in einem großen Industriekomplex entschied sich dazu, die vorhandene Anlage um mehrere Felder zu erweitern. Die Anlage wurde vor rund 10 Jahren

in Betrieb genommen und verfügt über ein modernes IEC-61850-konformes Schutz- und Leittechniksystem. Aufgrund der betrieblichen Gegebenheiten muss die Erweiterung ohne Netzunterbrechung und bei laufendem Betrieb der Anlage durchgeführt werden.

Die Befehlsverriegelungen sind mit SPS-Funktionen in den IEDs realisiert und der Austausch der relevanten Signale zwischen den IEDs erfolgt mittels GOOSE.

Die feldbezogenen Verriegelungen sind im jeweiligen Feldgerät implementiert. Außerdem berechnet ein spezielles Verriegelungs-IED in der Anlage die anlagenweiten Verriegelungen (Abb. 10). Zu diesem Zweck senden die Feldgeräte ihre Schalterpositionen und andere Informationen mittels GOOSE an das Verriegelungs-IED, welches die Topologieinformationen wie „Sammelschiene 1 geerdet“ berechnet und diese Informationen über GOOSE zurück an die Feldgeräte sendet, wo die endgültigen Befehlsfreigaben berechnet werden. Vorteil: Wenn das Zentralgerät ausfällt, bleiben die feldbezogenen Verriegelungen verfügbar. Und noch viel wichtiger: Erweiterungen der Anlage wirken sich nicht auf die vorhandenen Feld-IEDs aus!

Abb. 10



Prinzipielles Systemdiagramm der SAS

Eine solche Implementierung erlaubt nachfolgende Erweiterungen ohne eine erneute Prüfung der vorhandenen Felder und – bei Verwendung moderner Prüftools wie StationScout – auch während des laufenden Betriebs.

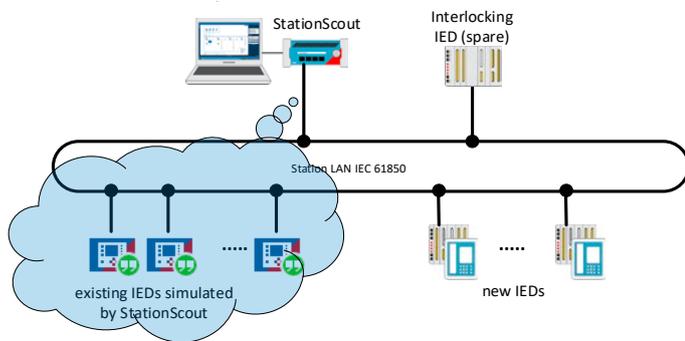
4.1 Prüfung der neuen IEDs im Werk

Da der Großteil der IEDs bereits in Betrieb ist, war es nicht möglich, die IEDs für die neuen Felder zusammen mit den vorhandenen IEDs und den Geräten auf Stationsebene im Werk zu prüfen. Der Betreiber entschied daher, die Prüfung der neuen IEDs mit einem Ersatz-Verriegelungs-IED durchzuführen und den Rest der Anlage durch StationScout simulieren zu lassen (Abb. 11).

Zunächst wurde die vorhandene SCD-Datei in eine neue Projektdatenbank importiert. Anschließend wurden die neuen IEDs hinzugefügt und das zentrale Verriege-

lungs-IED, die HMI und die Gateways wurden aktualisiert, damit die neuen Felder berücksichtigt werden. Zum Schluss wurde eine neue SCD-Datei der gesamten Anlage (vorhandene Anlage + Erweiterung) erstellt. Die vorhandenen Feldsteuerungs- und Schutz-IEDs blieben davon unberührt; sie erhalten keine neuen Parameter.

Abb. 11



Prüfaufbau für die Prüfung der neuen IEDs im Werk

Für jedes Öffnen bzw. Schließen des Trennschalters in den neuen Feldern wurden Prüffälle mit > 50 Prüfschritten als Permutationstabelle definiert (Abb. 7) und in StationScout implementiert. Die Prüffälle wurden nur einmal für ein typisches Feld erstellt und dann für die anderen Felder kopiert.

Zum Schluss wurden diese Prüfschritte ausgeführt, indem die vorhandenen IEDs simuliert und die relevanten CILO-Datenobjekte in den neuen IEDs ausgewertet wurden (Abb. 11). Auf diese Weise wurde die korrekte Implementierung des Verriegelungsschemas im zentralen Verriegelungs-IED und in die neuen Feld-IEDs verifiziert.

4.2 Prüfen der erneuerten Fernwirk-Gateways

Ein zweiter Teil des Erweiterungsprojekts erfordert aus IT-Sicherheitsgründen die Erneuerung der bestehenden Fernwirk-Gateways mit neuer Hardware und Firmware. Im Rahmen dieser Erneuerung war es notwendig, die ca. 2.000 Signale von den IEDs zur Leitstelle komplett neu zu prüfen.

Da die Anlage mit redundanten Gateways ausgestattet ist, kann jeweils eines der beiden Gateways vom Anlagen-LAN getrennt werden, ohne dass die Fernsteuerung durch die Leitstelle unterbrochen wird. Jedes Gateway wird einzeln erneuert und eine vollständige Signalprüfung durchgeführt, indem mit StationScout alle Signale simuliert und so die korrekte Funktion des Gateways bis zur Leitstelle prüft.

5 FAZIT

Im Artikel wurde ein innovativer Prüfansatz für das Prüfen eines Schaltanlagenautomatisierungssystem auf Grundlage der Informationen in der SCD-Datei vorgestellt. Es ist jetzt möglich, Prüfpläne zu erstellen, um die bisher sehr zeitaufwendigen Prüf- und Dokumentationsabläufe zu automatisieren. Automatisierte Prüfpläne ermöglichen auch schnelle Wiederholungsprüfungen nach dem Installieren der heutzutage recht häufigen Sicherheitspatches und Firmwareaktualisierungen. Das Prüfen wird damit zu einem integralen Bestandteil des Systems und unterstützt in Zukunft auch die permanente Funktionsüberwachung der Anlage im Betrieb.

Die Autoren



Christian Brauner, OMICRON electronics GmbH, Austria
Christian.Brauner@omicronenergy.com



Eugenio Carvalheira, OMICRON electronics Corp., USA
Eugenio.Carvalheira@omicronenergy.com

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