Verifizierung und Überwachung der Prozessbus-Kommunikation

Andreas Klien, Matthias Wehinger, Fred Steinhauser, OMICRON electronics GmbH, Österreich

Zusammenfassung

Mit zunehmender Nutzung nicht-konventioneller Messwandler werden gemäß IEC 61850-9-2 Sampled Values (SV) und GOOSE (Generic Object Oriented Substation Events) - Meldungen auch für die Kommunikation auf Prozessebene eingesetzt. Das Kommunikationsnetzwerk überträgt somit auch weitaus kritischere Informationen. Damit erhält die korrekte Funktion der Kommunikationsinfrastruktur des Prozessbusses eine systemkritische Bedeutung. Entsprechend zuverlässige Verfahren zur Überprüfung und Überwachung des korrekten Betriebs der Prozessbus-Kommunikation sind daher unbedingt erforderlich.

Dies beginnt schon während der Inbetriebnahme. Bereits in dieser Phase sind Konfigurationsfehler und Kommunikations-probleme auszuschließen sowie die korrekte Übertragung sämtlicher Signale sicherzustellen. Im laufenden Betrieb müssen in digitalisierten Anlagen auftretende Kommunikationsprobleme schnellstens erkannt werden, sodass das Bedienpersonal sofort entsprechend reagieren kann.

Dieser Artikel beschreibt zunächst, wie während der Inbetriebnahme die Konfiguration für die Prozessbus-Kommunikation gemäß IEC 61850 mit der sogenannten Substation Configuration Description (SCD) abgeglichen werden kann. Dies gewährleistet die korrekte Konfiguration für SVs und GOOSE-Nachrichten. Darüber hinaus stellt es sicher, dass alle IEDs gemäß ihrer Definition in der SCD per Client/Server-Kommunikation erreichbar sind. Anschließend wird gezeigt, wie sich die Prozessbus-Kommunikation permanent überwachen lässt, um beispielsweise Probleme durch verlorene Samples, mit dem GOOSE-Timing oder bei der Synchronisierung via PTP aufzudecken. Den Abschluss des Artikels bilden Einstellbeispiele für die Netzwerküberwachung in redundanten Netzwerkstrukturen, die mit Redundanzprotokollen wie RSTP, HSR oder PRP arbeiten.

Prüfung der IEC 61850-Kommunikation während der Inbetriebnahme

In Anlagen, die gemäß IEC 61850 kommunizieren, lassen sich das Kommunikationssystem und die dort integrierten IEDs mit Hilfe der standardisierten Substation Configuration Language (SCL) [1] beschreiben. Die SCL kann dabei bereits in der Spezifikationsphase verwendet werden, um die Anforderungen für das Projekt in SSD-Dateien (Substation Specification Description) festzulegen. Nach der Realisierung des Projektes ist die tatsächliche Implementierung des Systems in der SCD-Datei (Substation Configuration Description) beschrieben. Bei Werksabnahmeprüfungen (FAT) und am Betriebsort (SAT) lässt sich anhand der SCD-Datei verifizieren, ob alle IEDs korrekt kommunizieren. Hierzu kann die tatsächlich auf der Leitung stattfindende Kommunikation mit den Daten der SCD-Datei verglichen werden.

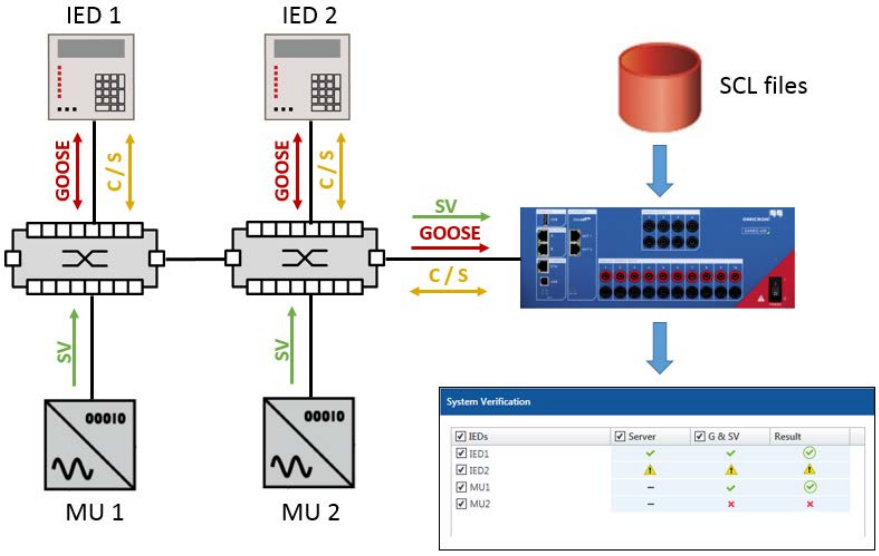

Bild 1: Aufbau zur Überprüfung der IEC 61850-Kommunikation

Bei der Inbetriebnahme von IEC 61850-Systemen treten häufig Kommunikations- und Kompatibilitätsprobleme auf, da manche Kommunikationsparameter im sendenden Gerät anders konfiguriert sind als im empfangenden Gerät. Dies kann beispielsweise vorkommen, wenn die Konfiguration des sendenden Gerätes geändert wird, nachdem das empfangende Gerät bereits in Betrieb genommen wurde. Um in einem solchen Fall die Fehlerursache zu finden, müssten sämtliche Konfigurationsparameter des sendenden und des empfangenden Gerätes miteinander verglichen werden, um vorhandene Unterschiede aufzuspüren. Mit dem nachfolgend beschriebenen Aufbau zur System-Verifikation können solche Unterschiede mit erheblich geringerem Aufwand gefunden werden.

Bild 1**Error! Reference source not found.** zeigt einen Aufbau zur Überprüfung der Kommunikation für ein kleines Beispielsystem, bestehend aus Merging Units (MU) und Schutz-IEDs. Die Prüfung erfolgt mit einem Netzwerkanalysators mit Verifizierungsfunktion [7]. In diesem Aufbau kann die komplette Kommunikation der GOOSE-Nachrichten [3] und IEC 61850-9-2 [4] SVs in einem einzigen Schritt mit der Beschreibung in der SCD-Datei verglichen werden. Dadurch lässt sich erkennen, ob Kommunikationsparameter nicht mit der Konfiguration übereinstimmen oder ob die in der SCD-Datei beschrieben GOOSE-Meldungen oder SVs fehlen. Bietet das IED auch Server-Funktionalität gemäß IEC 61850, wird zudem geprüft, ob der Server für die Client/Server-Kommunikation verfügbar ist. Um sicherzustellen, dass der richtige Server erreicht wurde, werden auch die logischen Ge-

Defined		Found	
AM174KBX/LLN0GOGCB		AM174KBX/LLN0GOGCB	
Details		Details	
Control block reference	AM174KBX/LLN0GOGCB	Control block reference	AM174KBX/LLN0GOGCB
Destination MAC address	01-0C-CD-01-00-00	Destination MAC address	01-0C-CD-01-00-00
Application ID	2 (0x0002)	Application ID	⚠ 1 (0x0001)
GOOSE ID	GoID1	GOOSE ID	⚠ GoID
DataSet reference	AM174KBX/LLN0$GooseDataSet1	DataSet reference	AM174KBX/LLN0$GooseDataSet1
VLAN ID	1	VLAN ID	not present
VLAN priority	4	VLAN priority	not present
Needs commissioning	False	Needs commissioning	False
Configuration revision	2	Configuration revision	⚠ 1

Bild 2: Unterschiede zwischen der GOOSE-Definition in der SCD-Datei (links) und der GOOSE-Nachricht im Netzwerk (rechts)

rätenamen (Logical Device names) des erreichten Servers mit den in der SCD-Datei beschriebenen verglichen. Das in Bild 1 dargestellte Ergebnis der Überprüfung zeigt, dass für IED 1 die IEC 61850-Kommunikation korrekt ist, während es bei der GOOSE- und Client/Server-Kommunikation von IED 2 zu Problemen kommt. Für MU 2 konnte überhaupt keine SV-Kommunikation gefunden werden. Dies kann entweder an Fehlern in der Netzwerkkonfiguration liegen oder daran, dass MU2 noch nicht in Betrieb genommen wurde.

Error! Reference source not found. 2 zeigt das Resultat der Überprüfung für eine GOOSE-Nachricht, die sich anders als definiert verhielt. Der linke Teil zeigt die in der SCD-Datei festgelegten GOOSE-Parameter, der rechte Teil die im Netzwerk vorgefundenen GOOSE-Parameter. Die GOOSE-Nachricht weist abweichende Werte für Applikations-ID, GOOSE ID und die Revision für die Konfiguration auf. Aufgrund der abweichenden GOOSE ID und Applikations-ID wurde diese GOOSE-Nachricht von den subskribierenden IEDs nicht empfangen. Man erkennt, dass das sendende Gerät offenbar mit einer älteren Revision der SCD-Datei konfiguriert worden sein muss, da die Revisionsnummer der Konfiguration niedriger ist. Eine unterschiedliche Konfigurationsrevision kann abhängig von der Implementierung des IEDs dazu führen, dass die empfangenden Geräte die GOOSE-Daten nicht akzeptieren. Damit die Kommunikation reibungslos funktioniert, ist also die Konfiguration des sendenden Gerätes so zu korrigieren, dass diese mit der SCD übereinstimmt.

Überwachung der Prozessbus-Kommunikation während des Betriebs

Nach der Inbetriebnahme sind Konfigurationsfehler ausgeschlossen und sämtliche Anwendungen des PAC-Systems (Protection, Automation & Control) getestet. Auch die zugrunde liegende Netzwerk-Infrastruktur ist verifiziert. Für einen korrekten Betrieb des PAC-Systems sind die einzelnen Anwendungen des Systems auf die korrekte Funktion der zugrunde liegenden Netzwerk-Infrastruktur angewiesen. So erfordern beispielsweise Schutzfunktionen den rechtzeitigen Eingang der SVs und eine verfügbare Zeitsynchronisation. Wird das Zeitsynchronisationsprotokoll PTP [6] gemäß IEEE 1588 verwendet, so ist auch die Zeitsynchronisation von der Netzwerk-Infrastruktur abhängig. Wie aber können während des Betriebs auftretende Fehlfunktionen in der Infrastruktur des Kommunikationsnetzwerks oder anderer wichtiger Dienste rund um die Uhr erkannt werden? Hierfür gibt es im Wesentlichen zwei Varianten: Eine Möglichkeit ist die separate Überwachung sämtlicher IEDs oder PAC-Anwendungen. Solche Funktionen werden in letzter Zeit zunehmend von den Anbietern implementiert. Die andere (ergänzende) Möglichkeit ist die Überwachung kritischer Dienste direkt am Prozessbus, also im Netzwerk, wo alle Dienste sichtbar sind. Nachfolgend werden wir uns auf die netzwerkbasierte Überwachung konzentrieren.

Bild 3 zeigt einen Aufbau, bei dem ein Netzwerkanalysator an eine zentrale Kommunikationsverbindung angeschlossen ist, um die

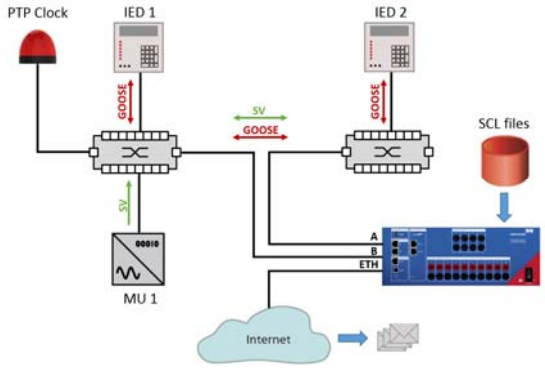

Bild 3: Aufbau zur Überwachung der Prozessbus-Kommunikation

GOOSE- und SV-Kommunikation permanent überwachen zu können Die Überwachung greift den Netzwerkverkehr auf der Ethernet-Verbindung passiv ab, ohne die Kommunikation auf dieser Verbindung zu stören. Bei diesem Aufbau ist es nicht erforderlich, Port-Spiegelungen an den Ethernet-Switches zu konfigurieren.

Das Prüfgerät kann mit der SCL-Datei der Anlage konfiguriert werden. Es erkennt Abnormitäten im GOOSE- und SV-Verkehr und protokolliert diese mit entsprechenden Detailinformationen (Event-Details, erfasster Netzwerkverkehr) in seinem Speicher. Je nachdem,

wie kritisch das jeweilige Ereignis ist, muss eventuell neben der Aufzeichnung auch das zuständige Bedienpersonal benachrichtigt werden. Bei dem in Bild 3 gezeigten Aufbau erfolgt die Benachrichtigung des Bedienpersonals per E-Mail. Eine weitere Möglichkeit zur Signalisierung von Ereignissen ist das Umschalten eines Binärausgangs am Netzwerkanalysator. Dieses Signal kann dann via SCADA zur Leitstelle übertragen werden.

Für SV ist es hilfreich, das Verlorengehen einzelner Abtastwerte (Meldungen) zu erkennen. Das Prüfgerät erkennt dies durch Kontrolle des Sample Counts in den SV-Meldungen. Einzelne derartige Ereignisse können zwar toleriert werden, allerdings ist solch ein Verlust in modernen Ethernet-Netzwerken sehr ungewöhnlich und sollte weiter untersucht werden. Wenn länger als 4 Millisekunden keine SVs empfangen werden, tritt eine Zeitüberschreitung des SV-Datenstroms auf. Dies ist ein kritisches Ereignis und erfordert eine sofortige Reaktion. Durch Auswerten der Zeitstempel in den SV-Meldungen lässt sich außerdem erkennen, ob der Takt des Gerätes, das die SVs sendet, eine zu große Abweichung aufweist. Ist das Prüfgerät mit einer PTP-Zeitquelle synchronisiert, können auch Fehlfunktionen in der PTP-Zeitsynchronisation angezeigt werden.

Zeitüberschreitungen von GOOSE-Meldungen lassen sich erkennen, indem man die Einträge im Feld für deren Gültigkeitsdauer im Netzwerk überprüft. Zeitüberschreitungen von GOOSE-Meldungen werden entweder durch Kommunikationsausfälle (z.B. aufgrund eines fehlerhaften Netzwerkkabels) oder durch Störungen des sendenden IED verursacht. Durch Überwachen der Sequenznummern (sqNum) der Meldungen sind fehlende Neuübertragungen von GOOSE-Meldungen erkennbar.

Ein weiteres kritisches Ereignis ist, wenn zwei Geräte im Netzwerk dieselbe GOOSE-Nachricht senden. Dies kann beispielsweise vorkommen, wenn jemand versehentlich mit einem Prüftool dieselbe GOOSE-Nachricht generiert und vergessen hat, das Simulation/Test-Flag dieser GOOSE-Nachricht einzuschalten. Solche Situationen erkennt der Prüfer auch durch Kontrollieren der Status- und der Sequenznummern. Bild 4 zeigt eine solche Situation: Die originale GOOSE wird mit einer um 1 aufsteigenden sqNum für jedes einzelne Paket gesendet. Bei Eintreffen des GOOSE-Duplikats springt die sqNum jedoch wieder auf 0. Werden also im selben Netzwerk zwei identische GOOSE-Nachrichten versendet, so erkennt das Prüfgerät mehrere "Falsche Reihenfolge"-Ereignisse. Außerdem weicht unter normalen Umständen im Duplikat der GOOSE nicht nur die sqNum ab, sondern auch die Statusnummer (stNum).

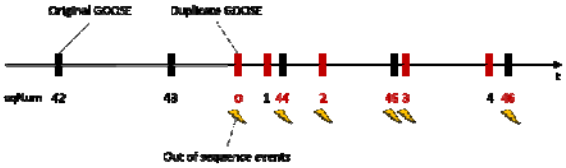

Bild 4: "Falsche Reihenfolge" durch ein GOOSE-Duplikat

Bild 5 zeigt eine Liste der vom Prüfgerät erfassten Ereignisse. Bei dem in der Abbildung ausgewählten Ereignis hat das Prüfgerät erkannt, dass die Gültigkeitsdauer einer GOOSE-Meldung aufgrund eines Kommunikationsausfalls abgelaufen ist. Eine Minute später trat die GOOSE-Nachricht erneut auf. Da zwischen den Sequenznummern der GOOSE-Nachrichten eine Lücke bestand, wurde ein "Falsche Reihenfolge"-Ereignis aufgezeichnet. Die Detailinformation zu diesem Ereignis zeigte, wie viele GOOSE-Neuübertragungen fehl-

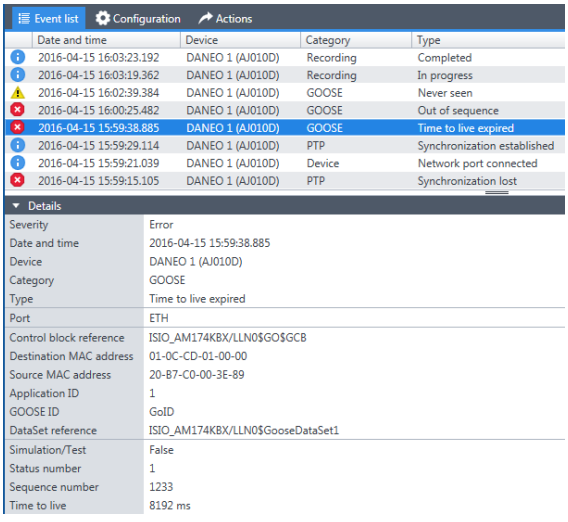

Bild 5: Prüf-Ereignisliste mit Detailinformationen zur Zeitüberschreitung von GOOSE

ten. Außerdem wurde protokolliert, ob während des Kommunikationsausfalls Statusänderungen (Änderung von stNum) der GOOSE-Meldung auftraten. Ein weiterer Eintrag zeigt, dass eine in der SCD-Datei festgelegte GOOSE-Nachricht während der Überwachung im Netzwerk tatsächlich "niemals gesehen" wurde. Dies wird manchmal durch GOOSE-Meldungen verursacht, die nur für die Inbetriebnahme verwendet wurden und nach Beendigung der Inbetriebnahme eigentlich aus der SCD-Datei hätten entfernt werden sollen.

Überwachung in RSTP-Netzwerken

Für Anlagennetzwerke werden häufig Ringstrukturen mit dem Rapid Spanning Tree Protocol (RSTP) verwendet. Hierbei sind die Netzwerk-Switches so miteinander verbunden, dass diese einen Ring bilden und jeder Switch von zwei Richtungen aus erreichbar ist. Manche Schutzrelais und Feldsteuerungen besitzen Ethernet-Switches mit zwei Ports und können daher direkt in solche Ringstrukturen integriert werden, was die zum Aufbau von solchen Netzwerken erforderliche Anzahl von Ethernet-Switches reduziert. Die Verwendung von RSTP gewährleistet, dass keine geschlossenen Schleifen für die Pakete entstehen können, d.h. der Ring ist durch Deaktivieren von redundanten Verbindungen immer geöffnet. In dem in Bild 6 gezeigten Aufbau wird eine der Verbindungen L1, L2 oder L3 als redundante Verbindung gesehen und durch RSTP deaktiviert werden.

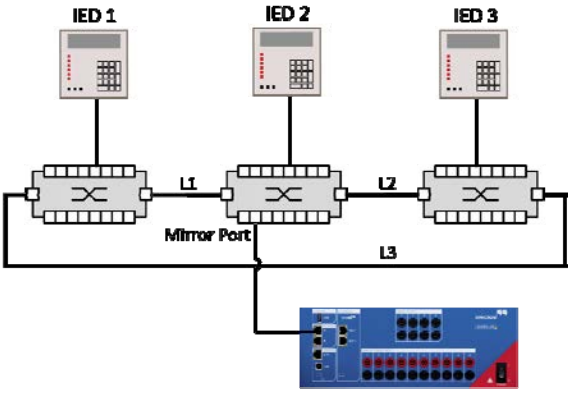

Abbildung 6: Aufbau für die Überwachung in RSTP-Netzwerken

Fällt eine der Verbindungen aus, konfiguriert das RSTP-Protokoll die Pfade neu und reaktiviert eine der zuvor deaktivierten Verbindungen, um die Kommunikation wieder herzustellen. Allerdings wird während der Neukonfiguration die Kommunikation unterbrochen und Pakete, die Ihr Ziel nicht erreichen konnten, werden fallengelassen. Abhängig von den Gegebenheiten kann bei RSTP eine solche Neukonfiguration bis zu einigen Sekunden dauern. Für die Prozessbus-Kommunikation (wie SVs und GOOSE-Nachrichten) sind derart lange Kommunikationsausfälle jedoch normalerweise nicht tolerierbar. Aus diesem Grund wird für Prozessbus-Netzwerke die Verwendung der Redundanzmechanismen HSR (High-availability Seamless Redundancy) und PRP (Parallel Redundancy Protocol) gemäß IEC 62439-3 [2] empfohlen [5]. Diese Protokolle werden im nachfolgenden Abschnitt behandelt.

Bei der Analyse oder Überwachung des Netzwerkverkehrs in RSTP-Netzwerken ist zu berücksichtigen, dass immer eine der Verbindungen deaktiviert ist. Wird der Netzwerkanalysator wie zuvor in Bild 3 beschrieben angeschlossen (also als Abgriff an einer der Kommunikationsverbindungen), kann es vorkommen, dass genau diese Verbindung von RSTP gerade nicht verwendet wird. Der Netzwerkanalysator kann dann keinen Netzwerkverkehr erkennen. Wird der Netzwerkanalysator hingegen mittels eines Mirror-Ports an den Switch angeschlossen (siehe Bild 6), ist immer der gesamte SV- und GOOSE-Verkehr sichtbar, selbst wenn eine der Verbindungen L1, L2 oder L3 deaktiviert ist. Der Grund hierfür ist, dass es sich bei SVs und GOOSE-Nachrichten um Multicast-Verkehr handelt, der an allen Ports des Switches ausgesendet wird. Punkt-zu-Punkt-Verkehr, wie der IEC 61850 Client/Server-Verkehr, ist dagegen für den Analysator in Bild 6 nicht immer sichtbar. Dies ist abhängig von den beteiligten Kommunikationspartnern. Beispielsweise ist hier der Verkehr für den Netzwerkanalysator nicht sichtbar, wenn Verbindung L1 deaktiviert ist und IED 1 versucht, via Client/Server-Kommunikation mit IED 2 zu kommunizieren. In diesem Fall läuft die Punkt-zu-Punkt-Verbindung über Verbindung L3.

Überwachung in HSR-Netzwerken

HSR-Netzwerke [2] werden für Schutz- und Stationsautomatisierungsnetzwerke verwendet, die im Fehlerfall eine Redundanz mit einer Wiederbereitschaftszeit von null benötigen. HSR erfordert eine Ringstruktur des Netzwerkes. Jeder Knoten dieses Rings ist durch zwei Ethernet-Ports angebunden. Auf beiden Ports wird derselbe Ethernet-Frame gesendet. Der Ethernet-Frame wandert daher in beiden Richtungen durch den Ring. Der Empfänger erhält somit aus beiden Richtungen identische Frames. Der erste Frame wird verwendet, der zweite Frame verworfen. Multicast-Meldungen werden solange an jeden Knoten im Ring weitergeleitet, bis beide Frames wieder beim sendenden Gerät ankommen. Das Löschen von Unicast-Meldungen erfolgt am Ziel.

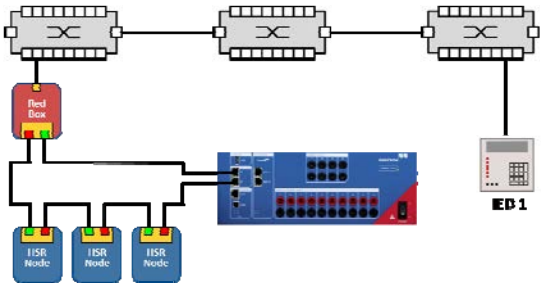

Bild 7: Aufbau für die Überwachung in einem HSR-Netzwerk

Bild 7 zeigt einen exemplarischen Aufbau mit einem HSR-Ring, welcher mit einem normalen Ethernet-Netzwerk verbunden ist. Die Integration des Ethernet-Netzwerkes in das HSR-Netzwerk erfolgt durch eine Redundanz-Box (Red Box). Der Netzwerkanalysator ist als Abgriff in den HSR-Ring geschaltet. Bei diesem Aufbau ist der gesamte Verkehr im HSR-Ring für das Prüfgerät sichtbar. Da es sich bei SVs und GOOSE-Nachrichten um Multicast-Verkehr handelt, empfängt das Prüfgerät sämtliche Meldungen aus beiden Richtungen und die SV- und GOOSE-Meldungen können separat für beide Richtungen überwacht werden. Dadurch werden Verbindungsstörungen im HSR-Ring erkannt, da diese zu Zeitüberschreitungen für die SV- und GOOSE-Meldungen führen. Der Analysator empfängt außerdem die SV- und GOOSE-Meldungen von IED 1, da die Multicast-Meldungen in das HSR-Netzwerk weitergeleitet werden.

Überwachung in PRP-Netzwerken

PRP (Parallel Redundancy Protocol) verwendet zwei unabhängige Ethernet-Netzwerke. Redundanz wird dadurch erreicht, dass die Geräte mit beiden Netzwerken verbunden sind. Jedes Paket wird über beide Pfade gesendet und demzufolge am Ziel zwei Mal empfangen. In PRP-Netzwerken sind die Netzwerkpakete am Ende des Frames durch den Redundancy Control Trailer markiert. Der Empfänger muss eines der doppelt vorhandenen Pakete entfernen. Dies kann in einer Red Box erfolgen. Im Gegensatz zu HSR erfordert PRP für den Zugriff auf das Netzwerk keine spezielle Hardware. Daher könnte die Red Box-Funktionalität von PRP auch per Software in IEDs mit zwei Ethernet-Ports realisiert werden.

Ein möglicher Aufbau für die Überwachung der Kommunikation in PRP-Netzwerken ist in Bild 8 gezeigt. Bei diesem Aufbau empfängt der Netzwerkanalysator den gesamten Verkehr, da dieser in beiden Netzwerkpfaden identisch ist. Alternativ lassen isch auch beide Pfade überwachen, entweder durch nur ein Prüfgerät, das mittels Mirror-Ports an beide Netzwerke angeschlossen ist, oder durch Einsatz zweier Prüfgeräte, welche für den Abgriff mit den Kommunikationsverbindungen beider Pfade verbunden sind. Dies ermöglicht eine unabhängige Erkennung von Zeitüberschreitungen für SVs und GOOSE-Nachrichten

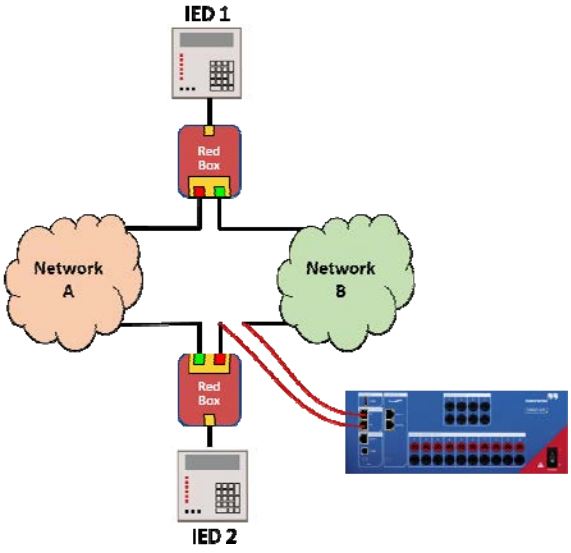

Bild 8: Aufbau für die Überwachung in einem PRP-Netzwerk mit einem Prüfgerät

in beiden Netzwerkpfaden. Wie bereits zuvor für den HSR-Aufbau beschrieben, kann dies zur Erkennung von Verbindungsstörungen verwendet werden, da in einem der beiden redundanten Netzwerke Zeitüberschreitungen für SVs und GOOSE-Nachrichten auftreten.

Fazit

Der Einsatz von IEC 61850-Kommunikation in PAC-Systemen birgt neue Herausforderungen. Allerdings können die hieraus erwachsenden Vorteile und neuen Möglichkeiten diese Schwierigkeiten bei Weitem überwiegen.

Das Entwicklungskonzept und die daraus resultierende Verfügbarkeit der Konfigurationsdaten in maschinenlesbarer Form (als SCL-Dateien) bieten wesentliche Verbesserungen für die Prüfbarkeit der Systeme. Die im ersten Teil dieser Arbeit dargelegte Verifizierung der Kommunikation in der Anwendungsschicht wird durch diese Funktionen ganz erheblich erleichtert. Dies gilt für den gesamten Lebenszyklus von PAC-Systemen. So können Konfigurationen und Prüfaufbauten, die ursprünglich für die Werksabnahmeprüfung erarbeitet wurden, auch für die Inbetriebnahme wieder verwendet werden. Zwischenzeitlich eventuell vorgenommene Konfigurationsänderungen lassen sich sofort erkennen und können entsprechend bereinigt werden. Wenn sich die Konfiguration nicht geändert hat, ist dies verifiziert und kann somit noch schneller abgehakt werden. Die Konfigurationsdaten erfüllen außerdem bei der Überwachung während des Betriebs oder bei späteren Wartungsarbeiten Ihren Zweck.

Bedenkt man, dass Skeptiker die Performance und Zuverlässigkeit der Kommunikationsnetzwerke häufig in Frage stellen, ist es eigentlich überraschend, dass bisher nur so geringe Anstrengungen unternommen wurden, um diese wichtigen Aspekte zu verifizieren und zu überwachen. Die Inbetriebnahme der Kommunikationsinfrastruktur sollte für sich alleine eine eigenständige Tätigkeit werden, um eine solide Grundlage für die darauf aufgesetzte Kommunikation von PAC-Systemen sicherstellen zu können. Mit hochmodernen Tools können solche Aufgaben auch von auf die Schutz-, Automatisierungs- und Steuerungstechnik spezialisierten Energietechnik-Ingenieuren einfach durchgeführt werden.

Referenzen

[1] IEC. *Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs (IEC 61850-6, Ed. 2.0)*. International Electrotechnical Commission, Dez. 2009.

[2] IEC. *Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) (IEC 62439-3),* Feb. 2010.

[3] IEC. *Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3 (IEC 61850-8-1, Ed. 2.0).* International Electrotechnical Commission, Juni 2011.

[4] IEC. *Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3 (IEC 61850-9-2, Ed. 2.0).* International Electrotechnical Commission, Sept. 2011.

[5] IEC. *Communication Networks and Systems for Power Utility Automation. Part 90-4: Network Engineering Guidelines (IEC Technical Report 61850-90-4).* International Electrotechnical Commission, 2012

[6] IEEE Power & Energy Society. *IEEE Standard Profile for use of IEEE 1588 Precision Time Protocol in Power System* Applications (IEEE C37.238-2011). Institute of Electrical and Electronics Engineers, Inc., 2011.

[7] M. Wehinger und F. Steinhauser. *Verification and Supervision of Communication Networks for Utility Automation*. PAC World Magazine, Ausgabe Juni 2016, Seiten 54–59, 2016

Autoren:

Andreas Klien wurde 1986 in Österreich geboren. Er studierte Computer Engineering an der Technischen Universität Wien und arbeitet seit 2005 bei OMICRON. Dort leitet er aktuell ein Entwicklungsteam für Produkte rund um IEC 61850. Als Mitglied der Working Group 10 im Technical Committee TC 57 der IEC, arbeitet er an der Weiterentwicklung der Normenserie IEC 61850 mit.

andreas.klien@omicronenergy.com

Matthias Wehinger studierte Computerwissenschaften an der Hochschule Konstanz Technik, Wirtschaft und Gestaltung. An der Fachhochschule Vorarlberg erwarb er den Master of Science im Bereich Integrierte Produktentwicklung. Seit 2003 arbeitet er bei OMICRON. Er begann dort in der Produktentwicklung für Prüfwerkzeuge und war an der Einführung neuer Technologien für die Modellierung von Prüfobjekten beteiligt.

2014 übernahm er dort die Aufgabe des Innovationsmanagers für Produkte im Bereich der Kraftwerkskommunikation.

matthias.wehinger@omicronenergy.com

Dr. Fred Steinhauser studierte Elektrotechnik an der Technischen Universität Wien, wo er 1986 sein Diplom machte. 1991 promovierte er zum Doktor der Technischen Wissenschaften. Er ist seit 1998 bei OMICRON und arbeitete zunächst an diversen Themen bezüglich der Schutzprüfung von Energiesystemen. Von 2000 bis 2014 arbeitet er als Produktmanager mit dem Schwerpunkt auf der Kommunikation in Schaltanlagen. Seit 2014 leitet er den Bereich Kraftwerkskommunikation bei OMICRON.

Fred Steinhauser repräsentiert OMICRON in der UCA International Users Group. Als Mitglied der WG10 und WG17 im TC57 der IEC arbeitet er an dem Standard IEC 61850 mit. Außerdem ist er Mitglied des SC B5 des CIGRÉ.

fred.steinhauser@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 140 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