ciena
Experience. Outcomes.

WHITEPAPER

Eine Lösung mit extrem kurzer Latenzzeit für Energieversorgungsunternehmen

Im Jahr 2003 erlebte der Nordosten der USA den größten Stromausfall in der Geschichte der Nation. Zwei Tage lang hatten 50 Millionen Stromkunden in acht Staaten und in Teilen von Ontario keine Stromversorgung, was zu wirtschaftlichen Verlusten von schätzungsweise 6 Milliarden USD führte. Der Hauptgrund des Stromausfalls: die Unfähigkeit, unzureichende Leistung und Verschleiß bei Bestandteilen des Weitbereichs-Stromnetzes zu erkennen, abzuschätzen und zu verstehen; ein Problem, welches beim Management kritischer Infrastrukturen nicht unbekannt ist. Zuverlässige Netze, insbesondere auf der kritischen Infrastrukturebene, können Folgen in Form von Rufschädigung und teuren Sanktionen bis hin zu direkten finanziellen Verlusten in Milliardenhöhe verhindern; daher hat dieser Punkt nach wie vor oberste Priorität in der Energieversorgungsbranche.

Abgesehen davon, dass System- und Geräteschäden teure Reparaturen verursachen, können Fehler der Stromversorgung auch zu Störungen des normalen Systembetriebs führen. Ernste Störungen können sogar zur Instabilität der Systeme und zu großflächigen Stromausfällen führen. Die Fehlerbeseitigung muss daher ein integraler Bestandteil des Designs, der Wartung und des Betriebs von Energieübertragungs- und Verteilungssystemen sein. Die Schutzverfahren zur Identifizierung und Beseitigung von Fehlern müssen eine Reihe von Zielen im gesamten Netzwerk erfüllen:

- Trennung des fehlerhaften Elements vom Rest des Systems.
- Begrenzung bzw. Verhinderung von Schäden an Geräten.
- Verhinderung von starken Stromschwankungen und Systeminstabilität.
- Minimierung von nachteiligen Auswirkungen auf die Verbraucherlast.
- Aufrechterhaltung der Übertragungsfähigkeit des Stromversorgungssystems.
- Verhinderung von Personenschäden.

Leistung, mit der die Lichter nicht ausgehen
Mehr erfahren

Verfahren, Applikationen und Konvergenz

Eine Methode, die oft in Umspannstationen von Energieversorgern implementiert wird, basiert auf kommunikationsgestützten Schutzverfahren im WAN. Diese Verfahren vereinfachen die Koordination und den Datenaustausch zwischen Schutzeinrichtungen und ermöglichen den Einsatz von Methoden, welche die Zuverlässigkeit, Selektion, Sicherheit und Geschwindigkeit verbessern. Eine zuverlässige Kommunikation ermöglicht die Implementierung differentieller Vergleichsverfahren, wie beispielsweise dem Netzstrom-Differentialschutz (87L).

WANs werden eingesetzt, um Relaisschutz-Multiplexkanäle sowie andere Unterstationsservices (Sprache, Teleprotektion, Telemetrie, Video, Steuerung und Automatisierung, E-Mail und Firmen-LANs) zu übertragen, und sind ein integraler und notwendiger Teil moderner Stromnetzschutzsysteme.

TDM/SONET wird in der Stromversorgungsbranche als die bevorzugte WAN-Transporttechnologie eingesetzt, da damit niedrige Latenzzeiten sowie eine deterministische und minimal-asymmetrische Leistung unterstützt wird. Es gibt jedoch einen deutlichen Trend in der Branche hin zum Einsatz von Ethernet und paketbasierten Netzwerken für alle Stromversorgungsanwendungen und Services, inklusive Schutz. Die Motivation zur Umstellung von TDM-basierten Systemen, besonders von SONET- und SDH-Systemen, resultiert aus dem Wunsch, IT- und OT-Netzwerke zusammenzuführen und ein gemeinsames, standardisiertes Schnittstellenset einzuführen, um die Investitions- und Betriebskosten zu senken. Aufgrund der Migration auf paketbasierte Netzwerktechnologien, wie z. B. Carrier Ethernet, ergab sich die Herausforderung, Teleprotektions-Services zu entwickeln, welche den Determinismus und die garantierte Leistung bieten, wie sie für Schutzanwendungen erforderlich sind.

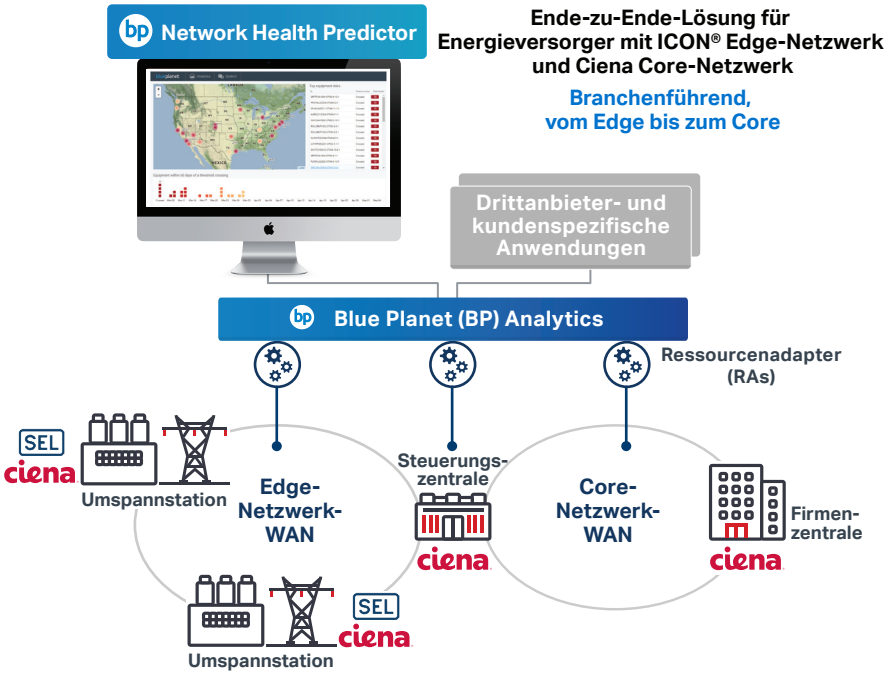

Abbildung 1. Ende-zu-Ende-Lösung für Energieversorger mit ICON Edge-Netzwerk und Ciena Core-Netzwerk

Die Motivation zur Umstellung von TDM-basierten Systemen, besonders von SONET- und SDH-Systemen, resultiert aus dem Wunsch, IT- und OT-Netzwerke zusammenzuführen und ein gemeinsames, standardisiertes Schnittstellenset einzuführen, um die Investitions- und Betriebskosten zu senken.

Um einen weiteren Stromausfall wie 2003 zu vermeiden, ist eine Lösung mit extrem niedriger Latenzzeit und sehr schneller Failover-Leistung erforderlich. Falls ein Fehler im Stromversorgungssystem auftritt, wird mithilfe von durch WAN-Kommunikation unterstützten Schutzverfahren der Fehler isoliert, um eine Instabilität im Umfeld des Fehlers zu verhindern. Die Störungsbeseitigungszeiten für die wichtige Übertragungsleitungsinfrastruktur müssen in der Größenordnung von Millisekunden liegen. Wenn der Fehlerzustand des Versorgungssystems nicht erkannt und mit möglichst geringer Latenzzeit kommuniziert wird, können Anlagenschäden auftreten, von denen größere Teile des Stromnetzes betroffen sind.

Um diese Herausforderungen zu adressieren, setzt Ciena im Rahmen einer Partnerschaft die branchenführende Lösung für Unterstationen von Schweitzer Engineering Labs (SEL) ein.

Die deterministische Pakettransportlösung SEL Integrated Communications Optical Network (ICON) beruht auf dem innovativen Ansatz, geschäftskritischen Datenverkehr mit niedriger und deterministischer Latenzzeit über ein Ciena Carrier Ethernet-Transportnetzwerk bereitzustellen. Dieses Konzept stellt die Leistungsmerkmale von TDM sicher, welche derzeit auf Basis der ICON SONET-Plattform verfügbar sind, ohne dass ein Leistungsverlust auftritt, wenn die Übertragung mittels WAN-Transportprotokoll über Carrier Ethernet erfolgt.

Mehr über die Lösung von Ciena und SEL

Testergebnisse zu Latenz- und Failover-Zeiten bei SONET- Kapselung im Ciena Carrier Ethernet-Core

Die folgenden Testergebnisse zeigen, dass es mit dem SEL ICON Virtual SONET Network (VSN)-Konzept möglich ist, konsistent niedrige Latenzzeiten, eine geringe Kanalasymmetrie und eine sehr schnelle OT-System-wiederherstellung bei Fehlern in den Core- und Edge-Netzwerken bereitzustellen. Diese Ergebnisse erfüllen die Leistungsanforderungen für Schutzanwendungen.

Die Leistungsanforderungen an Kommunikationskanäle für die Anwendung bei Stromversorgungs-Umspannstationen sind in einer Reihe von Normen festgelegt. Durch Verbindung der Leistungsanforderungen gemäß IEEE 1646 und IEC TR 61850-90-12 mit den Anforderungen von Relaisherstellern in Bezug auf Asymmetrie und Wiederherstellung kann eine Zusammenfassung der Leistungsanforderungen an Kommunikationskanäle für Schutzanwendungen aufgestellt werden (Tabelle I).

Verfahren	Latenzzeit (ms)	Asymmetrie (ms)	Wiederherstellung (ms)
87L-Schutz	5	< 0,5	5
Pilot-Schutz	8	5	5
Direktüber-tragung	10	5	5

Tabelle I. Kommunikationskanal-Leistungsanforderungen für Schutzschaltungen

Latenzzeit-Leistungstest und Ergebnisse

Die folgenden Testfälle liefern Leistungsdaten für die Service-Kapselung bei Einsatz von SEL ICON über ein Carrier Ethernet Core-Netzwerk (Ciena 3930/3932 IT WAN Node). Das Netzwerk hat die in Abbildung 2 gezeigte Topologie.

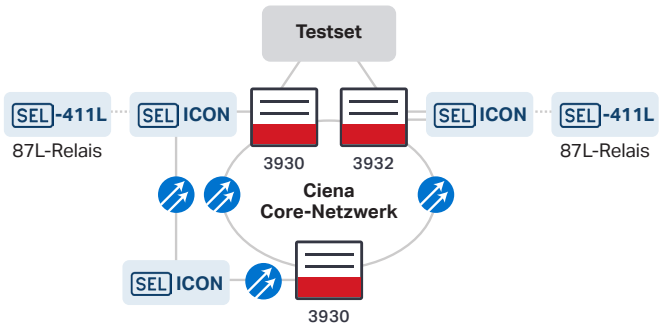

Abbildung 2. Testnetzwerk-Topologie

Um ein Basisdatenset festzulegen, wurden zwei 87L-Relais direkt mit einer faseroptischen Brückenleitung verbunden (Abbildung 3).

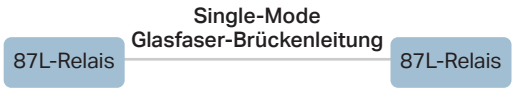

Abbildung 3. Testnetzwerk-Topologie

Als nächstes wurden diese 87L-Relais über ein VSN mit drei Knoten verbunden. Die Informationen bezüglich Latenzzeit und Asymmetrie wurden zum Vergleich mit den Relais-Basisdaten erfasst. Abbildung 4 zeigt die Topologie des VSN-Testsystems.

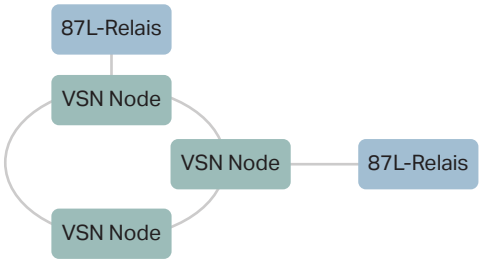

Abbildung 4. VSN-Testnetzwerk

Das VSN-Testnetzwerk wurde dann auf die in Abbildung 1 gezeigte Topologie erweitert. Als Core-Netzwerk wurde ein Ciena Carrier Ethernet-WAN mit drei Knoten eingefügt.

Das Test-VSN wurde somit über das WAN getunnelt, und die 87L-Relais waren nach wie vor mit dem VSN verbunden. Ein Testset wurde benutzt, um Netzwerk-Datenverkehr zu generieren und typische Lastbedingungen zu simulieren. Damit konnte bestätigt werden, dass das Core-Netzwerk die QoS-Einstellungen benutzte, um dem VSN eine höhere Priorität gegenüber dem übrigen Netzwerk-Datenverkehr zu geben und so eine deterministische Leistung bereitzustellen. Im Ciena Carrier Ethernet-Netzwerk-Core wurde dem VSN ein F-RCoS (Fixed Resolved Class of Service) von 0 zugeteilt, und dem Testset-Datenverkehr wurde ein F-RCoS von 7 zugeteilt.

Der Test wurde über die WAN-Knoten des Ciena Carrier Ethernet-Core durchgeführt, wie in Abbildung 1 dargestellt. Bei allen Tests wurde ein 87L-Relais verwendet, um eine 87L-Schutzschaltung zu etablieren. Mithilfe der internen Messfunktionen der Relais wurden die Latenzzeit und Asymmetrie des Kanals gemessen. Die Leistungsparameter für Latenzzeit und Asymmetrie wurden für die Carrier Ethernet-Netzwerkimplementierung erfasst. Bei allen Tests wurde eine Reihe von fünf Einzelmessungen durchgeführt, und die durchschnittlichen Latenzzeiten und Asymmetrien wurden berechnet.

Tabelle II zeigt die Ergebnisse im Vergleich zu den Basisdaten und den reinen VSN-Daten. Alle VSN OT Edge-Geräte verwendeten einen Jitter-Buffer mit variabler Größe, basierend auf den PDV-Werten des Core-Netzwerks, um die Latenzzeit des IT-Core-Netzwerks zu optimieren. Mithilfe einer PDV-Einstellung wurde die Größe des Jitter-Buffers angepasst. Für das Carrier Ethernet-Netzwerk wurde eine PDV von 50 µs verwendet.

Die Testergebnisse in Tabelle II zeigen, dass das Ciena Carrier Ethernet-Netzwerk die Round-Trip-Latenzzeit im Vergleich zu den Basisdaten und den reinen VSN-Konfigurationen nur um 1 ms erhöhte. Das Core-Netzwerk führte zu einer minimalen Asymmetrie, wobei die Ergebnisse deutlich unter den Leistungsanforderungen für Kommunikations-kanäle für 87L-Schutzschaltungen lagen, die in Tabelle I zusammengefasst sind.

Parameter	Basisdaten (ms)	VSN (ms)	VSN und Carrier Ethernet (ms)
Latenzzeit (RTD)	0,1	0,1	1,1
Asymmetrie	0,0	0,0	0,04

Tabelle II. Kommunikationskanal-Leistungstestergebnisse

Vor allem bestätigten die Tests, dass geeignete QoS-Einstellungen definiert werden können, so dass die VSN-Übertragung eine ausreichende Priorität gegenüber anderen Services hat und die deterministische Bereitstellung von VSN-Frames sichergestellt ist. So bleiben die Integrität und das Timing der gekapselten SONET-Daten erhalten.

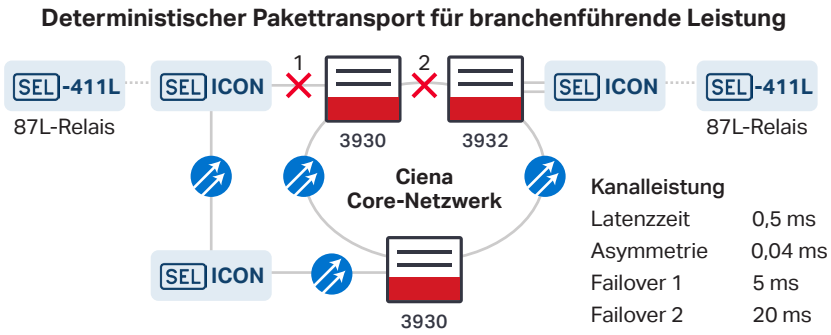

Abbildung 5. Failover-Testergebnisse für Core- und Edge-Netzwerk

Testergebnisse zur Netzwerk-Wiederherstellung

Die Netzwerk-Wiederherstellung für VSN-Pfade kann optimiert werden, indem ungeschützte Point-to-Point-Tunnel über das Core-Netzwerk bereitgestellt werden. Die Netzwerk-Wiederherstellung wird dann durch das VSN OT-Edge-Gerät durchgeführt anstatt durch das Core-Netzwerk.

Die folgenden Wiederherstellungstests wurden durchgeführt, um die Leistung von Edge- und Core-Netzwerk-Failover-Lösungen zu vergleichen. Beim Core-Netzwerk-Failover-Test wurde die Glasfaser am Link unterbrochen, wie in Abbildung 5 (Failover 1) gezeigt, und es erfolgte ein Failover des Core-Netzwerks auf den redundanten Pfad auf der entgegengesetzten Seite des Rings. Beim Edge-Netzwerk-Failover-Test, der in Abbildung 5 (Failover 2) dargestellt ist, wurde ein Link vom OT Edge-Gerät zum Ciena Carrier Ethernet-WAN-Knoten unterbrochen, und die Wiederherstellung erfolgte über das OT Edge-Netzwerk.

Die Failover-Testergebnisse in Abbildung 5 zeigen, dass eine erhebliche bessere Leistung erreicht werden kann, wenn die Wiederherstellung über das OT Edge-Netzwerk erfolgt.

Zusammenfassung

Versorgungsunternehmen implementieren hochintelligente Energieversorgungsnetze, um die Betriebseffektivität zu erhöhen, die Anforderungen der Verbraucher zu erfüllen und behördliche Vorschriften einzuhalten. Diese intelligenten Stromnetze stützen sich auf ein bidirektionales Kommunikationsnetzwerk, das äußerst zuverlässig sein und über niedrige Latenzzeiten verfügen muss, zugleich aber auch wirtschaftlich installiert und betrieben werden kann.

Dieses Dokument zeigt, dass ein VSN-basierter Ansatz eine Methode für den Schutz geschäftskritischer Verbindungen bietet und der Systemdatenverkehr über ein Carrier Ethernet-WAN gesteuert werden kann, wobei sichergestellt ist, dass die Leistungseigenschaften des Kommunikationskanals den Anforderungen gemäß IEEE 1646 und IEC TR 61850-90-12 entsprechen. Dies bietet eine elegante Möglichkeit, um TDM-basierte Schutzschaltungen auf Ethernet zu migrieren, ohne die Leistung des Netzwerks zu beeinträchtigen. Der Entwurf, die Planung und die Implementierung komplexer OT-Netzwerke werden stark vereinfacht, wenn in den Umspannstationen Edge- und Core-Netzwerkelemente enthalten sind, die aus einer Kombination von Herstellergeräten und Transporttechnologie bestehen.

Bei dieser Lösung kommt ein vereinfachtes Provisionierungsmodell zum Einsatz, welches leicht an Änderungen und Wachstum der Netzwerk-Topologie angepasst werden kann. Durch die Verwendung von Point-to-Point-Tunneln über das Carrier Ethernet Core-Netzwerk mit der höchsten QoS-Einstellung unterhalb des NMS wird sichergestellt, dass die Leistung von wichtigen Verbindungen erhalten bleibt, während Änderungen am Netzwerk vorgenommen werden. Damit ist es nicht länger erforderlich, jede Schutzschaltung einzeln zu managen. Trotz der höheren Priorisierung dieses Datenverkehrs ist die Verzögerung der übrigen Datenübertragung vernachlässigbar (maximal 0,1 µs pro Netzwerk-Link bei einem 10GbE-Core-Netzwerk).

Erhalten Sie Antworten auf Ihre Fragen
Die Ciena-Community