Übertragung von Differentialschutzdaten über paketorientierte IP-Netzwerke

Norbert Schuster, Siemens / Michael Simon, Cisco / Stefan Steger, TenneT TSO

Motivation für den Einsatz paketorientierter IP-Netzwerke

Ethernet basierte Datentransportnetzwerke werden zukünftig immer mehr im EVU-Bereich und in der Industrie eingesetzt. Sie lösen die bisherigen SDH-Netze ab, die nicht mehr signifikant weiterentwickelt werden. Im Weitverkehrsbereich dieser Datennetze wird oft die MPLS-Technologie verwendet, wobei spezielle Router die Aufgabe der Erfassung, Verdichtung und Verteilung der Daten übernehmen. Diese Daten werden dann gebündelt über Lichtwellenleiter zwischen Standorten übertragen werden. MPLS-Netzwerke können beliebige Daten transportieren, wie z.B. Sprachdaten und traditionelle serielle Daten. Ein besonderes Merkmal ist der Quality of Service (QoS), mit dem man gewisse Datenpakete hoch priorisiert übertragen kann. Neben zeitunkritischen Daten, wie z.B. Messwerten, sollen diese Netze damit auch extrem zeitkritische Daten der Schutzdaten-übertragung wie dem Signalvergleich oder die Differentialschutzdaten übertragen, die dann den QoS verwenden. Dazu lassen sich sogenannte Pseudo Wire Verbindungen schalten, die mit hoher Priorität und in Echtzeit diese kritischen Daten speziell behandeln und schnell von A nach B übertragen. Diese Punkt-zu-Punkt Verbindungen im IP-Netzwerk müssen hinsichtlich ihrer Eignung für diesen zeitkritischen Datenverkehr überprüft werden. Dazu wurde das Pilotprojekt durchgeführt. Ziel ist es existierende Differential-Schutzgeräte zusammen mit der neuen Übertragungs-Technologie einzusetzen und die Eignung dieser Netzwerke nachzuweisen.

Zeitkritische Differentialschutzanwendung

Der Differentialschutz stellt hohe Anforderungen an die Übertragung. Idealerweise werden diese durch direkte Lichtwellenleiter Verbindungen erzielt, die aber exklusiv für den Differentialschutz in vielen Fällen nicht zur Verfügung stehen. Stattdessen werden die Daten über hoch priorisierte Verbindungen oder Standleitungen über Kommunikationsnetze übertragen. Folgende Anforderungen hat TenneT für die Übertragung definiert:

Die maximale Laufzeit der Daten auf einer Verbindung soll kleiner 5 ms sein. Eine lange Laufzeit verlängert die Auslösezeit des Schutzes und addiert sich bei Mehrenden Konfigurationen um die Laufzeit jeder Strecke.

Die Daten müssen mit einer gewissen Periodizität vom Schutzgerät empfangen werden. Der Jitter zwischen empfangenen Telegrammen soll ± 300 µs nicht übersteigen. Ansonsten meldet der Differentialschutz Laufzeitsprünge, erhöht die Stabilisierung und wird unempfindlicher.

Die Laufzeit die gesendeten und empfangenen Telegramme sollte nahezu gleich sein. Ungleiche Laufzeit erzeugt einen Differentialstrom und erfordert damit eine unempfindlichere Einstellung des Schutzes.

TenneT lässt max. 500 km Lichtwellenleiterlänge und bis zu 15 Router zu, über die der Datenverkehr laufen kann. Die Laufzeitanforderung von max. 5 ms auf einer Schutzstrecke ist dabei einzuhalten.

Versuchsaufbau

Für den Versuch wurde im Prüfraum der TenneT in Bayreuth ein Kommunikationsnetz von Cisco mit 6 Routern aufgebaut. Tennet hat die Serien Geräte ASR901 und ASR903 ausgesucht, die mit unterschiedlichen Schnittstellen angeboten werden (u.a. E1-Schnittstellen). Zwischen den Knoten / Routern sind 1 Gbit Verbindungen mit Lichtwellenleiter realisiert. Mit Dämpfungsgliedern werden lange LWL-Strecken zwischen den Routern nachgebildet, die Schaltanlage 1 und Schaltanlage 2 verbinden. Physikalisch befindet sich das Netzwerk in einem Raum.

Schutztechnisch ist eine Vierbein-Topologie realisiert. Die Differentialschutzgeräte 7SD52 – die von TenneT seit Jahren im HöS-Netz eingesetzt werden – haben je zwei Wirkschnittstellen und topologisch wird über das Kommunikationsnetz ein Ringbetrieb angestrebt. Der Anschluss an die Router erfolgt über Kommunikationsumsetzer, die über 820 nm Multimodefaser mit den optischen Wirkschnittstellen der Schutzgeräte verbunden sind. Zwischen Kommunikationsumsetzern und Schutz wird ein siemensspezifisches serielles HDLC-Protokoll verwendet, das die Daten über gesicherte Telegramme überträgt. Die Umsetzer #1a und #3a setzen auf eine 2 Mbit/s E1 Schnittstelle um, die als Interface im Router zur Verfügung steht. Es handelt sich um Seriengeräte, die TenneT auch schon seit Jahren für die Anbindung des Schutzes an SDH-Netze einsetzt. Die anderen Umsetzer sind Prototypen, die den seriellen HDLC-Datenstrom auf optische 1300 nm

100 Mbit/s Ethernetschnittstellen konvertieren und damit direkt über Ethernet die Daten in die Router einspeisen. In diesen Umsetzern sind spezielle Eigenschaften implementiert, die ein optimales Einkoppeln der Daten in das Ethernetnetzwerk ermöglicht.

Alle Geräte sind über einen SNTP-Server auf 1 ms synchronisiert, der sich im Kommunikationsnetzwerk befindet und die Zeitbasis für die Betriebs- und Störfallmeldungen in den Schutzgeräten bildet. Der Differentialschutz ist autark und synchronisiert sich selbst über die Kommunikationsverbindungen. Alle Geräte können über Ethernet von einem zentralen Bedien-PC abgefragt werden. Dazu wird über das Kommunikationsnetz ein Servicekanal bereitgestellt. Auch eine Fernabfrage über eine DSL-Verbindung wurde installiert, um z.B. von Berlin aus die Geräte im Dauerbetrieb zu überwachen. Auch das Kommunikationsnetz wird fernüberwacht.

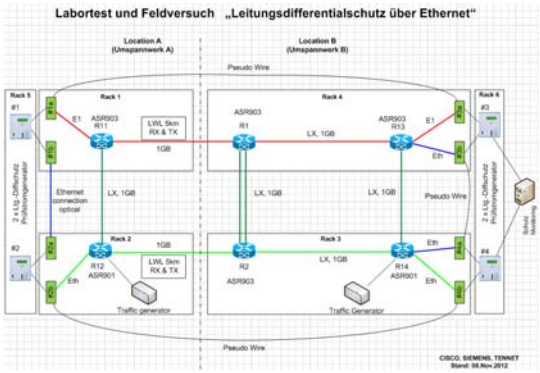


Bild 1 Versuchsaufbau

Einstellung der Schutzgeräte

Das Differentialschutzsystem ist auf eine Vierbein Topologie parametriert. Eine Ringtopologie wird an allen Geräten durch eine LED signalisiert. Der Ansprechwert des Differentialschutzes beträgt 20 % von Nennstrom und ist bewusst empfindlich eingestellt, um bei unerwünschten Effekten im Kommunikationsnetz wie unterschiedlicher Laufzeit in Hin- und Rückrichtung eine Überfunktion unter Last zu provozieren.

Auf die LED und Betriebsmeldepuffer sind hauptsächlich die Überwachungsmeldungen der Kommunikation rangiert, die z.B. einen Sprung in der Laufzeit melden oder die Störung oder Ausfall auf den Strecken. Auch die Laufzeit wird durch die Geräte kontinuierlich gemessen und überwacht. Ferner wird fortwährend gemessen, ob es zu Störungen bei empfangenen Telegrammen kommt.

Einstellung der Router

Drei Schutzverbindungen werden über das geroutete Netzwerk geführt (R11 <-> R13 (E1-Verbindung), R13 <-> R14 (Ethernet), R12 <-> R14 (Ethernet)). Die MPLS Implementierung erlaubt es unterschiedliche Anwendungen und Services sicher voneinander getrennt über das gleiche Netzwerk zu transportieren. Services können Layer 2 Punkt-zu-Punkt Kommunikation (Pseudo Wire) oder auch Mehrpunkt-Verbindungen (VPLS) sein. Weiterhin ist die Konfiguration von Layer 3 Mandanten (L3VPN) möglich. Ein Quality of Service Modell beschreibt die Einteilung der Daten in unterschiedliche Prioritätsklassen. Für die Daten des Differentialschutzes werden sogenannte Pseudo Wire Verbindungen geschaltet, die auf Basis des Quality of Service Modells in der höchsten Prioritätsklasse mit absolutem Vorrang übertragen werden. Die Übertragung der einzelnen Services erfolgt alternativ durch MPLS-IP oder MPLS-TP, beide Betriebsarten sind gleichzeitig möglich. Das Kommunikationsnetz wird über PTP (Precision Time Protocol) oder über synchrones Ethernet synchronisiert und kann mit einer präzisen internen Uhr auch über lange Zeit ohne externe Synchronisierung über einen GPS-Zeitempfänger auskommen. Der Takt wird externen Komponenten ebenfalls zur Verfügung gestellt.

Inbetriebsetzung der Anordnung

Eine Erstinbetriebsetzung wurde durch TenneT durchgeführt. Neben der aufwändigen Verkabelung zwischen den Geräten wurden der Differentialschutz und die Kommunikationsgeräte / Router entsprechend den Vorgaben parametriert.

Für die Schutzgeräte wurde eine transformatorische Einspeisung geschaffen, um Last- und Differentialströme zu erzeugen, damit sowohl normale betriebliche Lastzustände als auch Fehlerfälle (Kurzschlüsse) und damit verbundene Schutzauslösungen auf den Leitungen simuliert werden können.

Die weitere funktionale Inbetriebsetzung durch Experten von Siemens und Cisco dauerte einen Tag bis über das Kommunikationsnetz fehlerfreie Verbindungen zustande kamen und der Differentialschutz in einer Ringtopologie funktionierte. Dabei erwies sich als hilfreich, dass Diagnosen in den Geräten eine Bewertung der Qualität und Laufzeit der Datenverbindungen ermöglicht. Die Verbindungen zwischen den Geräten wurden schrittweise aufgebaut und ausgemessen. Die enge Kooperation von Schutz- und Kommunikationsexperten war in diesem Versuch sehr vorteilhaft.

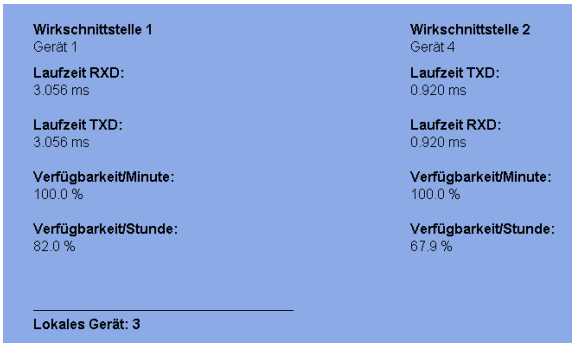


Bild 2 Anzeige von Laufzeit und Übertragungsqualität am 3. Gerät (kurz nach dem Hochlauf)

Für die direkt über Ethernetschnittstellen angeschlossenen Geräte wurde eine Laufzeit von 0,9-0,95 ms ermittelt. Auf der E1-Strecke beträgt die Laufzeit ca. 3 ms. Diese Laufzeit konnte durch Einstellungen in den Routern z.B. hinsichtlich des Wertes des Jitterpuffer auf 1,6 ms im Laufe der Versuche reduziert werden.

Teststrategie

Die Testfälle wurden in einem Test-Book beschrieben, das zwischen den Beteiligten vorab abgestimmt wurde. Bei potentiellen Problemen war die Strategie die Testtiefe punktuell zu erhöhen, um Fehlerursachen zu identifizieren. Es wurden bewusst auch Fälle getestet, z.B. ein automatisches Umrouten der Datenverbindungen, die TenneT später im Betrieb nicht zulassen will.

Die Testergebnisse wurden in einem Testbericht in Englisch dokumentiert, um die Ergebnisse auch international verwerten zu können. Nachfolgend sind einige interessante Testfälle näher beschrieben.

Überlast-Simulation im IP-Netzwerk

Der durch den Differentialschutz erzeugte Datenverkehr beträgt nur wenige Promille der im Netzwerk zur Verfügung stehenden Bandbreite von 1 Gbit/s. Zu testen ist, ob die Pseudo Wire Verbindungen auch störungsfrei und ohne Laufzeitsprünge arbeiten, wenn das Netzwerk überlastet ist. Mit Ethernet-Lastgeneratoren wurde eine Überlast von > 1 Gbit/s erzeugt und über einen längeren Zeitraum jeweils über Nacht beibehalten. Wird der Differentialschutz aus dem Pseudo Wire in die normale Übertragungspriorität parametriert, kommt es zu Telegrammstörungen und die Geräte melden Laufzeitsprünge, da die paketierten Daten nicht konstant ankommen und sogar verdrängt werden. Mit den Daten im Pseudo Wire und der richtigen Quality of Service Einstellung wurden keine Störungen in den Geräten aufgezeichnet. Der Ringbetrieb der Schutzkommunikation wurde dabei kontinuierlich aufrechterhalten. Die Einrichtung der Pseudo Wire im Kommunikationsnetz kann durch Einstellwerte für die VLAN-ID im Layer 2 der Ethernet Telegramme durch die Endgeräte unterstützt werden.

Umschaltung von Pfaden

Das automatische Umschalten von MPLS-Pfaden für die Differentialschutzstrecken ist von TenneT im Betrieb nicht vorgesehen. Man kann das Kommunikationsnetz so parametrieren, dass dies bei Unterbrechungen z.B. von LWL-Strecken oder Router Ausfall geschieht. So wurde z.B. die direkte E1-Verbindung (R11 <-> R13) unterbrochen und der Datenverkehr über die parallele Strecke gelenkt.

Das Schutzgerät sieht kurzzeitig eine Datenstörung, der Ringbetrieb wird in einen Kettenbetrieb überführt und in den vielen Fällen der Differentialschutz im Kettenbetrieb aufrechterhalten. Nachdem der neue Pfad aufgebaut ist, wird wieder der Ringbetrieb aufgenommen. Außerdem messen die Geräte eine neue Laufzeit für diese Strecke und melden ggf. einen Laufzeitsprung. Unterschiede in der Laufzeit in Hin- und Rückrichtung wurden beim Umschalten nicht registriert. Dies hätte bei großem Unterschied zu einer Überfunktion des Differentialschutzes geführt.

Nr.	Datum	Zeit	Ereignis	Urs.	Wert
71	06.03.2013	08:30:12,508	WS2 LZ Sprung	SPN KOM	VQ = Auto Gerät
72	06.03.2013	08:30:12,568	WS2 LZ Sprung	SPN GEH	VQ = Auto Gerät
73	06.03.2013	08:30:24,508	WS2 LZ Sprung	SPN KOM	VQ = Auto Gerät
74	06.03.2013	08:30:24,568	WS2 LZ Sprung	SPN GEH	VQ = Auto Gerät
75	06.03.2013	08:30:30,508	WS2 LZ Sprung	SPN KOM	VQ = Auto Gerät
76	06.03.2013	08:30:30,568	WS2 LZ Sprung	SPN GEH	VQ = Auto Gerät
77	06.03.2013	08:30:36,508	WS2 LZ Sprung	SPN KOM	VQ = Auto Gerät
78	06.03.2013	08:30:36,568	WS2 LZ Sprung	SPN GEH	VQ = Auto Gerät
79	06.03.2013	08:30:42,508	WS2 LZ Sprung	SPN KOM	VQ = Auto Gerät
80	06.03.2013	08:30:42,568	WS2 LZ Sprung	SPN GEH	VQ = Auto Gerät
81	06.03.2013	08:30:48,507	WS2 LZ Sprung	SPN KOM	VQ = Auto Gerät
82	06.03.2013	08:30:48,567	WS2 LZ Sprung	SPN GEH	VQ = Auto Gerät
83	06.03.2013	08:30:54,507	WS2 LZ Sprung	SPN KOM	VQ = Auto Gerät
84	06.03.2013	08:30:54,567	WS2 LZ Sprung	SPN GEH	VQ = Auto Gerät
85	06.03.2013	08:31:00,507	WS2 LZ Sprung	SPN KOM	VQ = Auto Gerät
86	06.03.2013	08:31:00,567	WS2 LZ Sprung	SPN GEH	VQ = Auto Gerät
87	06.03.2013	08:31:06,507	WS2 LZ Sprung	SPN KOM	VQ = Auto Gerät
88	06.03.2013	08:31:06,567	WS2 LZ Sprung	SPN GEH	VQ = Auto Gerät
89	06.03.2013	08:41:41,287	WS2 LZ Sprung	SPN KOM	VQ = Auto Gerät
90	06.03.2013	08:41:41,290	WS1 LZ Sprung	SPN KOM	VQ = Auto Gerät
91	06.03.2013	08:41:41,348	Diff wirksam	SPN GEH	VQ = Auto Gerät
92	06.03.2013	08:41:41,404	WS2 LZ Sprung	SPN GEH	VQ = Auto Gerät
93	06.03.2013	08:41:41,603	Diff wirksam	SPN KOM	VQ = Auto Gerät
94	06.03.2013	08:41:41,652	WS1 LZ Sprung	SPN GEH	VQ = Auto Gerät

Bild 3 Meldebild bei einer Routenumschaltung (dunkle Zeilen)

Bandbreitenbegrenzung und bandbreitenoptimiertes Übertragen

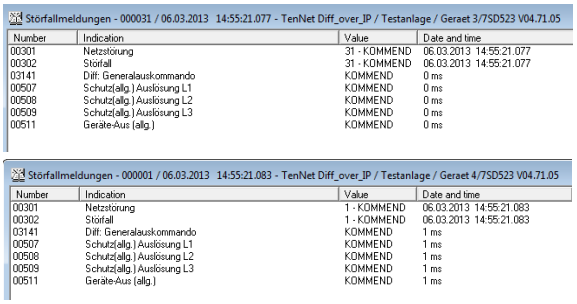
Für die E1-Verbindung müssen über das Ethernet etwas mehr als 2,5 Mbit/s Bandbreite zur Verfügung gestellt werden, da E1 mit 2 Mbit/s den seriellen Datenstrom einspeist. Die Übertragungsmethode ist Pseudo Wire Emulation Edge-to-Edge und für TDM-basierte Daten (Time Division Multiplexing) werden die beiden Verfahren CESoPSN (Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network) oder SAToP (Structure-Agnostic Time Division Multiplexing (TDM) over

Packet) verwendet. Bei den Ethernetstrecken genügen dagegen ca. 750 Kbit/s, wenn die Schutzgeräte den seriellen Datenstrom mit 512 Kbit/s zum Kommunikationsumsetzer schicken. Im E1-Telegramm belegt der Differentialschutz nur ca. 25 % der verfügbaren 32 Zeitschlitze. Welche dies sind, ist im Herstellerhandbuch beschrieben. In einem Versuch wurden über das Pseudo Wire über MPLS nur die mit Daten belegten Zeitschlitze übertragen. Der Brandbreitenbedarf ging um den Faktor 4 auf ca. 500 Kbit/s zurück und auch die Laufzeit reduzierte sich von 1,7 ms auf 1,4 ms. Erkenntnis ist, dass sowohl Bandbreitenbedarf als auch die Laufzeit durch das CESoPSN Übertragungsverfahren positiv beeinflusst werden, falls das Übertragungsgerät diese Eigenschaften bietet. Allerdings erfordert dies höheren Konfigurationsaufwand und detaillierte Kenntnisse der Datenstruktur im E1-Telegramm. Auf dem Markt befindliches E1-Equipment kann damit effektiv über die Pseudo Wire über MPLS eingesetzt werden.

In einem weiteren Versuch wurde die zulässige Bandbreite der Ethernetschnittstelle der Router begrenzt. Dies verhindert ein versehentliches Einspeisen mit hohen Bandbreiten in die hoch priorisierte Pseudo Wire und eine mögliche Überlastung des Netzes. Bei einer Bandbreitenbegrenzung auf 750 Kbit/s wurde kein Einfluss auf die Qualität der Differentialschutzübertragung festgestellt. Erst Werte von 100 Kbit/s (kleinster Einstellwert am Router) führen zu Telegrammstörungen aber zu keiner Unterbrechung der Differential-schutzfunktion.

Differentialschutz-Auslösung

Über eine transformatorische Lasteinspeisung wurde zwischen den Geräten 3 und 4 ein hochohmiger Kurzschluss simuliert. Bei einem Differentialstrom von ca. 50 % vom Nennstrom betrug die Kommandozeit der Geräte zwischen 30 ms – 38 ms. Durch die kurzen Übertragungszeiten im Kommunikationsnetz, die auf ca. 0,9 ms (Ethernetstrecken) und 1,6 ms (E1-Strecke) reduziert, wurden konnte keine merkliche Verlängerung der Auslösezeit gemessen werden. Es werden Werte erreicht, die mit direkten Lichtwellenleiter Verbindungen vergleichbar sind.



Störfallmeldungen - 000031 / 06.03.2013 14:55:21.077 - TenNet Diff_over_IP / Testanlage / Geraet 3/7SD523 V04.71.05

Number	Indication	Value	Date and time
00301	Netzstörung	31 - KOMMEND	06.03.2013 14:55:21.077
00302	Störfall	31 - KOMMEND	06.03.2013 14:55:21.077
03141	Diff: Generalauskommando	KOMMEND	0 ms
00507	Schutz(allg.) Auslösung L1	KOMMEND	0 ms
00508	Schutz(allg.) Auslösung L2	KOMMEND	0 ms
00509	Schutz(allg.) Auslösung L3	KOMMEND	0 ms
00511	Geräte-Aus (allg.)	KOMMEND	0 ms

Störfallmeldungen - 000001 / 06.03.2013 14:55:21.083 - TenNet Diff_over_IP / Testanlage / Geraet 4/7SD523 V04.71.05

Number	Indication	Value	Date and time
00301	Netzstörung	1 - KOMMEND	06.03.2013 14:55:21.083
00302	Störfall	1 - KOMMEND	06.03.2013 14:55:21.083
03141	Diff: Generalauskommando	KOMMEND	1 ms
00507	Schutz(allg.) Auslösung L1	KOMMEND	1 ms
00508	Schutz(allg.) Auslösung L2	KOMMEND	1 ms
00509	Schutz(allg.) Auslösung L3	KOMMEND	1 ms
00511	Geräte-Aus (allg.)	KOMMEND	1 ms

Bild 4 Störfallprotokoll der Differentialschutz-Auslösung in Gerät 3 und Gerät 4

Versuchsergebnisse

Mit den Versuchen könnte der Nachweis erbracht werden, dass sich paketierende MPLS-Ethernet Netze zur Übertragung kritischer Differential Schutzdaten eignen. Während der mehrtägigen Versuche mit umfangreichen Rekonfigurationen im Netzwerk wurde keine Überfunktion des Differentialschutzes festgestellt. Es ist allerdings eine sorgfältige Konfiguration der Pseudo Wire notwendig, damit die Schutzdaten nicht verdrängt werden und es in Folge zu Störungen in der Datenübertragung kommt. Die Pseudo Wire und das Quality of Service Modell müssen von Anfang an in die Netzwerkplanung aufgenommen werden. TenneT kann die bereits vorhandenen Schutz-geräte und E1-Umsetzer auch in diesen neuen Netzen verwenden. Der Dauerversuch kann durch den Netzwerkausrüster und Schutzgerätehersteller von Ferne überwacht werden. Es sind weitere Messungen geplant, um das Zusammenspiel der Komponenten zu optimieren und zukünftige Verbesserungen in den Produkten daraus abzuleiten.

Literatur

[1] M. Rentschler, H. Heine; “The Parallel Redundancy Protocol for Industrial IP Networks”; ICIT 2013, Cape Town, South Africa

[2] AKEKACHAT PAO-ON; “Communication System Division Electricity Generating Authority of Thailand (EGAT)”; Cigre 2006; http://www.labplan.ufsc.br/congressos/cigre06/DATA/D2_314.PDF

[3] Minei Ina, Lucek Julian; “MPLS-Enabled Applications. Emerging Developments and New Technologies”; Wiley, 2008, 2nd Edition; ISBN 978-0-470-98644-8

[4] Lobo Lancy, Lakshman Umesh; “MPLS Configuration on Cisco IOS Software”; Cisco Press, 2006; ISBN 1-58705-199-0

Über die Autoren

Norbert Schuster ist Produktmanager für die Kommunikation in Schutzgeräten. Er arbeitet im Produktmarketing für SIPROTEC – Schutzgeräte bei der Siemens AG in Nürnberg.

Michael Simon ist Customer Solution Architect bei der Cisco Systems und ist technischer Ansprechpartner für die TenneT in Deutschland. Er gehört zur Niederlassung der Cisco Systems in Düsseldorf.

Stefan Steger ist im Assetmanagement in der Unternehmensleitung der TenneT TSO GmbH in Bayreuth, Bereich Schutztechnik, tätig.