Steuerung aller Versorgungsbereiche über WAN-Ringe

Hohe Sicherheitsstandards im Netzleitsystem für ewl Luzern

Moderne Übertragungstechniken beeinflussen zunehmend die Konzepte der Fernwirk- und Leittechnik. Immer öfter wird konventionelle Fernwirktechnik in Netzwerkstrukturen gemäß IEC 870-5-104 eingebettet. Neue Leitsysteme kommunizieren mit der Außenwelt über TCP/IP – eingebunden in effiziente Sicherheitsstandards. Auf der Basis dieser Technologien baut ewl Energie Wasser Luzern ein neues Netzleitsystem auf.

Dr.-Ing. *Jürgen Langhans*, Projektleiter für fernwirk- und leittechnische Anlagen, SAG IDS GmbH, Ettlingen.

Das Schweizer Unternehmen ewl Energie Wasser Luzern ist ein selbstständiges Querverbundunternehmen. Über sechs Tochtergesellschaften bietet ewl die regionale Versorgung mit Strom, Erdgas und Wasser an. Dabei unterhält die Kabelnetz AG ein 50/10-kV- und 110/10-kV-Verteilernetz, die Kraftwerk AG produziert jährlich rd. 128 MWh Strom und unterhält kleinere Wasserturbinen, die Rohrnetz AG betreibt u. a. fünf Druckreduzierstationen. Der Wasser AG gehören alle wassertechnischen Anlagen in der Stadt Luzern. In das Wassernetz werden jährlich rd. 10,5 Mio. m^3 Wasser aus Quellgebieten, dem Grundwasser und dem Vierwaldstätter See eingespeist. Die Summe aller gespeicherten Wasservorräte beträgt 27 400 m^3.

Aufgabenstellung

Bei der Entscheidung für die Neuerrichtung eines Leitsystems standen vor allem Überlegungen zur Datensicherheit und der Wunsch nach Abschottung der gesamten Fernwirk- und Leittechnik von der EDV-Außenwelt im Vordergrund. Ende 2004 erhielt die SAG IDS GmbH, Ettlingen, gemeinsam mit ihrem Schweizer Kooperationspartner Chestonag Automation den Auftrag über ein Leitsystem IDS High-Leit.

Die vorhandenen Fernwirkanlagen werden entweder mit Netzwerkschnittstellen aufgerüstet oder über das proprietäre Fernwirkprotokoll TG80x angebunden. Neue IDS-Fernwirksysteme kommunizieren fast ausnahmslos über IEC 870-5-104 und nutzen dabei LWL-Wege.

Bezüglich der Sicherheit setzt ewl besondere Schwerpunkte:

- strikte räumliche Trennung von redundant arbeitenden Serverkomponenten zwecks Verfügbarkeit bei einem möglichen Brand oder anderweitiger Zerstörung,
- strikte Abschottung des Energiemanagements und der EDV-Außenwelt vom Technik-LAN der Netzleitstelle zum Schutz vor Missbrauch durch Dritte,
- das Technik-LAN muss gegenüber Angriffen über die WAN-Anbindungen der Fernwirkstationen in den Außenbauwerken abgesichert sein.

Diese Anforderungen lassen sich heute unter Nutzung der modernen Kommunikationstechnik mit vertretbarem Aufwand an Material und Kosten bei gleichzeitig hoher Zuverlässigkeit und Verfügbarkeit umsetzen.

Fernwirkebene

Die Front-End-Rechner, die bei ewl in allen Versorgungsbereichen eingesetzt sind, garantieren die redundante Verfügbarkeit aller Fernwirklinien zu den Außenbauwerken und sorgen für eine entsprechende Telegrammumsetzung auf IEC 870-5-101 (über WT bzw. örtliche V.24) und auf IEC 870-5-104 (über LAN/WAN). Weitere Front-End-Rechner bauen auf der Fernwirkseite mehrere WAN-Netzwerke auf und schließen jeweils einen LWL-Ring. (*Bild 1* und *2*).

Im Bereich Wasser werden mehrere Außenbauwerke mit Siemens-Steuerungen bestückt und über Profibus DP und einen IEC-104-Konverter (IDS 850) an das Leitsystem gekoppelt. Die Anlagen erhalten eine autarke Vor-Ort-Steuerung auf der Basis von IDS High-Vis Aqua. Zwei LSA von Siemens kommunizieren über TG/104-Umsetzer (IDS 850) mit dem Leitsystem.

Außenbauwerke, die sich nicht über Leitungen erreichen lassen, erhalten Funkstrecken. Stationen, die nicht ersetzt werden sollen, werden über deren eigenes Protokoll angebunden oder IEC-konform umgerüstet.

Leitebene

Das Leitsystem IDS High-Leit, auf der Basis des Betriebssystems Windows 2003/XP realisiert, enthält neben den Scada-Funktionen höherwertige Entscheidungsfunktionen für Optimierungen: Gasprognose und -bezugsoptimierung unter Einbeziehung historischer Daten und

des Bestands an Sonderkunden im Einzugsgebiet. Zur Berechnung der aktuellen und simulierten Zustände des elektrischen Leitungsnetzes auf der Grundlage von Schalterzuständen einschl. Strangberechnung und der Berücksichtigung von Netzprovisorien ist ein Topologie-Modul integriert.

Sicherheitskonzept in der Netzleitstelle

Im inneren Bereich der Netzleitstelle gibt es drei Netzwerke:

Technik-LAN
Hier befinden sich die Server-PC und Funktionsrechner des Netzleitsystems, die es zu schützen gilt. An den vorhandenen Arbeitsplatzrechnern darf nur ausgewähltes Wartenpersonal arbeiten.

Büro-LAN
Das ist die Ebene des Energiemanagements. Die an den Büroarbeitsplätzen bedienenden Personen unterliegen nicht den Auswahlkriterien für den Technik-LAN und dürfen daher nicht unmittelbar mit dem geschützten Bereich kommunizieren.

Demilitarisierte Zone
Die Demilitarisierte Zone (DMZ) (*Bild 3*) trennt Technik- und Büro-LAN in der Weise, dass der Datenaustausch zwischen beiden Netzwerken über einen Terminalserver geführt wird; respektive die Leitsystemanwendungen stellen Daten aus dem Technik-LAN auf diesem Terminalserver zur Verfügung, und die Anwendungen auf den Arbeitsplatzrechnern greifen aus dem Büro-LAN heraus auf diese Daten zu – analog in Schreibrichtung. Ein direkter Austausch von Daten zwischen Technik-LAN und Büro-LAN findet also nicht statt.

Aus Sicherheitsgründen wird das gesamte Prozessabbild zusätzlich zu den Archiven im Leitsystem auch in einer gesonderten Datenbasis (Oracle-Datenbank) gehalten, die sich auf einem Datenbankserver innerhalb der DMZ befindet. Von hier aus können Daten ohne Risiko für das Netzleitsystem in ewl-eigenen Anwendungen weiterverarbeitet oder einfach nur archiviert werden.

Technisch wird die Firewall mit Cisco PIX 515E, einem Drei-Bein-Router, realisiert. Firewalls schützen nicht vor dem Fehlverhalten autorisierter Anwender und auch nicht vor absichtlichen Umgehungen. Letztlich entscheidet das innerbetriebliche Sicherheitskonzept samt Ausbildung und Auswahl der Anwender über die realistisch erreichbare EDV-Sicherheit in Summe. Klare Reglementierungen und regelmäßige Kontrollen, Passwortmanagement und eine professionell parametrierte Firewall sind unabdingbare Voraussetzungen für einen störungsfreien Betrieb.

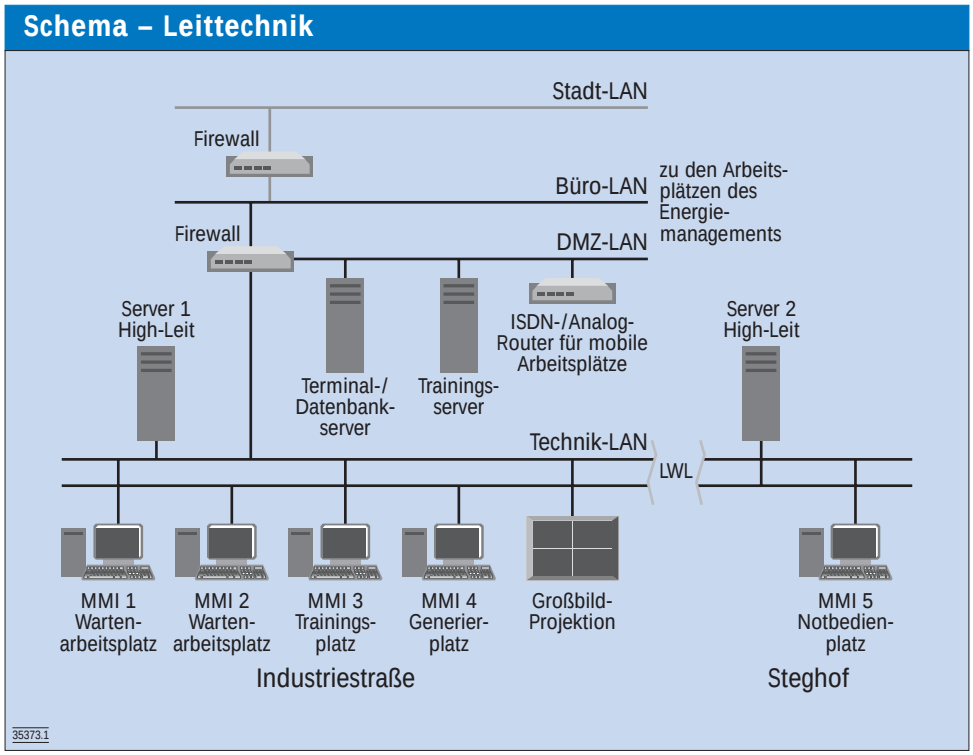


Bild 1. Vereinfachte Darstellung der leittechnischen Konfiguration

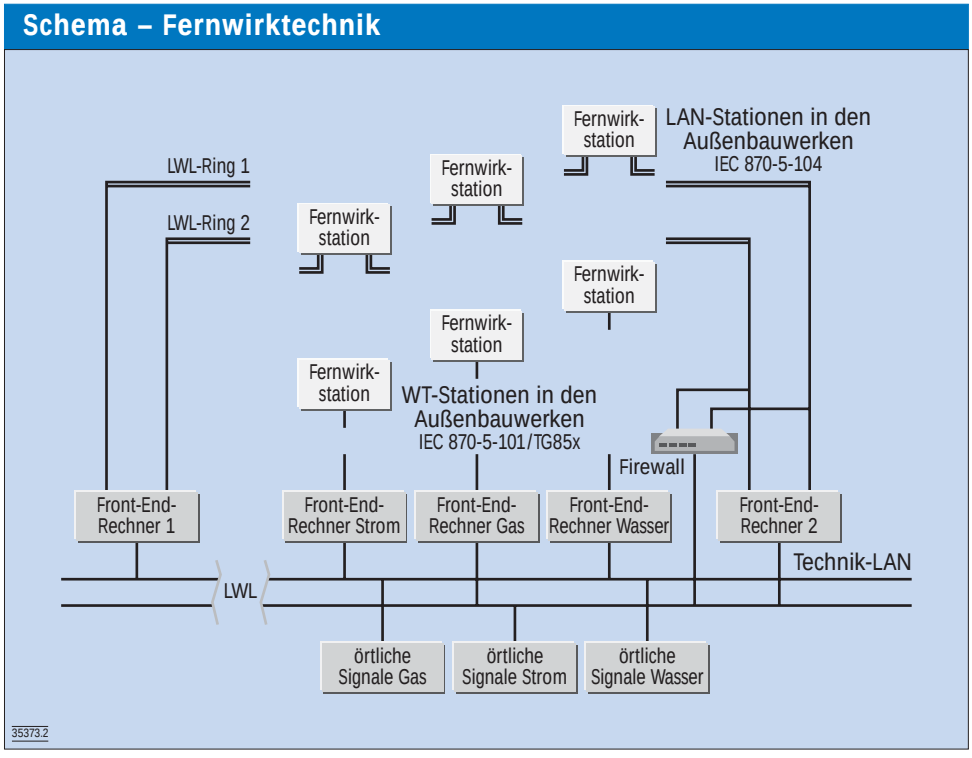
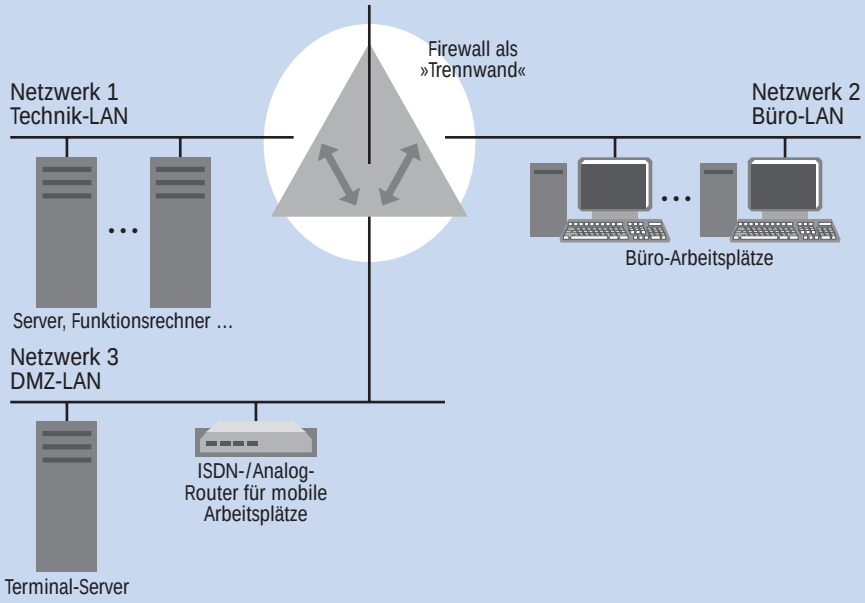


Bild 2. Vereinfachte Darstellung der fernwirktechnischen Konfiguration

Demilitarisierte Zone mit Terminalserver und Firewall

Eine demilitarisierte Zone (DMZ) im Sinne der EDV bezeichnet allgemein ein geschütztes Computernetz, das sich zwischen zwei anderen Netzwerken befindet, die miteinander im Verbund arbeiten sollen. Der Schutz des Computernetzes wird dabei durch eine innere und eine äußere Firewall erreicht oder durch eine Firewall mit mindestens drei Netzwerkanschlüssen. Am Beispiel ewl Luzern stellt sich das so dar:



Ein Anschluss geht zum zu schützenden internen **Technik-LAN**, ein weiterer zu einem öffentlichen Netzwerk, dem **Büro-LAN**, und der dritte bildet die DMZ, in die ein Terminalserver integriert ist. Über diesen **Terminalserver** läuft dann der gesamte Datenaustausch; ein direkter Datenaustausch zwischen internem und öffentlichem Netzwerk findet nicht statt.

Ziel ist, dass im Falle eines »Angriffs« von außen nicht der Technik-LAN, sondern bestenfalls der in der DMZ verankerte Terminalserver beeinträchtigt wird.

35373.3

Bild 3. Demilitarisierte Zone

Sicherheitskonzept auf Fernwirkebene

Die Betrachtungen beziehen sich ausschließlich auf Fernwirktechnik, die innerhalb von TCP/IP-Netzwerken via IEC 870-5-104 kommuniziert und daher grundsätzlich wie jeder andere Netzteilnehmer gefährdet ist.

Es gibt zwei Möglichkeiten, netzwerkfähige Stationen an das Leitsystem anzubinden:

- direkt als eigenständiger Front-End-Rechner über eine Netzwerkkarte an das Technik-LAN,
- über einen zentralen netzwerkfähigen Front-End-Rechner.

Letztgenanntes bietet sich an, wenn absehbar ist, dass im Endausbau sehr viele Stationen über LAN/WAN betrieben werden sollen und/oder wenn besondere Forderungen an die EDV-Sicherheit gestellt werden. Der zentrale Front-End-Rechner bildet sowohl zum Technik-LAN als auch zum Fernwirk-WAN jeweils ein eigenes Netzwerk. Die Kommunikation findet im Standardfalle mit einer IP-Adresse und einem Port mit max. 254 Kopplungen zu einer Netzwerkkarte im Front-End-Rechner statt. Dabei wirkt der zentrale Front-End-Rechner zudem als Barriere, respektive als herstellerspezifische Firewall.

Bei ewl werden derzeit zwei Fernwirknetze über einen zentralen netzwerkfähigen Front-End-Rechner angebunden, wobei jedes für sich außerdem einen Ring bildet und somit die eingebundenen Fernwirkstationen allesamt über einen Zweitweg verfügen. Zum Einsatz kommen LWL-Ring-Switches von Hirschmann. Eine zusätzliche Firewall als Umgehung des Front-End-Rechners 2 (*Bild 2*) ermöglicht das direkte Durchschalten der Kommunikation zwischen einem mobilen Arbeitsplatz in den Außenbauwerken und dem Leitsystem.

Ein unschätzbarer Vorteil der LAN-/WAN-Technologie ist die faktisch unbeschränkte Ortsungebundenheit beim Setzen der Fernwirkstationen in den Außenbauwerken oder im örtlichen Bereich der Leitwarte.

Schlussbetrachtungen

ewl erhält ein auf neuestem technischen Standard basierendes Fernwirk- und Netzleitsystem für die Überwachung, Steuerung und Optimierung der Versorgungsbereiche Strom, Erdgas und Wasser. Dabei wird den hohen Sicherheitsanforderungen von ewl mit einem ausgefeilten Netzwerkkonzept entsprochen, und dies sowohl auf der leittechnischen als auch auf der fernwirktechnischen Seite.

(35373)

juergen.langhans@ids.de

www.ids.de