

# ENERGIEKONTROLLZENTREN - KNOTENPUNKTE DER ENERGIEVERSORGUNG

Verfasser: Thomas Beer, Karl Adolf Neubecker, Walter Schmitz

## GLIEDERUNG

Gliederung.....	1
1. Einführung.....	2
2. Die Versorgungskette in der Stromwirtschaft .....	4
2.1 Erzeugung von Elektrizität .....	4
2.2 Transport .....	5
2.3 Verteilung.....	5
3. Die Funktionen der Kontrollzentren.....	6
4. Ausgangslage, Bedrohung und Verwundbarkeit.....	12
4.1 Ausgangslage .....	12
4.2 Bedrohungen .....	15
4.3 Verwundbarkeit .....	16
5. Sicherheitsanforderungen .....	17
5.1 Regelungen für Authentifizierung und Zugriffskontrolle .....	17
5.2 Verschlüsselung.....	18
5.3 Konfiguration von Firewalls.....	18
5.4 Virenschutz.....	19
5.5 Weitere Anforderungen .....	19

# 1. EINFÜHRUNG

Am 8. April 2009 meldete Thomson Reuters<sup>1</sup>, dass professionelle „Cyberspione“ in das Stromnetz der USA eingedrungen seien und Softwareprogramme hinterlassen hätten, die in der Lage gewesen wären, die Stromversorgung zu unterbrechen. Der Angriff war in diesem Fall ohne Folgen, da es sich nach Ansicht der Behörden nur um einen „Erkundungsangriff“ gehandelt hatte; bereits im Vorjahr hatte es eine Reihe von Eindringversuchen in das elektrische Netz der Vereinigten Staaten von Amerika gegeben

Derartige Vorgänge weisen einmal mehr auf ein rapide angewachsenes neues Gefährdungspotenzial und seine gravierenden Auswirkungen hin: flächendeckende Stromausfälle beeinträchtigen fast alle kritischen Infrastrukturen: die Informations- und Kommunikationstechnologien (IKT), das Transport- und Verkehrswesen mit allen Verkehrsträgern und Dienstleistungen, Industrie- und Produktionsbetriebe, Handel und Gewerbe, das Gesundheitswesen einschließlich des Notfall- und Rettungswesens, die Wasserversorgung, Nahrungsmittelversorgung einschließlich der Transportlogistik, die Entsorgung von Abwasser, Schadstoffen und Müll, die Behörden und die öffentliche Verwaltung, das Banken- und Finanzwesen einschließlich der Bargeldversorgung, Forschungseinrichtungen, Medien und nicht zuletzt die Energieversorgung selbst. Die Folgen sind gravierend und komplex. Alle Bereiche des öffentlichen und privaten Lebens sind einschneidend betroffen: vom Flugverkehr bis zur Toilettenspülung. Nicht zuletzt wegen der umfassenden Abhängigkeiten von Wirtschaft und Gesellschaft von dem Funktionieren der Energieversorgung wird diese im Vergleich zu anderen Infrastrukturen wie Transport und Verkehr, Wasserversorgung oder Telekommunikation als die Kritischste angesehen.

Die Entwicklung der Stromversorgung zu einer für die Gesellschaft *kritischen Infrastruktur* hat sich im Grunde erst in den letzten Jahrzehnten vollzogen: früher war die Versorgung dezentralisiert, mit einem Kraftwerk in jeder Region; ein lokales Verteilnetz verband den Hersteller mit den Verbrauchern. Wenn das Kraftwerk ausfiel, gab es in der gesamten Region keinen Strom! Es brauchte mehr als ein Jahrzehnt bis die regionalen Verteilnetze über ein flächendeckendes Transportnetz miteinander verbunden waren. Damit wurde nicht nur eine Verbesserung der Versorgungssicherheit erzielt, sondern auch ein effizienterer Betrieb der Kraftwerke. Es war nun möglich, Energie zwischen den regionalen Netzwerken nach Maßgabe ihrer Last auszutauschen – was viel Geld einsparte.

Der Betrieb der Kraftwerke und die Verteilung des produzierten Stroms werden durch *Kontrollzentren* (Leitwarten) überwacht und gesteuert. Im Zuge des zunehmenden Stromverbundes, der Liberalisierung der Strommärkte, der wachsenden Integrationserfordernis von Strom aus erneuerbaren Energien und zunehmendem Kostendruck wurden die Kontrollzentren zunehmend komplexer. Diese Entwicklung profitierte intensiv von der parallel laufenden Entwicklung und Anwendung der Informationstechnologie. Kontrollzentren verwenden heute moderne Methoden der Datenakquisition, Datenverarbeitung und Kommunikation. Sie haben sich zu zentralen Einrichtungen für die Energieversorgung entwickelt.

Die prinzipiellen Aufgaben der Kontrollzentren sind:

---

<sup>1</sup> „Cyberspies penetrate electrical grid“; Internet

1. Messung, Sammlung und Kontrolle von Daten durch Sensoren – einschließlich (auch satellitengestützter) Überwachung und Kontrolle von Kraftwerken, und Netzen (z.B. Stromnetze, Öl- und Gaspipelines).
2. Überwachung und Kontrolle durch Erfassung und Übermittlung von Daten von u. U. weit entfernten Messstationen über ein Kommunikationsnetz an die Kontrollzentren sowie die Übermittlung von Befehlen von den Kontrollzentren an die „operationellen“ Stationen.
3. Aufbereitung, Darstellung und Archivierung von Betriebsdaten, Generierung von Führungsinformationen. Datenakquisition und deren Verarbeitung mit Hilfe von SCADA Systemen<sup>2</sup>.
4. Analyse des Betriebszustandes der Energieversorgungskomponenten z.B. mit dem Ziel des Sicherheitsmanagements unter Nutzung der *Emergency Management System (EMS)* Technologie, Methoden der Netzwerkanalyse, der Ereignisplanung und Steuerung, sowie von Trainings- und Expertensystemen .

In der öffentlichen Wahrnehmung ist das Ausfallrisiko der Elektrizitätsversorgung in der Regel eng verknüpft mit Störungen in den Kraftwerken und Unterbrechungen in den Stromnetzen. Weniger bekannt ist die Tatsache, dass auch von den Kontrollzentren selbst erhebliche Risiken ausgehen, die zum Ausfall der Stromversorgung führen können. Diese begrenzte Wahrnehmung mag daran liegen, dass spektakuläre Störungen von Kontrollzentren mit nachhaltigen Auswirkungen auf die Stromversorgung bisher noch nicht öffentlich geworden sind. Aber Sicherheitsexperten sind sich einig, dass in den heutigen Kontrollzentren der Stromversorgung ein Risikopotential vorhanden ist. Hierbei ist das Risiko gleichermaßen verteilt auf konventionelle Angriffe gegen die Gebäudeinfrastruktur, Personen und elektronische Angriffe<sup>3</sup> gegen die IT-Infrastruktur. Die Zahl der Cyberangriffe auf Kontrollzentren hat in den letzten Jahren deutlich zugenommen, obwohl (und auch gerade weil) betriebsinterne, veraltete IT Lösungen ergänzt bzw. ersetzt wurden und die Funktionalitäten der Kontrollzentren vor allem durch sog. COTS-Produkte<sup>4</sup> und Standard-IT-Verfahren erweitert und verbessert worden sind. Die Implementierung *integrierter* Sicherheitslösungen, die dem Charakter der Kritikalität der Energieinfrastruktur Rechnung tragen, hat ein durchgehend gleiches Sicherheitsniveau hervor gebracht.

Weltweit bauen Sicherheitsdienste, Polizei und Militär Fähigkeiten zur Nutzung, Früherkennung, Analyse und Abwehr von Cyberangriffen auf; für den internationalen Terrorismus und das organisierte Verbrechen gehören Cyberangriffe praktisch zum Alltag. Die im Internet veröffentlichten einschlägigen Erfolge von Hackerclubs haben demgegenüber fast eine sportliche Note, demonstrieren aber den hohen Stand des weltweit vorhandenen Angriffspotenzials! Die erforderlichen Fähigkeiten zu Cyberangriffen werden nach Allen<sup>5</sup> über die Jahre hinweg trotz aller Sicherungsmaßnahmen immer niedriger!

Viele Kontrollstationen verfügen nur über bescheidene physische Sicherheitsvorkehrungen und sind damit potenziell gegenüber direkten konventionellen terroristischen Angriffen verwundbar. Die Gemengelage aus unzureichender Härtung der IT und nicht hinreichend gesicherter baulicher Infrastruktur erhöht das Risiko gegenüber kombinierten Angriffen auf Kontrollzentren.

---

<sup>2</sup> Supervisory Control and Data Acquisition

<sup>3</sup> Auch bekannt als Cyberangriffe

<sup>4</sup> Commercial-Off-The-Shelf

<sup>5</sup> Allen, J., A.Christie, W.Fithen, J.McHugh; J.Pickel und E.Stoner:” State of the practice of intrusion technologies.” Carnegie Mellon University, Software Engineering Institute, CMU/SEI-99-TR-028 ESC-TR-99-028

Die Europäische Kommission, Generaldirektorat *Justice, Freedom and Security* (Prevention, Preparedness and Consequence Management of Terrorism and other Security related Programs) hat dieses Problem mit dem Projekt **OCTAVIO: Energy System Control Centers Security, an EU Approach** aufgegriffen und gefördert.

Im ersten von drei aufeinanderfolgenden Schritten beschreibt OCTAVIO die Infrastruktur der Strom- und Gaswirtschaft vom Erzeuger bis zum Verbraucher und identifiziert Gefährdungspotentiale durch terroristische Einwirkungen und organisiertes Verbrechen. Im zweiten Schritt untersucht OCTAVIO die Bedrohung von Kontrollzentren durch elektronische („Cyber“) und physische Angriffe. Im dritten Schritt entwickelt OCTAVIO ein Protokoll für ein Sicherheitsaudit, das gemeinsam mit Energieträgern getestet wird.

Die nachfolgenden Ausführungen nehmen Bezug auf das Projekt OCTAVIO. Der Schwerpunkt liegt auf der Gefährdung von Kontrollzentren der Elektrizitätswirtschaft durch elektronische Einwirkungen

## 2. DIE VERSORGUNGSKETTE IN DER STROMWIRTSCHAFT

### 2.1 ERZEUGUNG VON ELEKTRIZITÄT

Der Strom fließt von den Erzeugungsanlagen über die Umspannanlagen und die Netze zum Verbraucher. Geeignete Steuerungssysteme ermöglichen die Interaktion zwischen Bedienern und der Hardware für Stromerzeugung, -transport und -verteilung. Bei der Stromerzeugung unterscheidet man zwischen thermischen Kraftwerken (Kernkraft, fossile Brennstoffe), Wasserkraftwerken und Stromgewinnung aus erneuerbaren Energien.

*Wasserkraftwerke* verwandeln die potenzielle Energie des Wassers über ein Turbinen-/Generator System in Elektrizität. Sie werden in Verbindung mit Staudämmen, Staustufen der Flüsse und als Pumpspeicherwerke betrieben. In dieser Form dienen sie dazu, Verbraucherspitzen abzufangen

Zur *Stromgewinnung aus erneuerbaren Energien* werden neben Biomasse, Müll etc. vor allem Wind- und Solaranlagen eingesetzt. Beiden Technologien ist gemeinsam, dass wegen der Schwankungen der Wetterlage eine präzise Vorhersage der Stromerzeugung nicht möglich ist. Daher eignen sich erneuerbare Energien im Grunde nicht für die Bereitstellung der Grundlast der Stromversorgung. (s.u.).

Da sich Strom nur begrenzt speichern lässt, muss im Prinzip immer genau so viel Strom erzeugt werden, wie von den Endverbrauchern benötigt wird. Ungleichgewichte zwischen Erzeugung und Verbrauch erzeugen Frequenzveränderungen im Netz, die je nach Größe des Ungleichgewichtes bis zum Zusammenbruch des Netzes führen können.

Aufgrund der unterschiedlichen Nachfrage schwankt der Verbrauch im Tages-, Nacht- und Jahresrhythmus. Zum Ausgleich der Schwankungen werden deshalb unterschiedliche Arten von Kraftwerken eingesetzt:

- *Grundlastkraftwerke* zur Erzeugung der Strommenge, die während des Tages nicht unterschritten wird („Grundlast“).

- *Mittellastkraftwerke* zur Abdeckung des prognostizierten Verbrauchs mit variabler Leistung.
- *Spitzenlastkraftwerke* zur Abdeckung kurzfristiger Leistungserfordernisse. Sie werden nur zu den absoluten Verbrauchsspitzen und bei ungeplanten Schwankungen des Stromverbrauchs, z.B. bei Ausfällen anderer Kraftwerke eingesetzt.

## 2.2 TRANSPORT

Der in den Kraftwerken erzeugte Strom wird durch Leitungsnetze über größere Distanzen zum Verbraucher transportiert. Elektrizität fließt auf allen Verbindungswegen zum Verbraucher und nur besondere Schaltmaßnahmen können den Strom auf einem *speziellen Weg* zu einem bestimmten Ziel bringen. Deshalb erfordert der Transfer von Strom erhebliche Koordination und proaktive Überwachung des Systems: wenn irgendwo ein Problem entsteht, beeinflussen seine Wirkungen u. U. Operationen an ganz anderer Stelle des Netzes!

Wegen der von Stromstärke und Leitungswiderstand verursachten Übertragungsverluste gibt es je nach Aufgabe *Transportnetze* und (regionale und lokale) *Verteilnetze*, die über Transformatorstationen miteinander gekoppelt sind. *Transportnetze* werden als „Höchstspannungsnetz“ mit 220kV bzw. 380kV und als Hochspannungsnetz mit 110kV betrieben. Sie nehmen die Stromproduktion aus Kraftwerken auf und transportieren sie zu den Zentren des Verbrauchs. Sie sorgen zudem für den großflächigen Verbund der nationalen und internationalen Netze einschließlich des Stromimports und -exports über entsprechende Koppelstellen mit dem Ausland. Das Transportnetz ermöglicht damit eine (energiesparende) Entkopplung von geografischen Lage und Verteilung des Verbrauches. Knotenpunkte (auch „Übertragungspunkte“) in den Netzen sind Schalt- und Transformatoranlagen. Sie dienen u.a. der Veränderung der Spannungen, zu Schaltvorgängen im Netz und zwischen Netz und Kraftwerken.

Transport- bzw. Übertragungsnetze müssen zur Vermeidung von Versorgungsausfällen in größeren Regionen hohen Netzsicherheits- und Zuverlässigkeitsanforderungen genügen. Die Netze sind deshalb mit Redundanzen in Form parallel geschalteter Übertragungsleitungen ausgestattet, die es ermöglichen, Strom von jedem Kraftwerk zu jedem beliebigen Verbrauchszentrum auf verschiedenen Wegen zu schicken. Damit können Störungen aufgefangen und Versorgungsausfälle verhindert werden. Das n-1-Kriterium ist hierbei verbindlich vorgegeben:<sup>6</sup> bei Ausfall einer Netzkomponente muss das übrige Netz in der Lage sein, die Versorgung ohne Ausfall zu gewährleisten.

Bei der Dimensionierung des Netzes spielen neben Netzsicherheit und Zuverlässigkeit natürlich auch Kosten eine treibende Rolle. Netze werden daher so effizient wie möglich gestaltet.

## 2.3 VERTEILUNG

**Verteilnetze** dienen dazu, den Strom aus dem Transportnetz an den „Übergabepunkten“ zu übernehmen und Haushalten, Gewerbe und Industrie zugänglich zu machen. Verteilungsnetze sind überwiegend als Ringnetze ausgeführt. Bei einem Ausfall einer Netzkomponente tritt in der Regel eine lokal begrenzte Versorgungsunterbrechung auf. Die Versorgung kann aber durch Umschaltung im Netzverbund im Allgemeinen schon nach relativ kurzer Unterbrechungsdauer

---

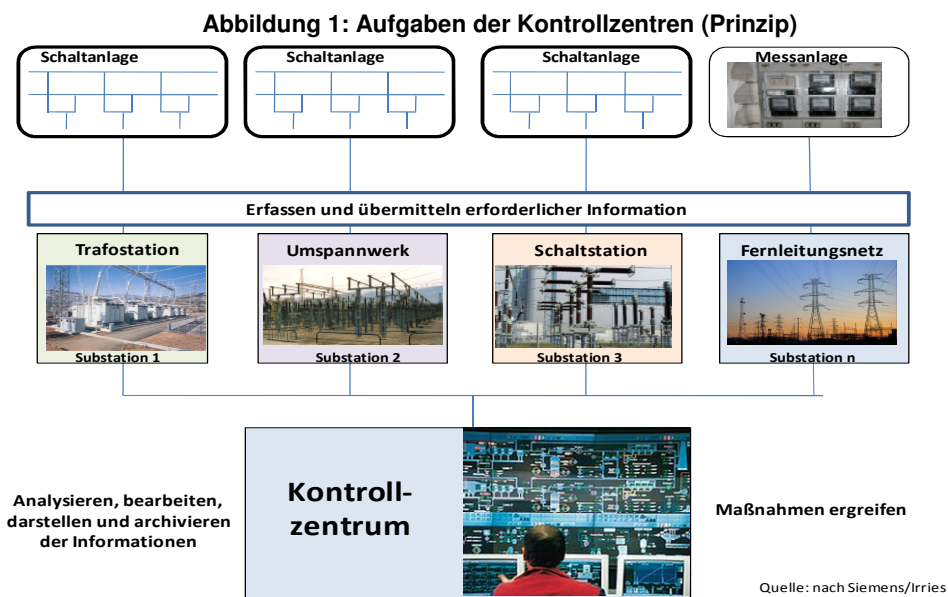
<sup>6</sup> Siehe VDN Transmission Code

wieder aufgenommen werden. Auf der Verteilnetzebene ist das n-1 Kriterium übrigens nicht zwingend vorgeschrieben.<sup>7</sup>

### 3. DIE FUNKTIONEN DER KONTROLLZENTREN

Kontrollzentren dienen der Überwachung, Steuerung und Kontrolle der Prozessabläufe bei Produktion, Transport und Verteilung von Strom (siehe Abbildung 1). Bei Störungen und Ausfällen sind sie verantwortlich für die Einleitung der Ursachenermittlung und Schadensbeseitigung. Hier laufen die Meldungen der SCADA<sup>8</sup>-Systeme sowie die Telefonmeldungen von Betroffenen auf. Bei einem Störfall liegt die Entscheidung über die Wahl der zu ergreifenden Maßnahmen zur Schadensabwehr und Schadensbeseitigung im Allgemeinen bei den dezentralen, für den jeweiligen Netzabschnitt zuständigen Kontrollzentren.

Komplexe Strukturen, wie das elektrische Netz, werden über eine *Hierarchie von Kontrollzentren* überwacht und gesteuert (siehe Abbildung 2 **Fehler! Verweisquelle konnte nicht gefunden werden.**):

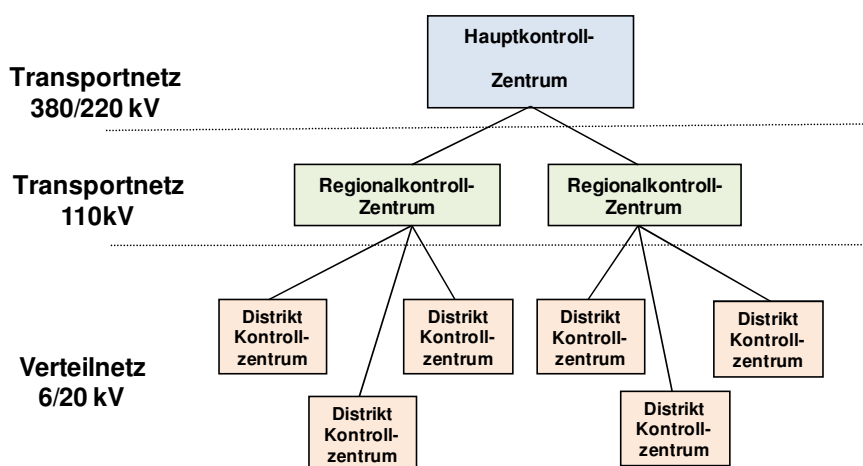


Man unterscheidet

- Hauptkontrollzentren, verantwortlich für Erzeugung, Koordination und Lastverteilung sowie für die Überwachung und Steuerung des Transportnetzes.
- Regionale Kontrollzentren, verantwortlich für Überwachung und Kontrolle des Transportnetzes innerhalb eines bestimmten Gebiets
- Distrikt Kontrollzentren, verantwortlich für Überwachung und Kontrolle des Verteilnetzes in einem bestimmten Gebiet.

<sup>7</sup> Vgl. VDN Distribution Code; nach Definition des VDN werden eine Reihe von 110kV-Leitungen zur Verteilnetzebene gezählt. Für die 110kV-Netzgruppen mit Übertragungsfunktion gilt der VDN Transmission Code, womit bei diesen Leitungen das n-1-Kriterium einzuhalten ist.

<sup>8</sup> Surveillance, Control and Data Acquisition



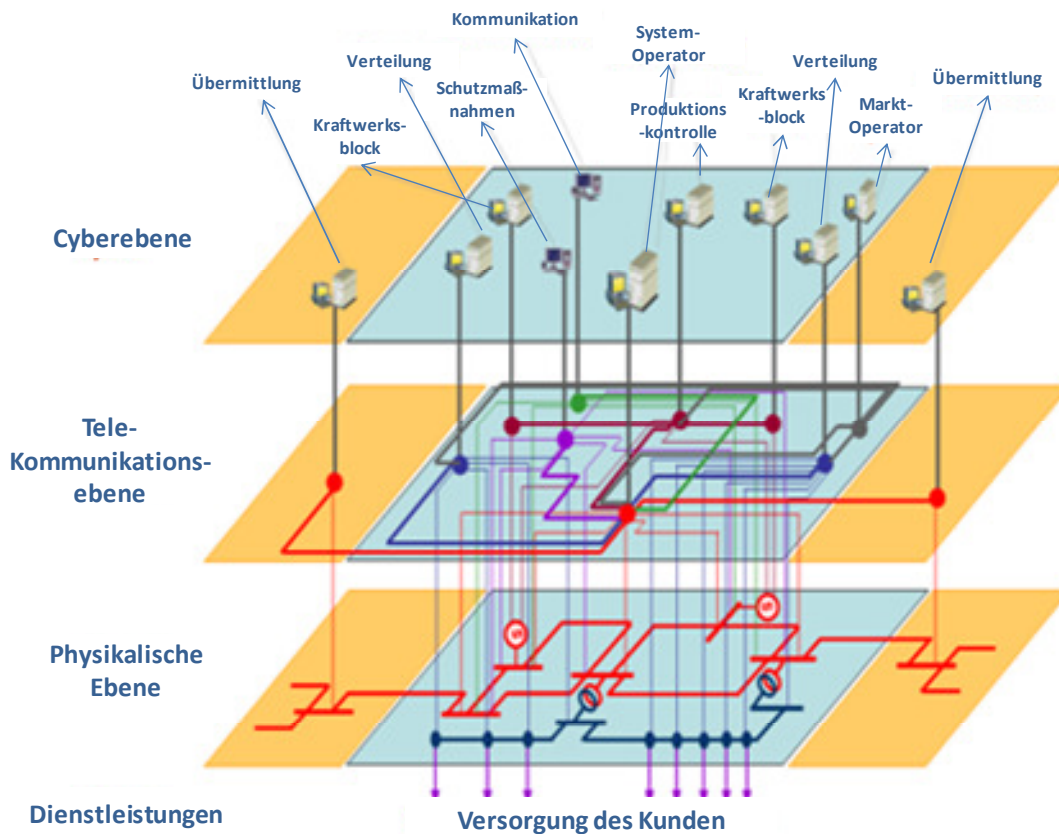
**Abbildung 2 :** Hierarchie von Kontrollzentren

Ohne Einsatz der Informations- und Kommunikationstechnologie wäre eine effiziente Überwachung und Steuerung der Betriebsabläufe nicht möglich. Der Umfang der Verflechtung der IT mit den Prozessen der Elektrizitätsinfrastruktur wird aus Abbildung 3 ersichtlich.

**Abbildung 3: Komplexität und Interdependenz der IT Funktionen<sup>9</sup>**

---

<sup>9</sup> Quelle: OCTAVIO



Dabei ist ganz offensichtlich, dass aus der ursprünglichen Unterstützungsfunktion der IT heute eine Primärfunktion geworden ist, an der sich die Prozesse der Energiewirtschaft ausrichten. Einige Funktionen der in Abbildung 3 dargestellten IT-Struktur seien beispielhaft beschrieben:

- Die Marktumgebung:* Der für Marktentwicklung, Kauf und Verkauf von Strom usw. verantwortliche „Markt Operator“ steht in direkter Verbindung nach außen mit den Marktteilnehmern und nach innen mit dem System Operator, um Angebot und Nachfrage effizient in Übereinstimmung zu bringen. Der Informationsaustausch läuft über IT-Systeme und öffentliche Kommunikationsmittel einschließlich Internet.
- Überwachung und -kontrolle:* Übertragungs- und Verteilsysteme (auf der physikalischen Ebene) sind miteinander vernetzt und jede Komponente hat für Überwachung und Kontrolle ein zugehöriges IT-System. Dazu kommen die Produktionseinrichtungen der Stromerzeuger mit ihren eigenen Kontrollzentren und zugeordneten Informations- und Kommunikationssystemen und den Verbindungen zum Übertragungs- und Verteilungssystem, über die selektiv Informationen eingespeist und entnommen werden. Kommunikationssysteme verfügen über eigene Kontrollzentren mit entsprechenden Steuer- und Überwachungsnetzwerken, über die im Fall von Störungen der Kommunikationsfluss gesteuert werden kann.
- Schutzsysteme:* Bis noch vor wenigen Jahren basierte der Schutz gegen technisches Versagen auf elektromagnetischen Funktionen (z.B. Relais). Sie sind heute durch Mikroprozessoren ersetzt, die eine Erweiterung der Funktionalitäten von Schutzrelais erlauben, wie z.B. die

computergesteuerte, automatische Schadensbehebung über größere Entfernungen. Derartige Funktionen sind in sog. Schutzzentren zusammengefasst.

- d) *Zählersysteme*: An allen Abgabe- Übergabe-, Kontroll- und Endverbrauchspunkten werden die durchfließenden Strommengen gemessen. In regelmäßigen Abständen zwischen 15 Minuten und einer Stunde werden die Messwerte an die Kontrollzentren weitergeleitet. Der Mess- und Kontrollbedarf ist in den letzten Jahren drastisch angestiegen: bis zu 30 Millionen Zähler sind in manchen Ländern im Einsatz.

Nahezu alle Kontrollzentren greifen bei der Kontrolle der Prozesse auf SCADA Technologie zu. Der Begriff "SCADA" wird gewöhnlich im Zusammenhang mit ausgedehnten, zentral überwachten Systemen wie etwa der Energie-Infrastruktur verwendet, die über große Entfernungen verteilte Anlagen, Leitungsnetze und Funktionsgruppen („Remote Terminal Units“ (RTU)) durch Datenerfassung, Abgleich der Daten und daraus abgeleiteter Maßnahmen überwachen und steuern. Ein großer Teil dieser verteilten Einrichtungen ist für jedermann sichtbar, meist unbewacht und in vielen Fällen mehr oder weniger direkt zugänglich. Ihre physische Sicherheit ist auch von Überwachungssensoren und der sie mit den Kontrollzentren verbindenden Informations- und Kommunikationstechnologie abhängig.

Die traditionellen Funktionen von SCADA sind:

- Erfassung der in den „Fernbedienungseinrichtungen“ (RemoteTerminal Units, RTU's) anfallenden Daten
- Verifizierung der erfassten Daten durch Vergleich mit Sollwerten
- Darstellung der Daten im Kontrollzentrum über eine benutzerfreundliche Oberfläche (Human-Machine-Interface, HMI))
- Überwachung und Kontrolle nach Maßgabe der Operatorvorgaben. Datenerfassung und Auswertung (z.B. als Trenddaten)
- Sicherung der Datenbasis
- Kommunikationsmanagement, z. B. Verbindungsaufbau mit den RTU's, nutzungsgerechte Transformation der übertragenen Daten.

Moderne SCADA Systeme ermöglichen durch proaktive Datenerfassung in hoher Auflösung eine neue Dimension der Zuverlässigkeit und der Sicherheit der Stromlieferung und erzielen damit eine Reduktion der Kosten sowie eine Verbesserung der Kundenzufriedenheit. Sie schaffen damit auch Grundlagen für zeitnahe Entscheidungen.

Steigende Kosten moderner SCADA-Systeme konnten durch die Einführung von COTS Produkten aufgefangen werden, die die ursprünglichen patentrechtlich geschützten Eigenentwicklungen („legacy proprietary systems“) ersetzen und die gleichzeitig zu einer weiteren Steigerung der SCADA- Funktionalitäten führten.



**Abbildung 4:** *Typische SCADA Konsole*

Bei kleineren SCADA Systemen besteht die Master Station im Kontrollzentrum nur aus einem PC. Bei größeren SCADA Systemen gibt es im Kontrollzentrum mehrere Server, verteilte Software Anwendungen und integrierte Arbeitsplätze für Systemschutz. SCADA Systeme nutzen offene Standards: für die Kommunikation zwischen Master Station und nachgeordneten Einrichtungen werden z.B. WAN Protokolle wie das Internetprotokoll (IP) benutzt.

Zu den Funktionen der Kontrollzentren<sup>10</sup> gehören:

- *Grundlegende Funktionen*
  - *Management des elektrischen Netzwerks (SCADA)*
    - Überwachen des Netzzustandes
    - Durchführung geplanter Schaltoperationen und Verhindern falscher Schaltoperationen
    - Entdeckung und Korrektur von Fehlern in der Versorgungskette
  - *Koordination der Stromerzeugung*
    - Auslastungsplanung (kurz-, mittel- und langfristig)
    - Produktionsplanung
    - Energieaustausch
    - Produktionsoptimierung
  - *Netzsicherheitsanalysen*
    - Zustandsüberwachung
    - Belastungsberechnungen
    - Kurzschlussberechnungen
    - Optimaler Energiefluss

---

<sup>10</sup> Scriptum Siemens AG: Basics of Power System Management for IRRIS Workshop "Control Centres"05.07.07  
Nürnberg

- Optimierung der Betriebsmittel (z. B. Gas, Wasser, Dampf)
  - Energie Importkontrolle und Lastmanagement
  - Trainingssimulator
- Funktionen in der Hierarchie der Netzwerk Kontrollzentren und Aufgabenzuordnung
    - Lastverteilungszentrum und Hauptkontrollzentrum
      - Produktionskoordination, Lastverteilung
      - Überwachung und Kontrolle des Transportnetzwerkes
      - Durchführung aller Netzwerk Sicherheitsanalysen (NA)<sup>11</sup>, SCADA- und EMS<sup>12</sup> Aufgaben
    - Regionale Kontrollzentren
      - Überwachung und Kontrolle des Transportnetzwerkes
      - Ausführung von Schaltbefehlen des Lastverteilungszentrums
      - Fernüberwachung des Transportnetzwerkes in der Region
      - Ausführung von SCADA- und NA Aufgaben
    - Distrikt Kontrollzentren
      - Überwachung und Kontrolle des Verteilnetzwerkes
      - Durchführung von Schalteroperationen im Auftrag der regionalen Kontrollzentren
      - Durchführung von SCADA und gelegentlich NA Aufgaben
      - Einsatzplanung des Personals für örtliche Schaltaufgaben

Die Anforderungen an die Kontrollzentren sind hoch: Kontrollzentren arbeiten im 24-Stunden-Betrieb, die geforderte Verfügbarkeit beträgt 99.96%. Prozessbezogene Informationen müssen in Echtzeit über große Entfernungen (100 Kilometer und mehr) zum Kontrollzentrum übermittelt werden. Die Koordination des Systemmanagements mit den entsprechenden Ebenen benachbarter Kontrollhierarchien erfolgt in der Regel über Computerlinks.

Ein Kontrollsystem besitzt bis zu 50 Operatorarbeitsplätze, ein Arbeitsplatz verfügt über bis zu vier Bildschirme (siehe z.B. Abbildung 4). Information muss parallel und in Echtzeit verarbeitet und übermittelt werden können. Bei einer größeren Störung treffen über das Netzwerk bis zu 1000 Ereignisse pro Minute im Kontrollzentrum aus den nachgeordneten Stationen ein. Ein großes System muss in der Lage sein, bis zu 1.000.000 Vorgänge (Hinweise, Messwerte, Befehle, Zählerwerte, etc.) in kürzester Zeit zu verarbeiten, denn der Datenstand ändert sich ständig. Alle Maßnahmen im Kontrollsystem müssen online so erfolgen, und zwar so, dass andere Operationen nicht unterbrochen werden.

Generell werden vier Betriebszustände in der Stromversorgung unterschieden:

**Normalbetrieb:** alle Verbraucher sind versorgt, gleichzeitig sind ausreichende Reserven verfügbar. Das Ziel dieses Betriebszustandes ist die wirtschaftliche Optimierung der Energieversorgung.

**Alarmierung:** Alle Verbraucher sind *noch* versorgt, aber die weitere Versorgung ist gefährdet (z.B. wegen Ausfall eines Kraftwerkes, Teilen des Netzwerkes oder der Kontrolleinrichtungen). Das Ziel dieses Betriebszustandes ist die Wiederherstellung des Normalzustandes durch geeignete Maßnahmen.

---

<sup>11</sup> Network Security Analyses

<sup>12</sup> Emergency Management System

**Notfall:** *nicht alle* Nutzer sind versorgt, das Netz droht zusammenzubrechen. Das Ziel in diesem Betriebszustand ist die Begrenzung des Schadens im betroffenen Netz (z.B. durch Lastbegrenzung).

**Restaurativer Betrieb:** Ausfall der Versorgung in einem größeren Gebiet. Das Ziel in diesem Betriebszustand ist die Wiederherstellung des Normalzustandes durch Neutralisierung und erneuter Herstellung der Verbindung.

Diese Darstellung mag hinreichen, um einen Eindruck von der Komplexität der IT Struktur und der Vielfalt der Überwachungs- und Kontrollprozesse in der Stromversorgung in den Kontrollzentren zu vermitteln. Aus der früheren Unterstützungsfunktion für die Kontrolle der Abläufe in Kraftwerken und Netzen ist ein zentralisiertes, komplexes Steuerungsinstrument geworden, ohne die jede Operation innerhalb der Erzeugungs-, Transport- und Verteilungskette unmöglich wäre. Diese eindrucksvolle Entwicklung hat jedoch ihren Preis: die Anbindung an COTS Produkte, Internet, IT, standardisierte Protokolle u.v.m. hat die Verwundbarkeit der Systeme gegenüber Angriffen auf die IT Infrastruktur erst einmal erhöht. Die Dynamisierung der Funktionen der Kontrollzentren hat nicht automatisch und gleichzeitig zur Entwicklung geeigneter Sicherheitsstrukturen für die Kontrollzentren geführt. Angreifer und Verteidiger, Risiken und Schutz, Störung und Abwehr befinden sich in einem ständigen Wettlauf.

## 4. AUSGANGSLAGE, BEDROHUNG UND VERWUNDBARKEIT

### 4.1 AUSGANGSLAGE

Kritische Infrastrukturen wie Energie oder Gas Transport hängen in hohem Maße von Informationssystemen an, um die die Infrastruktur zu steuern und zu kontrollieren. Während viele von ihnen noch auf urheberrechtlich geschützten firmeneigenen Kontrollsystemen beruhen, hat sich doch eine klare Tendenz hin zu standardisierten Kommunikations-Architekturen herausgebildet. Die Einführung neuer, gemeinsam genutzter Protokolle, offener Standard API's (application programming interfaces), Kommunikationsstandards, die in COTS-Produkten implementiert sind, verbessern die Überwachungs- und Kontrollmechanismen sowie die Kommunikation zwischen den Geschäftspartnern im wettbewerbsorientierten Markt. Der scharfe Wettbewerb im Weltenergiemarkt, die über große Entfernungen und Flächen verteilte Energieerzeugung, Verteilungsnetze und Kontrolleinrichtungen, die Zunahme erneuerbarer Energien und die wachsende Abhängigkeit von importierter Energie erhöhen aber auch die Zahl der Akteure und Einrichtungen und damit die Komplexität auf der betrieblichen Ebene der Energieinfrastruktur, um alle erforderlichen Prozesse zu steuern.

Vor diesem Hintergrund hat z.B. das EU-Projekt IRRIS<sup>13</sup> für den Zeitraum 2015+ zwei mögliche Zukunftsszenarien für die Stromversorgung in der EU unterschieden<sup>14</sup>. Szenario 1 setzt mehr auf einen Internet-basierten, offenen, liberalisierten Strommarkt mit zunehmender Ausnutzung von ausgeklügelten, konvergierenden Netzen. Szenario 2 sieht eher einen Konzentrationsprozess auf wenige Stromanbieter mit langsamer Annäherung an Marktliberalisierung vor, die ihre Dienste mehr über proprietäre Netze abwickeln. In beiden Szenarien werden -neben den internen Betriebsaufgaben- Operationen der Kontrollzentren zunehmend von Angebot und Nachfrage

---

<sup>13</sup> IST Project Nr 027568 „Integrated Risk Reduction of Information-based Infrastructure Systems“;  
<http://www.irriis.org/>

<sup>14</sup> D2.1.1 „Report of the Scenario Analysis“; IRRIS

beeinflusst, wobei sich der „Markt-Operator“ als Vertriebsinstanz administrativer Netze bedient, über die die erforderlichen Daten zwischen den Kontrollzentren und (konkurrierenden) Geschäftspartnern ausgetauscht werden.

Generell wird die Energie-Infrastrukturen von vernetzten Kontrollzentren aus über sog. „Industrial Control Systems“ (ICSs) und weitere unterstützende „Information & Communication Technology“ (ICT) Systeme gesteuert und überwacht. Da alle Systeme gleichzeitig mit IT-Systemen zur Unterstützung von Geschäftsprozessen und Management verbunden sind und damit wichtigen Input liefern, sind sie potenziell Opfer möglicher Angriffe. Diese können physischer oder elektronischer Natur sein mit nachfolgenden physischen Auswirkungen, sie können zu Störungen von Geschäftsprozessen, zu Datendiebstahl oder vielfachen Kombinationen anderer Auswirkungen führen.

Die industriellen Steuerungssysteme für kritische Infrastrukturen waren über die Jahre getrennt von den administrativen Netzwerken der Verwaltung und der Geschäftsabwicklung, nicht zuletzt aufgrund von Eigentumsrechten und aus Sicherheitserwägungen. Heute hat sich diese Situation verändert: einerseits wegen der wachsenden Komplexität und der zunehmenden Integration und andererseits wegen der Notwendigkeit zur Verbesserung von Produktions- und Geschäftsprozessen in einer Wettbewerbsumgebung, wo schnelle Kommunikation und Datentransfer kritische Faktoren sind und der Einsatz von Kommunikationsnetzwerken, offenen Technologien und Protokollen zur Steuerung und Überwachung von kritische Infrastrukturen zunehmend erforderlich wird. Auf kostengünstigen Internet Protokollen (IP) basierende Systeme ersetzen zunehmend betriebseigene Lösungen und verbinden analog zu den Informationsnetzen die Steuerungs- und Kontrollsysteme der Infrastrukturen mit der früher getrennten Domäne der Geschäftsprozesse. Das ist attraktiv im Hinblick auf den kostengünstige Gebrauch von Ressourcen, der Optimierung der Abläufe und des Geschäfts, führt aber auch zu hohen Sicherheitsrisiken, denn sie öffnet die Netze externen Bedrohungen, die typisch für IT-Systeme sind.

Ein Beispiel für ein derartiges, modernes, verteiltes industrielles System, das ein elektrisches Netzwerk kontrolliert, zeigt Bild 5. Das Bild zeigt verschiedene Sektoren und Kommunikationsverbindungen zu verschiedenen Partnern eines ICS. Es illustriert die Trennung zwischen der Kontrolle (SCADA LAN) und den administrativen Netzen durch die „Demilitarized Zone (DMZ)“. Auf diese Weise können sichere Daten für Planung und Geschäftsoperationen vom Kontrollnetz in das administrative Netz gelangen. Das SCADA LAN (Local Area Network) enthält u.a. den SCADA Server und die Master Terminal Units (MTU), die Information von den entfernten, unbemannten Terminaleinheiten (RTUs) übermitteln und programmierbare „logic controllers“(PLCs) die in Substations oder anderen Messstationen untergebracht sind.

Die Kommunikation zwischen den RTU's, PLC's und MTU erfolgt –abhängig von der Größe der Anlage – über Wide Area Networks (SCADA MANs/WANs). Das Kontrollzentrum nutzt diese Verbindungen bei der Abfrage der Messstationen nach Daten oder registriert Unterbrechungen, die über das Alarmierungssystem angezeigt werden. Derartige zentralisierte Systeme befähigen den Operator, weiträumig verteilte Systeme zu beobachten und zu kontrollieren sowie Fernwartung oder Reparaturoperation durchzuführen. Die Kommunikation mit anderen Kontrollzentren oder Geschäftspartnern erfolgt über öffentliche oder private WAN's. (Wide area networks).

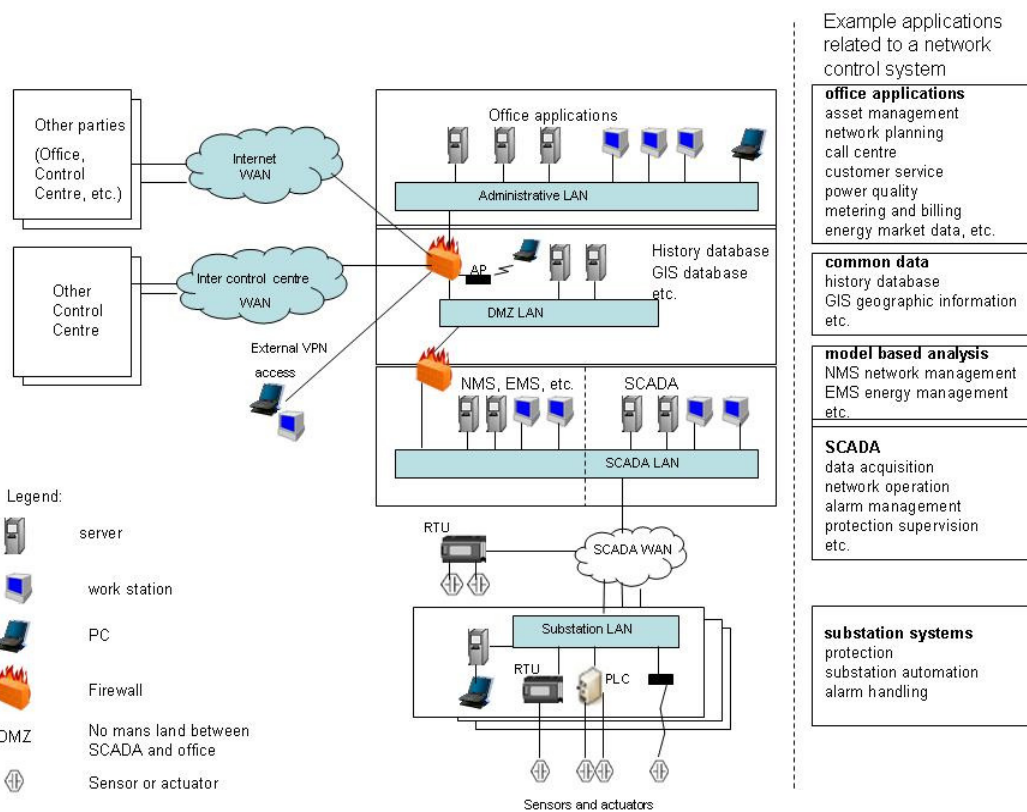


Abbildung 5: Logische Netz Konfiguration<sup>15</sup>

SCADA Systeme sind herausfordernde Ziele für die organisierte Kriminalität oder terroristische Gruppen. Cyber-Terroristen sind heutzutage gut ausgerüstete, trainierte und motivierte Computer- und Software-Experten. Für jeden Angreifer auf die Energieinfrastruktur ist das Kontrollzentrum das beste Angriffsziel. Wenn der Angreifer erst einmal Zugang zum Überwachungs- und Steuerungsnetzwerk bekommen hat, dann kann er die Kommunikation zwischen den SCADA Arbeitsplätzen und den diversen Messstationen überwachen und die Systemprozesse manipulieren und in seinem Sinne nutzen.

Alternativ kann der Angriff auch gegen die unbemannten externen Messstationen des SCADA-Systems gerichtet sein. Häufig ist der physische Schutz dieser Messstationen gering, nicht zuletzt wegen der Kosten aufgrund der großen Zahl von Messstationen und weil man davon ausging, dass die Bedeutung einer einzelnen Station im Falle eines Angriffs gering ist. Diese Meinung erwies sich jedoch angesichts eines zielgerichteten, erfolgreichen Angriffs gegen eine entfernte, unbemannte Messstation als irrig<sup>16</sup>.

<sup>15</sup> © , OCTAVIO, VTT

<sup>16</sup> D. Holstein, J. Tengdin, J. Wack, R. Butler, T. Draelos, P. Blomgren, Cyber Security for Utility Operations, April 2005, [www.sandia.gov/scada/documents.htm](http://www.sandia.gov/scada/documents.htm)

## 4.2 BEDROHUNGEN

In dem Maße, wie sich die Steuerungs- und Überwachungsnetzwerke von „Stand-Alone“ Inseln zu verbundenen Netzwerken in einer IT Umgebung entwickelten, zogen sie die unterschiedlichsten Bedrohungen auf sich. Dieser Trend verstärkte sich, nachdem die industriellen Steuerungs- und Überwachungssysteme zunehmend auf COTS Soft- und Hardware Produkten aufbauten, mit Standard-Protokollen und gemeinsam genutzter Standard Software wie Microsoft Windows. Die Nutzung von COTS Produkten verbesserte zwar die Leistungsfähigkeit bei gleichzeitiger Reduktion der Systemkosten, erhöhte aber gleichzeitig die Wahrscheinlichkeit von elektronischen Angriffen über die standardisierten Schnittstellen. Werkzeuge zur Durchführung derartiger Angriffe sind gemeinhin im Internet verfügbar.

Das Eindringen in spezielle IT - Systeme erforderte früher seitens des Angreifers erhebliche Expertise; heutzutage genügt es, Angriffswerkzeuge (z.B. zum „Knacken“ von Passwörtern) aus dem Internet herunter zu laden. Heute ist für elektronische Standardangriffe ein immer geringeres Expertenwissen erforderlich<sup>17</sup>.

Derzeit sind die am häufigsten vorkommenden Angriffe die schon seit langem bekannten „Denial of service“ (DoS), „Malware Installation“, und „Identity Interception“ (Abfangen der persönlichen Identifizierung). Seit einigen Jahren entwickelt sich mit der „Bot-Installation“ ein neuer Typ von gefährlichen Angriffen. Hierbei handelt es sich um eine Ansammlung schädlicher „Software-Roboter“, die sich selbständig und automatisch in IT Netzen verbreiten. Sie werden von einem sogenannten Bot-Operator gestartet, damit sie in fremde Systeme eindringen –z.B. in das SCADA Netz, dort die Kontrolle für koordinierte und verteilte Angriffe übernehmen oder diese ferngesteuerten Computer als illegale Speicher- und Verarbeitungsgeräte nutzen. Terroristen und organisierte Kriminalität verfügen über die entsprechenden Möglichkeiten, derartige Botnets zu organisieren: Bot -Operatoren bieten „ihre Dienste“ für DoS Angriffe auf bestimmte Server sogar auf dem Schwarzmarkt an.

Zusätzlich zu derartigen aktiven Angriffsmitteln werden auch passive Bedrohungen wie z.B. „Sniffer“ eingesetzt. Es handelt sich hierbei um Software Tools, die in feindlicher Absicht z.B. den Datenverkehr eines digitalen Netzwerks – Festnetz oder Funk - abhören und analysieren. Die gewonnene Information kann später ausgewertet werden, um z.B. Nutzeridents und Passwörterherauszufinden. „Sniffer“ sind nur schwer zu entdecken, weil sie Information nur lesen, aber keine Signale versenden. Abhilfe ist in erster Linie von durchdachten Sicherheitsarchitekturen zu erwarten.

Angriffe gegen SCADA Systeme können vor allem über die offenen oder offeneren administrativen Systeme eines Kontrollzentrums durchgeführt werden. Audits und Analysen nach großen Störfällen wie August 2003 in den USA haben gezeigt, dass Kontrollsysteme häufig mit den administrativen Systemen verbunden waren. Die administrativen Netzwerke waren nur insoweit gesichert, als sie die allgemeinen Geschäftsprozesse unterstützen, nicht aber die sogenannten

---

<sup>17</sup> Allen, J., A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner. 2000. "State of the practice of intrusion detection technologies." Carnegie Mellon University, Software Engineering Institute, CMU/SEI99TR028  
ESCTR99028

„sicherheitskritischen“ Systeme<sup>18</sup>. Kann ein Bot-Operator über eine solche Verbindung auf das Kontrollsystem zugreifen, dann kann er die Kommunikation zwischen der SCADA Workstation und den zu kontrollierenden Anlagen ausspähen und die Steuerungsprozesse in seinem Sinne manipulieren.

Neben derartigen Werkzeugen für „illegale“ Angriffe gibt es auch elementare „technische“ Möglichkeiten, die für kriminelle Zwecke genutzt werden können, wenn sie unsachgemäß gehandhabt werden, wie z. B. technische Spezifikationen für Systemkomponenten und Geräte, Wartungshandbücher, Handbücher zur Störbehebung und zum Konfigurationsmanagement und v.a.m.. Die Kenntnis dieser Mittel ist Grundlage für vielfältige Angriffe.

### 4.3 VERWUNDBARKEIT

Obwohl die verschiedenen Bereiche eines umfassenden Steuerungs- und Überwachungssystems sowie die verschiedenen Netzwerke (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**), die diese Bereiche miteinander verbinden, unterschiedliche IT Protokolle und Standards nutzen, gleichen sich die verschiedenen IT Systeme im Prinzip hinsichtlich ihrer Verwundbarkeit. Damit sind sie gleichermaßen anfällig für bestimmte Bedrohungen und Angriffe. Ursache dafür ist u.a. die schon angesprochene Standardisierung; neben COTS Soft- und Hardware sind die Kommunikationsprotokolle ebenfalls standardisiert und Schutzvorkehrungen wie „Firewalls“ und „Intrusion Detection Systeme“ (IDS), sind häufig „open source“ und „commercial-off-the shelf“ –d.h. das Wissen, wie Stärken und Schwächen solcher Systeme ausgenutzt werden können, ist damit im Grunde bereits vorhanden, unabhängig von dem beispielloses Anwachsen des kriminellen Know-hows, das in der Lage ist, Schwachpunkte von Sicherheitsstrukturen zu erkennen und auszunutzen. Mängel und Schwächen im Sicherheitsmanagement machen deshalb Kontrollzentren und ihre Betriebs- und Kommunikationsnetze gegenüber potenziellen Bedrohungen anfällig.

Mit Hilfe umfassender Sicherheitsarchitekturen und der dafür verfügbaren Verfahren und Werkzeuge ist es jedoch möglich, die meisten Bedrohungen abzumildern. Dies ist allerdings keine einfache Aufgabe, insbesondere, weil sich die Cyberumgebung und als Folge daraus die Art der Angriffe ständig ändern. Angesichts dieser Tatsache nehmen sich verschiedene, weltweite Initiativen der Sicherheitsproblematik an, wie z.B. die IEC<sup>19</sup> (International Electrotechnical Commission), die sich in verschiedenen Arbeitsgruppen mit Fragen der sicheren Kommunikation in industriellen Netzwerk und mit der Herausgabe relevanter Standards wie IEC/TS 62351 befasst. Andere Gruppen sind das NIST (National Institute of Standards and Technology), das u.a. zur Sicherheit Industrieller Kontrollsysteme (ICS) entsprechende Dokumente veröffentlicht, oder die ISA (Instrumentation, Systems, and Automation Society) mit Anleitungen und Standards [ISAS99] zur Einführung von IT Sicherheit in vorhandene industrielle Kontroll- und Automationssysteme. Die Sicherheitsarchitekturen, die von den verschiedenen Foren vorgeschlagen werden, fordern eine strikte Trennung über „Sicherheitsbrücken“ zwischen den Steuerungs- und Überwachungssystemen, den firmen-internen administrativen Netzen und externen Verbindungen.

---

<sup>18</sup> NIST SP 80082,  
Guide to Industrial Control Systems (ICS) Security, Draft

<sup>19</sup> [www.iec.org](http://www.iec.org)

Die Entwicklung des künftigen Europäischen Stromverbundes trägt dem im Prinzip mit der Vernetzung der Administrations-, Kontroll- und Betriebsnetze über IP Netze mit Schnittstellen nach außen oder über intern gekapselte Netz, die die IP Technologie einsetzen, Rechnung. Vor und verstärkt nach dem großen Blackout hatte es in den USA Bemühungen gegeben, die unmittelbare Kopplung von administrativen und Steuerungs- und Überwachungsnetzen-Netzen einzuschränken oder gar gesetzlich zu unterbinden. Diese waren zwar nicht die eigentliche Ursache der großen Störung 2003, aber im Zuge der Untersuchungen wurde die Verkoppelung bereits als große Schwachstelle festgestellt, (ebenso wie Verstöße gegen existierende Auflagen). Es wird abzuwarten sein, ob es hierzu national und /oder auf EU-Ebene entsprechende Regulierungen geben wird.

Die Technik physischer Angriffe hat sich trotz der Veränderungen bei Prozessen, Transport- und Administrationsnetzen, Leitungen, Strukturen und Ausrüstungen im Prinzip nur wenig verändert, die Auswirkungen von Angriffen sind aber infolge der komplexeren Struktur der Kontrollzentren gravierender geworden<sup>20</sup>. Im Gegensatz dazu ist wegen der mit der IT-Entwicklung einhergehenden Vermehrung der Funktionalitäten der Kontrollzentren und der daraus resultierenden Anforderungen an die Überwachungs- und Kontroll-, Kommunikations- und administrativen Netzwerke die "Cyber" Bedrohung gegen die IT Infrastruktur potenziell größer geworden und damit die Verwundbarkeit der Kontrollzentren nach Qualität, Vielfältigkeit und Quantität aus den angeführten Gründen erheblich angewachsen! Die Möglichkeiten von gekoppelten Angriffen, die elektronische Angriffe mit physischer Gewalt verbinden, erhöhen zusätzlich die Bedrohung und die daraus resultierende Systemverwundbarkeit und stellen weitere Anforderungen an ein integriertes Sicherheitskonzept.

## 5. SICHERHEITSANFORDERUNGEN

Es ist eine Binsenwahrheit: Kontrollzentren sind umso verwundbarer, je leichter ein Angreifer über Schwachstellen in das System eindringen kann. Derartige Schwachstellen sind z.B.:

- Unzureichende Bestimmungen für Authentifizierung und Zugriffskontrolle
- Fehlende oder zu einfache Verschlüsselung
- Nicht vorschriftsgemäße Konfiguration der Sicherheitseinrichtungen wie z.B. Firewalls oder demilitarisierte Zonen (DMZ) etc.
- Überholte Programme gegen Viren, Trojaner etc.

Im Folgenden soll beispielhaft auf einige potenzielle Schwachstellen hingewiesen werden, die im Rahmen eines integrierten Sicherheitskonzeptes minimiert bzw. eliminiert werden müssen

### 5.1 REGELUNGEN FÜR AUTHENTIFIZIERUNG UND ZUGRIFFSKONTROLLE

Da einige Kontrollprotokolle keine Authentifizierungsmechanismen nutzen, muss eine Zugangsregelung („User Access Control Policy“) eingeführt werden, die einen unbefugten Fernzugriff („Remote Access“) zum Kontrollsystem verhindert, indem sie festlegt, wer, wann, welches Password nutzt und wie die Passwörter zu verwalten sind. Es kommt vor, dass Passwörter zu Netzwerkeinrichtungen einer Gruppe von Personen und nicht einem einzigen Individuum zugeordnet sind, was zu Missbrauch verführen kann. Ein sauber konfiguriertes Zugangssystem teilt nur *die* Privilegien zu, die eine Person zur Ausübung ihrer Aufgabe auch

---

<sup>20</sup> Siehe OCTAVIO-Bericht: „Energy Systems Cyber Security

wirklich benötigt. Es versteht sich von selbst, dass Passwörter häufig gewechselt werden müssen. Es ist bekannt, dass unzureichende Regelungen für Authentifizierung und Zugriffskontrolle bei Wartungsarbeiten eine ernste Sicherheitslücke darstellen: in vielen Fällen führen Produktlieferanten oder ihre Beauftragten unkontrolliert Wartungsarbeiten unter Umgehung aller Firewalls durch!

Das Sicherheitskonzept sollte auch die Regeln definieren, die im Falle eines Notfalles zur Anwendung kommen sollen, um die dann erforderliche, verzugslose Kommunikation zwischen bestimmten Parteien zu ermöglichen.

## 5.2 VERSCHLÜSSELUNG

Fehlende oder zu einfache Verschlüsselungsmethoden für schutzbedürftige Passwörter und Daten, die zwischen unterschiedlichen Parteien ausgetauscht werden, können durch Sniffers oder Phishing ausgenutzt werden.

Bei der Anwendung von Verschlüsselungsmethoden müssen folgende Aspekte beachtet werden:

- a) Kontrollsysteme sind oft auf ganz bestimmte Plattformen zugeschnitten, die u.U. nicht über das erforderliche Leistungsvermögen verfügen, um auch noch Verschlüsselungsoperationen durchführen zu können. Das kann dadurch kompensiert werden, dass die Sicherheitsfunktionalität in eine eigene Sicherheitseinheit außerhalb des Kontrollsystems verlegt wird. Zwei Vorteile sind damit verbunden. Zum einen werden dadurch kurzlebige Sicherheitsfunktionen von langlebigen Kontrollfunktionen getrennt und zum anderen verleiht diese Trennung im Falle eines Angriffes einen zusätzlichen Schutz, weil die Angriffseffekte auf die Sicherheitseinheit beschränkt bleiben und nicht die Kontrollfunktionen beeinträchtigen.
- b) Der zweite Aspekt ist das Timing. Ver- und Entschlüsselung von Daten kostet Zeit und verursacht Verzögerungen bei der Übertragung von Meldungen. In einigen Situationen können zusätzliche Wartezeiten und die damit verbundene reduzierte Betriebsüberwachung kritisch sein. Obwohl bereits heute hinreichend mächtige Verschlüsselungsmethoden mit sehr kurzen Wartezeiten verfügbar sind, werden sie nicht immer bedarfsgerecht genutzt.

## 5.3 KONFIGURATION VON FIREWALLS

Da in vielen Fällen Kontroll- und Unternehmensnetz physisch nicht getrennt sind, ist eine klare logische Trennung von beiden unumgänglich, was mittels DMZ<sup>21</sup> (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**) geschehen kann. Eine DMZ trennt beide Netze durch Firewalls. Allerdings müssen die Firewalls sauber konfiguriert sein, um nur berechtigten Servern und Diensten von ganz bestimmten Knoten aus Zugriff zu gewähren. Auf diese Weise soll verhindert werden, dass Schadprogramme und nicht erforderliche Daten zwischen den beiden Netzen ausgetauscht werden. Die Konfigurationsregeln müssen häufig überprüft werden, um auf veränderte Bedrohungen reagieren zu können. Die Überwachung der Firewalls versetzt das System in die Lage, Angriffe zu entdecken und auf sie entsprechend zu reagieren. Zusätzliche Sicherheit kann erreicht werden, wenn für die Firewalls verschiedene Lieferanten und unterschiedliche Konfigurationsregeln ausgewählt werden.

---

<sup>21</sup> Demilitarized zone

## 5.4 VIRENSCHUTZ

Antivirenprogramme in Kontrollsystemen sind nicht immer auf dem neuesten Stand und machen so das System für neue Bedrohungen anfällig. Allerdings gibt es auch Argumente gegen IDS<sup>22</sup>, wenn deren Output zu Konfusion und zusätzlichem Stress beim Bedienpersonal führt. So kann zum Beispiel eine Fehlfunktion irgendwo in der zu überwachenden Anlage das automatische Schutzsystem veranlassen, kaskadierende Alarme abzusetzen, die das IDS wiederum als ungewöhnliche Vorkommnisse interpretiert und dann seinerseits Alarm auslöst. Das kann zu zusätzlicher Verwirrung des Bedienpersonals beitragen und verhindern, dass das Bedienpersonal rechtzeitig die kritische Information aus der Fülle der Alarme herausfiltert und geeignete Gegenmaßnahmen ergreift. Der Kaskadeneffekt kann schließlich zum Blackout führen.

Ein bewährtes Mittel zur Verhinderung von bösartiger Software wäre, an jedem Host einen Scanner im Hintergrund laufen zu lassen, der jeden neu heruntergeladenen File hinsichtlich bösartiger Software überprüft. Aus Effizienzgründen mag dies nicht an jedem Host möglich sein. In diesen Fällen kann eine strikte Kontrolle der Übertragungswege, auf denen Schadprogramme in das System gelangen können, den notwendigen Schutz gewähren. Alle Datenträger wie z.B. CDs, Memory Sticks oder Notebooks sollten an einer festgelegten Überprüfungsstelle, die nicht Teil des Kontrollsystems ist, auf Viren überprüft werden, bevor sie für die Nutzung im Kontrollsystem freigegeben werden.

## 5.5 WEITERE ANFORDERUNGEN

Es würde den Rahmen dieses Artikels sprengen, auch nur ansatzweise auf alle Sicherheitsaspekte von Kontrollzentren eingehen zu wollen. Sicherheitslücken bzw. Anforderungen, die beispielhaft für die IT Systeme des Energienetzwerkes dargestellt wurden, sind im Einzelnen auch für deren Teilsysteme wie z.B. SCADA LAN<sup>23</sup>, SCADA Messstationen, Demilitarized Zones und die Verbindungen zum administrativen Netz, das Kommunikation mit den entfernt liegenden Funktionseinheiten u.s.w. zu analysieren. Derartige Analysen bleiben jedoch Stückwerk, wenn sie nicht in den Rahmen eines integrierten Sicherheitskonzeptes eingeordnet werden. Angriffe gegen Kontrollsysteme haben z.B. gezeigt, dass die einzelnen Schutzmechanismen allein noch keinen hinreichenden Schutz gegen fachkundige Angreifer aufweisen. Ein Grund dafür ist oft die unzureichende Einteilung der Schutzmechanismen in Sicherheitsebenen und -zonen. Typischerweise umfassen Überwachungs- und Steuerungssysteme sowohl WAN<sup>24</sup> als auch LAN Kommunikation zwischen den verschiedenen Sicherheitszonen (administratives Netz und Kontrollnetz) und funktionalen Ebenen („Layern“). Es ist wichtig, dass eine derartige Struktur nicht zu viele Interdependenzen zwischen den funktionalen Ebenen schafft. Kontrollsysteme wie die SCADA Systeme, die über IP Netzwerke laufen, sind Teil des sog. „OSI-Layer Modells“. Dieses „Open System Interconnection Reference Model“ (OSI), besteht aus mehreren funktionalen Ebenen („Layern“), wie z.B. einer „physikalischen“ Ebene, einer „Netzwerk“-Ebene, einer „Transport“-Ebene u.s.w. Das OSI-Modell bildet den Datenverkehr in Kommunikationsnetzwerken ab, wobei die einzelnen Ebenen die verschiedenen Kommunikationsebenen zwischen Software und Hardware darstellen. Die insgesamt sieben Ebenen des OSI Modells können durch unterschiedliche Standards und

---

<sup>22</sup> Intrusion Detection System

<sup>23</sup> Local Area Network

<sup>24</sup> Wide Area Network

Protokolle realisiert sein. Jede Ebene des Modells bietet den benachbarten Ebenen bestimmte Dienstleistungen an.

Ein effektives Netz hängt von dem problemlosen Funktionieren aller Ebenen ab. Physische Störungen können aus Beschädigung oder Zerstörung der Hardware (Geräte und Kabel) resultieren, logische Fehler haben ihre Ursache in administrativen Eingriffen oder Cyber Angriffen. Wenn *eine* Ebene nicht mehr funktionsfähig ist, ist i.d.R. die Kommunikation durchgehend gestört.

Bei der Entwicklung eines integrierten Sicherheitskonzeptes würde ein Betreiber wegen der zentralen Bedeutung der SCADA Systeme bei einem neu zu entwickelnden Kontrollzentrum zuerst die SCADA Infrastruktur aufbauen und die anderen komplexen Netzwerke für Aufgaben wie Stromerzeugung, Transport, Zählermessungen und Gebührenerfassung ergänzen, um die Sicherheit im Kern des Netzwerks zu gewährleisten. Doch in der Regel ist ein Kontrollzentrum Ergebnis eines stetigen Weiterentwicklungsprozesses oder einer Integration von zwei oder mehreren etablierten, historisch gewachsenen Systemen. Die laufende Gewährleistung der Sicherheit von Kontrollsystemen der Energieversorgung <sup>25</sup> beruht deshalb grundsätzlich auf

1. der laufenden Überprüfung des übergreifenden Sicherheitskonzeptes
2. vorausschauender Entwicklung und Integration von Schutzmaßnahmen
3. der Aufspürung von Intrusionsversuchen und der Implementierung von Antwort-Strategien.
4. laufender Ausbildung und Training der Mitarbeiter im Hinblick auf Erkennen und Einschätzen möglicher Bedrohungen und einem angemessenen Reaktionsverhalten.

Energiekontrollzentren haben sich von einem Hilfsinstrument zur Überwachung von Stromerzeugung und Verteilung zu einer zentralen Einrichtung der Energieversorgung für die Gesellschaft entwickelt. Ihre Sicherheit gegenüber kriminellen und terroristischen Angriffen trägt ganz wesentlich zur Sicherheit der Stromversorgung von Bürgern und Wirtschaft bei. Zur Erreichung dieses Ziels ist auch die Intensivierung eines umfassenden, interdisziplinären und institutionalisierten Erfahrungsaustauschs und der internationalen Zusammenarbeit über aktuelle und neue Bedrohungen sowie der Austausch neuer Schlüsseltechnologien zur Stärkung der Sicherheit von Kontrollzentren (und natürlich darüber hinaus) auf nationaler und europäischer erforderlich!

In ihrer „*Mitteilung ... an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen*“<sup>26</sup> fordert deshalb die Europäische Kommission einen besser strukturierten Austausch von Informationen und eine Stärkung der Kooperationsmechanismen zum Schutz vor elektronischen Angriffen gegen kritische Informationsinfrastrukturen! Am 27. und 28.4.2009 trat eine Ministerkonferenz zu entsprechender Beschlussfassung zusammen.

---

<sup>25</sup> US Department of Energy, 2006, National SCADA Test Bed, DOE Visualization & Controls, [www.oe.energy.gov/DocumentsandMedia/CSS\\_Peer\\_Review\\_Intro\\_HK\\_Final.pdf](http://www.oe.energy.gov/DocumentsandMedia/CSS_Peer_Review_Intro_HK_Final.pdf), S. 10.

<sup>26</sup> „Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität“; 1.Quartal 2009

***Karl Adolf Neubecker,***

studierte in Gießen und Freiburg Mathematik und Physik. In seinem Berufsleben bearbeitete er Problemstellungen aus den Bereichen Verteidigung, Sicherheit und Krisenmanagement. Seit 2007 ist er als freier Mitarbeiter im Centrum für Europäische Sicherheits-Strategien (CESS) mit der Erarbeitung von Szenarien, der Analyse von kritischen Infrastrukturen sowie der Entwicklung und Durchführung von Planübungen für Training, Ausbildung und Krisenmanagement befasst.

***Walter Schmitz,***

Herr Schmitz studierte Mathematik und Physik an der Universität in Saarbrücken sowie Volks- und Betriebswirtschaft in Nürnberg. Sein Arbeitsgebiet ist Operation Research sowie Entwicklung von Planungs- und Simulationsmodellen zur Untersuchung von komplexen Sicherheitsfragen und kritischer Infrastrukturen. Produkte dieser Tätigkeit waren Planspiele, Simulationen, Zukunftsszenarien und Beratung.

***Thomas Beer,***

studierte Internationale Beziehungen, Völkerrecht, Soziologie und Rechtswissenschaften. Nach seinem Studium arbeitete er als Analyst in den Gebieten IT- Sicherheit, Notfallplanung und Schutz kritischer Infrastrukturen. Er war an mehreren EU Forschungsrahmenprogrammen beteiligt. Er ist gegenwärtig Programmmanager für CESS.