# Internet Science – Critical Infrastructures

Caterina Wanka
Betreuer: Dr. Heiko Niedermayer
Seminar Future Internet WS2014/15
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: caterina.wanka@tum.de

## KURZFASSUNG

Kritische Infrastrukturen versorgen uns mit dem Wasser, das wir trinken, dem Strom, welchen wir im Alltag benötigen, den Transportmitteln, welche uns zur Arbeit bringen, und den Kommunikationssystemen, über welche wir mit Freunden und Familie in Kontakt bleiben. Insbesondere Energieversorgungssysteme sind in der heutigen Gesellschaft von großer Bedeutung. Eine Störung oder ein Ausfall dieses Systems kann katastrophale Auswirkungen mit sich ziehen. Insbesondere Stromnetze verdeutlichen die Komplexität und Vielfältigkeit kritischer Infrastrukturen. Auf Grund ihrer Bedeutung in unserer heutigen Gesellschaft sind sie oft Zielscheibe von Angriffen unterschiedlichster Art. Jedoch gibt es eine Vielzahl von Schutzmaßnahmen, welche schädigenden Ereignissen entgegenwirken können.

## Schlüsselworte

Kritische Infrastruktur – Energieversorgungssystem –Informations- und Kommunikationstechnik (IKT) – Critical Infrastructure Protection (CIP) – Cyber-Sicherheit

## 1. EINLEITUNG

"[Critical infrastructures] are the foundations of our prosperity, enablers of our defense, and the vanguard of our future. They empower every element of our society. There is no more urgent priority than assuring the security, continuity, and availability of our critical infrastructures." [1]

Moderne Industrienationen sind auf komplexe Infrastrukturen angewiesen. Wirtschaft und Gesellschaft funktionieren nur, wenn die grundlegende Versorgung gesichert ist. Ein Ausfall oder eine Manipulation und Beeinträchtigung dieser Systeme über einen längeren Zeitraum oder auf einer größeren Fläche würde weitreichende Folgen nach sich ziehen. Deswegen stehen kritische Infrastrukturen und im besonderen Maße deren Schutz weltweit im Mittelpunkt nationaler Regierungsaktivitäten.

Die Energieversorgung ist ein zentraler Bereich kritischer Infrastrukturen, da das Energieversorgungssystem neben seiner weiten geographischen Verbreitung, zudem der Schlüssel zu den meisten sozialen Aktivitäten ist. Ausfälle oder Störungen des Energieversorgungssystems würden sich extrem und unmittelbar auf die anderen Sektoren und somit auf Staat, Wirtschaft und Gesellschaft auswirken.

Diese Arbeit schafft einen Einblick in die Thematik ‚Kritische Infrastrukturen'. Am Beispiel des Sektors der Energieversorgung werden die Akteure und deren Zusammenspiel im System kritischer Infrastrukturen näher untersucht. Daran anknüpfend wird ein Überblick über die ‚Critical Infrastructure Protection' verschafft, indem Ursachen für das Scheitern von kritischen Infrastrukturen untersucht und abschließend Schutzmaßnahmen vorgestellt werden.

## 2. WAS SIND KRITISCHE INFRASTRUKTUREN?

Der Begriff ‚Kritische Infrastrukturen' ist in der Wissenschaft, wie auch in der Politik vieldiskutiert. Auf Grund des weitreichenden Begriffsumfangs wird im Folgenden zusätzlich zu einer reinen Begriffsbestimmung auch eine Einteilung der zu untersuchenden Systeme in Sektoren vorgenommen.

### 2.1 Definition

Unterschiedliche Ansätze und Interpretationen führen zu unterschiedlich weitgreifenden Definitionen, weswegen eine unabhängige Untersuchung der beiden Worte ‚kritisch' und ‚Infrastruktur' sinnvoll erscheint, um schließlich zu einer umfassenden Definition zu gelangen.

**Infrastruktur**: Eine Infrastruktur ist die Gesamtheit an Elementen, welche zur Ausführung einer bestimmten Dienstleistung notwendig ist. Folglich ist es von der Perspektive abhängig, welches System für ein anderes eine Infrastruktur darstellt. Infrastrukturen können auch innerhalb von anderen Infrastrukturen existieren. Dieser Ansatz lässt sich gut anhand der beiden Systeme Energieversorgung und Informations- und Kommunikationstechnik erklären. Vereinfacht gesagt benötigt Stromübertragung Netzwerke und Netzwerke benötigen andererseits Strom. Aus Sicht des jeweiligen Systems stellt das andere wiederum Teil seiner Infrastruktur dar. Für diese Arbeit wird auf Grund der gesellschaftspolitischen Relevanz des Themas von der abstrakten Perspektive eines Staates ausgegangen. Obwohl jede Regierung den Rahmen zu betrachtender Objekte unterschiedlich definiert, erkannte die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), dass die meisten Staaten den Begriff ‚Infrastruktur' aus einer eher weiten Perspektive betrachten[2]. Aus dieser Sicht umfasst der Begriff physische Objekte, wie zum Beispiel Telefonleitungen, Stromnetze und Gasleitungen. Hinzu kommen kritische Informationsinfrastrukturen. Diese umfassen wiederum physische Systeme, unter anderem bestehend aus Highspeed- oder Breitbandnetzwerken. Der andere Teil umfasst die immaterielle Komponente, in Form von Daten und Software, welche eingebettet in Computersystemen, physische Infrastrukturen bedienen.


doi: 10.2313/NET-2015-03-1_09

**Kritisch**: ‚Kritisch' sind Infrastrukturen für einen Menschen, sobald sie ernstzunehmend für die Erhaltung seiner Lebensqualität notwendig sind. Das heißt, gegensätzlich betrachtet, bei dessen Ausfall das Leben eines Menschen gefährdet wäre oder geschädigt werden würde. Aus Sicht eines Staates sind folglich Infrastrukturen ‚kritisch', sofern sie einen essentiellen Beitrag zum wirtschaftlichen und sozialen Gemeinwesen des Landes leisten. Das bedeutet, sobald bei deren Ausfall oder Beeinträchtigung nachhaltig und/ oder weitreichend wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Schäden eintreten würden[3], wird eine Infrastruktur auf nationaler Ebene als ‚kritisch' eingestuft.

Auf Grund der sozialpolitischen Relevanz dieses Begriffs haben viele Staaten eigene Definitionen beziehungsweise Beurteilungskriterien formuliert, die im Rahmen ihrer nationalen Schutzprogramme für kritische Infrastrukturen verwendet werden. Die Vereinigten Staaten zum Beispiel bezeichnen kritische Infrastrukturen als Systeme oder Güter, physisch oder virtuell, welche für die Vereinigten Staaten dermaßen entscheidend sind, dass eine Störung beziehungsweise Zerstörung dieser Systeme und Güter eine lähmende Auswirkung auf die nationale Sicherheit mit sich ziehen würde[4]. Damit legen sie den Fokus auf den Schutz der nationalen Sicherheit und bewerten den Einfluss einer Infrastruktur auf das Gemeinwesen nach dem Maß der Auswirkungen auf ihre nationale Sicherheit. Empfehlenswert ist es zudem den Ansatz von der entgegengesetzten Seite zu betrachten und ein Gut oder einen Service als kritisch zu betrachten, sobald sie für die Aufrechterhaltung von lebenswichtigen sozialen Funktionen essentiell sind.

Somit wird der Grad an Bedeutung einer Infrastruktur nicht an den hypothetischen Auswirkungen im Falle eines Ausfalls, sondern an dem Beitrag zum nationalen Gemeinwesen gemessen. Beide Herangehensweisen führen im Durchschnitt zu den gleichen Ergebnissen, jedoch lassen sich durch die letztere mehr unterstützende Funktionen kritischer Infrastrukturen in die Betrachtungsweise mit aufnehmen.

## 2.2 Sektoreinteilung

Auch eine Einteilung kritischer Infrastrukturen in Sektoren ist Aufgabe der Regierung und folglich sind auch hier eine Vielzahl an unterschiedlichen Ansätzen vorzufinden. Kanada unterteilt kritische Infrastrukturen zum Beispiel in zehn Branchen, die Vereinigten Staaten dagegen haben achtzehn Sektoren. Alles in allem sind die Einteilungen trotz unterschiedlicher Anzahl an Sektoren vergleichbar. Als Ansatz für diese Arbeit dient die Einteilung des deutschen Bundesamts für Bevölkerungsschutz und Katastrophenhilfe[5] in neun Sektoren:

- Energie
- Gesundheit
- Staat und Verwaltung
- Ernährung
- Transport und Verkehr
- Wasser
- Finanz- und Versicherungswesen
- Informationstechnik und Telekommunikation
- Medien und Kultur

Hervorzuheben ist insbesondere der Bereich der Informationstechnik und Telekommunikation (IKT). Wie bereits im Rahmen der Definition erläutert, nennt man diesen Teilbereich der jeweiligen Sektoren kritischer Infrastrukturen in der Wissenschaft auch ‚kritische Informationsinfrastruktur'[6]. Auf eine solche Betrachtung wird in den meisten Ländern verzichtet. Ein beliebter Ansatz von Staaten ist die Zuordnung des Gefüges kritischer Informationsinfrastrukturen in den Sektor der IKT, welcher in engen Interdependenzen zu den restlichen Sektoren steht. Die zunehmende Durchdringung aller Lebens- und Arbeitsbereiche durch IKT bestimmt jedoch maßgeblich unseren technologischen Fortschritt und lädt zu einer Betrachtung der Informationsinfrastruktur als Teilbereich der einzelnen Sektoren ein. Ein Paradebeispiel hierfür ist das Energieversorgungssystem. Informationsinfrastrukturen stellen hierbei die Schnittstelle dar, welche im Rahmen der Kooperation und Koordination der miteinander verbundenen Stromnetze die Kommunikation und den Datenaustausch untereinander ermöglichen.

# 3. STRUKTUR UND FUNKTIONSWEISE VON KRITISCHEN INFRASTRUKTUREN

Die wachsende Vernetzung von Dienstleistungen, Infrastrukturen und Prozessen hat zur Folge[7], dass weite Bereiche des gesellschaftlichen und wirtschaftlichen Lebens von funktionierenden, robusten Infrastrukturen abhängig sind.

Stromnetzsysteme bestehen heutzutage aus einer Vielzahl an aufeinander wirkenden nationalen Systemen. Diese sind vorwiegend über weite geographische Gebiete miteinander verbunden. Am Beispiel des europäischen Netzes betrifft dies sogar den gesamten Kontinent. Kontroll- und Kommunikationszentralen dienen zum Austausch von Daten und Anweisungen zwischen den regional und national abgegrenzten Netzsystemen. Die Elemente innerhalb der Stromnetzsysteme lassen sich folglich, wie in Abbildung 1 verdeutlicht, laut den Wissenschaftlern Negenborn, Lukszo und Hellendoorn[8] in drei Ebenen einordnen:

- **Physische Ebene**: Energieerzeugung und -übertragung
- **Entscheidungsebene**: Organisatorische und menschliche Entscheidungen
- **Cyber-Ebene**: Übertragung von Informationen und Befehlen

## 3.1 Physische Ebene

In Stromnetzen besteht die physische Ebene aus der Netzwerkhardware. Das Joint Research Centre des Institutes für Energie und Transport[9] beschreibt diese als Anordnung technischer Bauelemente, welche interagierend den Prozess von der Stromerzeugung bis hin zur Lieferung des Stroms an den Endverbraucher realisieren.

Der Energiefluss ist unidirektional: von den zentralisierten Erzeugern bzw. Kraftwerken hin zu den Verbrauchern, welche sich auch nach ihrer Menge an verbrauchtem Strom unterscheiden lassen. Dieser Prozess kann in vier Subsysteme unterteilt werden. Abbildung 1 veranschaulicht im oberen Bereich (‚Physical Layer') eine vereinfachte Struktur eines Elektrizitätsnetzwerkes bestehend aus vier Spannungsebenen[10]:


doi: 10.2313/NET-2015-03-1_09

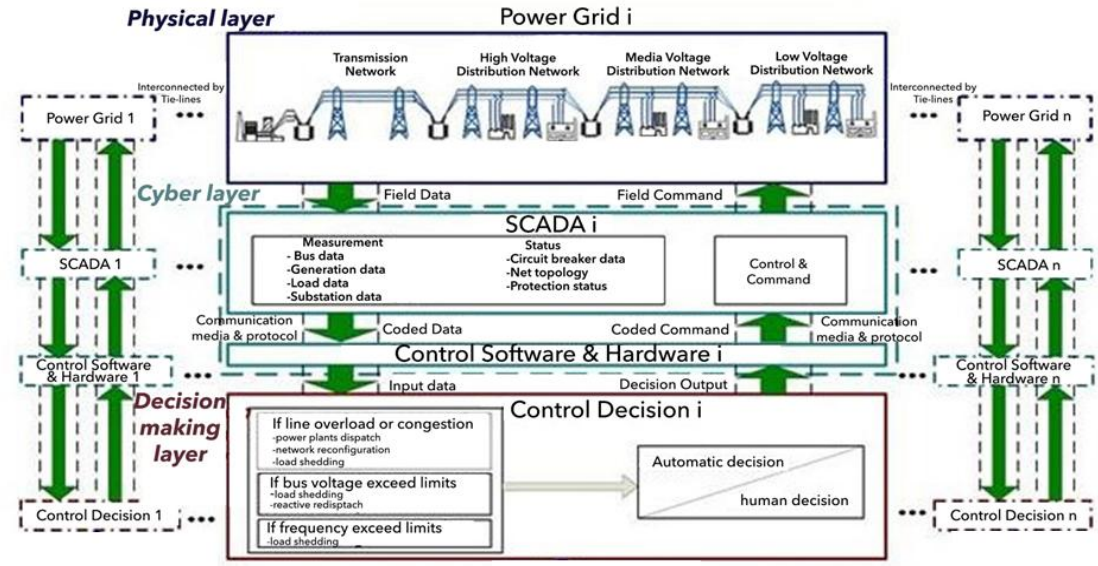


**Abbildung 1. Die drei Ebenen des Energieversorgungssystems [8]**

Dem Übertragungsnetz (Höchstspannungsnetz HÖS), dem Hochspannungsnetz (HS), dem Mittelspannungsnetz (MS) und dem Niederspannungsnetz (NS).

Die Übergänge zwischen den verschiedenen Spannungsebenen werden durch Transformatoren (Aufwärts- beziehungsweise Abwärtstransformatoren) in Umspannwerken oder Ortsnetzstationen realisiert.

Die Stromerzeugung findet heutzutage überwiegend in großen Kraftwerken, wie zum Beispiel Kohlekraftwerken oder Atomkraftwerken, statt. Ressourcen hierfür sind[11] vorwiegend Kohle und Kernenergie. Ein konstant wachsender Anteil der Stromerzeugung besteht zudem aus erneuerbarer Energie, welche in Windkraftanlagen, Solaranlagen etc. erzeugt wird. Der Betrieb in den Kraftanlagen wird zentral überwacht und die Einspeisung der erzeugten Energie in das Stromnetz koordiniert.

Über Aufwärtstransformatoren wird die erzeugte Energie in das Übertragungsnetz (‚Transmission Network') verbreitet. Auf der Höchstspannungsebene können lediglich Großkraftwerke mit Leistungen bis zu 700 MW einspeisen, kleinere Kraftwerke sowie Windkraftanlagen speisen auf Hoch- und Mittelspannungsebene ein.

Über die Höchstspannungsebene ist das deutsche Stromnetz einerseits in das europäische Verbundnetz UCTE (Union for the Coordination of Transmission of Electricity)/ ENTSO-E (European Network of Transmission System Operators for Electricity) für Mittel- und Südeuropa eingebunden. Darüber hinaus hat es über Hochspannungsleitungen Verbindungen in das skandinavische Verbundnetz NORDEL[10]. Zudem gibt es einige industrielle Verbraucher, die auf Grund der großen Menge an benötigtem Strom direkt über das Übertragungsnetzwerk versorgt werden.

Abwärtstransformatoren wandeln den Strom auf eine niedrigere Spannungsebene um, um ihn in das Verteilnetzwerk (‚Distribution Network') zu übertragen.

Die Vielzahl an Stromleitungen werden durch Knoten, sogenannte ‚Busse', miteinander verbunden. Im HS werden diese Busse durch Umspannwerke verkörpert. Umspannwerke wandeln folglich nicht nur den übertragenen Strom in eine niedrigere Spannungsebene um, sondern sind generell für die Kontrolle und Regulierung der Stromflüsse zwischen den Leitungen verantwortlich. Die Versorgungssysteme werden übergeordnet von einer nationalen Aufsichtsbehörde reguliert. Auf europäischer Ebene wurden die unterschiedlichen nationalen Vorschriften durch die ENTSO-E angepasst. Bezüglich des Verantwortungsbereichs identifizierten die Wissenschaftler Bompard et al.[12] Konsequenzen vor allem im Bereich der Busse. Folglich lassen sich diese ‚Übertragungsknoten' im Hinblick auf ihre Zugehörigkeit und ihres physischen Verhaltens in vier Kategorien unterteilen:

Busse des Übertragungsnetzwerkes werden durch sogenannte Transmission Stations (TS) verkörpert, welche direkt dem Transmission System Operator (TSO), dem sogenannten Übertragungsnetzbetreiber, angehören und durch diesen betrieben werden.

Power Plants (PP) sind Kraftwerke, welche verschiedenen, untereinander stark konkurrierenden Unternehmen angehören. Ein Unternehmen kann mehrere Kraftwerke besitzen, welche nicht an denselben Bussen des Netzwerkes angebunden sein muss.

Ein weiterer Bus-Typ sind die Distribution System Feeders (DS). Durch diese Busse können Betreiber über ein abgegrenztes Verteilnetzwerk als Monopolist verfügen.

Von Large Users (LU)-Bussen werden Verbraucher direkt versorgt, sobald ihre Nachfrage an Strom über 5 MW liegt.

Der Mensch ist als Akteur an sich auf physischer Ebene nicht direkt für den Betrieb eines modernen Stromnetzes notwendig. Neben automatisierten Vorrichtungen ist er in diesem Bereich zum Beispiel für die Ausführung von Wartungsarbeiten an den Elementen des Energieversorgungssystems zuständig.


doi: 10.2313/NET-2015-03-1_09

## 3.2 Entscheidungsebene

Der Betrieb von Kraftwerken wird auf der höchsten Ebene durch einen Layer der Entscheidungsfindung bewerkstelligt. Die Entscheidungsebene umfasst die organisatorischen und menschlichen Entscheidungen[8], welche den Betriebsablauf des Stromnetzsystems betreffen. Charakterisierend hierfür ist das Zusammenspiel automatischer Kontrollinstanzen und menschlicher Entscheidungen, wie auch in Abbildung 1 dargestellt. Die höchste Ebene im Energieversorgungssystem besitzt somit eine lenkende Funktion. Die Struktur dieser Ebene basiert auf einer klaren Trennung der Bereiche Steuerung und Monitoring. Abbildung 2 verdeutlicht die hierarchische Anordnung der Akteure der Entscheidungsebene, welche durch Kontrollzentren verkörpert werden.

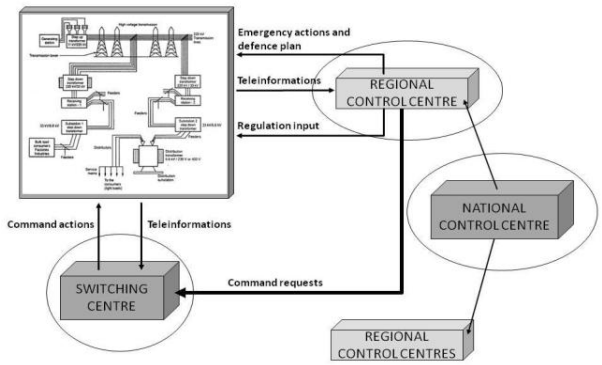


**Abbildung 2. Strukturüberblick der Kontrollzentren [12]**

Die Steuerung wird über die sogenannten Switching Centers (SC) ausgeführt, welche für die Übermittlung von Anweisungen an das Stromnetz zuständig sind. Diese Befehle resultieren letztendlich in Konfigurationsänderungen der Bauelemente (Leistungsschalter, Sicherungslasttrenner, Stufenschaltwerk etc.) des Stromnetzes.

Das Monitoring ist Aufgabe der Regional Control Centers (RCC). Sie kontrollieren den Netzwerkstatus, verwalten dessen Inputdaten und übermitteln an die Betreiber der SCs Steuerungsanfragen für das Stromnetz.

Über diesen beiden Institutionen steht das National Control Center (NCC), welches die Handlungen der RCCs überwacht und nach vorgegebenen Regelungen die Stromflüsse zu anderen Netzen koordiniert.

Kontrollzentren können über zwei Arten von erweiterter Anwendungssoftware verfügen. Beide übernehmen jeweils voneinander getrennte Aufgaben der Verwaltung und Steuerung eines Energieversorgungssystems. Systeme, die mit einer Software für analytische Funktionen im Bereich des Netzwerkbetriebs ausgestattet sind (u.a. Zustandsschätzungen, Netzwerkanalysen, Erzeugungssteuerung), nennt man Energy Management Systems (EMS). Das sogenannte Business Management System (BMS) ist der Teil der Kontrollzentren, welcher für die kommerziellen Anwendungen zuständig ist[13]. Durch Human-Machine-Interfaces (HMI) werden innerhalb der jeweiligen Kontrollzentren Schnittstellen zwischen dem Betreiber (‚Human') und den EMS- und BMS-Systemen hergestellt.

Alles in allem ist in der Entscheidungsebene der Mensch Hauptakteur, verkörpert durch das Personal der Koordinations- und Kontrollzentren. Neben der stetig wachsenden Automatisierung von Anweisungen, ist er grundsätzlich für die Initialisierung von organisatorischen und Sicherheitsmaßnahmen verantwortlich. Seine Anordnungen werden durch HMIs über EMS- oder BMS-Systeme auf eine Datenebene übersetzt und an die physische Ebene übermittelt.

## 3.3 Cyber-Ebene

Wie in Abbildung 1 dargestellt, wird durch die Cyber-Ebene eine bidirektionale Kommunikation zwischen der physischen Ebene und der Entscheidungsebene gewährleistet. Die Datenübertragung erfolgt in Richtung der Entscheidungsebene und die Kontrollhandlungen hin zur physischen Ebene.

Sogenannte Remote Terminal Units (RTU) stellen, wie Abbildung 3 veranschaulicht, die Schnittstelle zwischen den Netzwerk-Bussen in der physischen Ebene zur Cyber-Ebene dar[8]. RTUs sind einfache Bauelemente, welche mit einem Mikroprozessor und einer bestimmten Menge an digitalen und analogen Input/ Output-Kanälen ausgestattet sind. Manche Busse sind direkt und ausschließlich zu einem ausgewählten Bus verbunden, während dagegen andere gruppiert werden, um alle Informationen von einer Vielzahl an Bussen am gleichen Ort zu konzentrieren und sie für eine RTU zugänglich zu machen. Ein Kraftwerk ist in der Lage die Informationen von anderen Kraftwerkanlagen zu verwalten. Aus diesem Grund sind PPs mit einem fest zugehörigen RTU ausgestattet, insbesondere sobald Anlagen mit einer großen Menge an Informationen versorgt werden müssen.

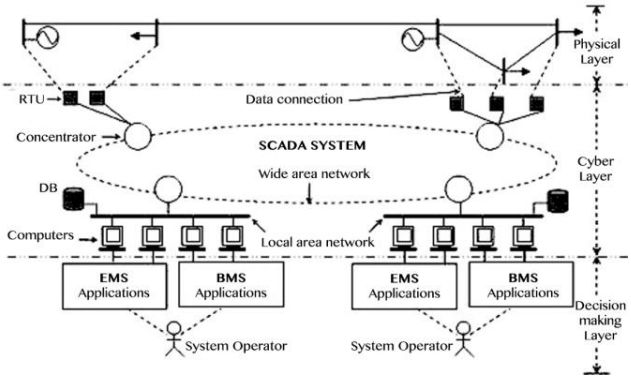


**Abbildung 3. Cyber-Ebene - Kontrollsystem [12]**

RTUs benötigen eine sichere bidirektionale Kommunikation zwischen den Einrichtungen der RCCs und SCs und der Netzwerkhardware. Im Rahmen dieser Kommunikation werden über das Supervisory Control and Data Acquisition (SCADA) System die Kontrollzentren mit einer Menge an Informationen über den Netzwerkstatus versorgt. Das SCADA System verkörpert somit eine ‚Cyber-Brücke'[8] zwischen dem physischem System und den Kontrollzentren, die über die EMS- und BMS-Anwendungen mit dem Kommunikationssystem verbunden sind.

# 4. CRITICAL INFRASTRUCTURE PROTECTION

Das allgemeine Ziel der Critical Infrastructure Protection (CIP) lässt sich als Gesamtheit aller Interessen der Stakeholder einer kritischen Infrastruktur umschreiben. Folglich müssen die zu schützenden Anliegen der Stakeholder betrachtet und zusammengefasst werden. Die Stakeholder lassen sich grob in drei Gruppen kategorisieren:


doi: 10.2313/NET-2015-03-1_09

Den Regulierer der Infrastruktur, den Infrastrukturbetreiber und den Infrastrukturnutzer.

Der Staat hat meistens die Rolle des Regulierers, wobei hier hierarchische Ebenen unterschieden werden müssen (in Deutschland zum Beispiel stehen EU-Regelungen vor Bundesregelungen vor Länderregelungen). Der Regulierer ist für das Verfassen von Vorschriften im Hinblick auf den Betrieb und auch den Schutz kritischer Infrastrukturen verantwortlich. Ziel seines Handelns ist ein kontrollierter Ablauf der Infrastruktur. Dadurch kann die Gesellschaft, in dessen Rahmen der Regulierer handelt, versorgt werden.

Ein Infrastrukturbetreiber besitzt eine Vielzahl an Möglichkeiten sich in einem Sektor am Betrieb einer Infrastruktur zu beteiligen. Verkörpert wird die Funktion überwiegend durch miteinander konkurrierenden Unternehmen. Als oberste Priorität setzen sie die Gewinnerzielung. Dieses Ziel kann nur in Verbindung mit einem erfolgreich geführten Betrieb erreicht werden, welcher auf der Zufriedenheit der Kunden basiert.

Der Nutzer (bzw. Kunde) kann je nach Sichtweise ein weiterer Infrastrukturbetreiber oder Regulierer sein. In der Prozesskette eines Infrastruktursystems stellt er jedoch den Endverbraucher dar. Sein Interesse liegt an einer verlässlichen Versorgung der nachgefragten Menge an Gütern und/ oder Diensten einer kritischen Infrastruktur.

Zusammenfassend lässt sich somit feststellen, dass sich die Interessen der drei Stakeholdergruppen grob in ein Ziel vereinen lassen. Sobald die Versorgung des Infrastrukturnutzers mit dem nachgefragten Gut oder der benötigten Dienstleistung gesichert ist, können die grundlegenden Anliegen aller Beteiligten mitberücksichtigt werden.

Im Folgenden werden nun die Ursachen untersucht, welche die reibungslose Versorgung, in Form von Störungen oder Ausfällen, unterbrechen kann, und deren Auswirkungen in Bezug auf das Energieversorgungssystem abgeschätzt.

## 4.1 Gefahren für kritische Infrastrukturen

Gefahren für kritische Infrastrukturen lassen sich dem Ursprung nach in drei Klassen einordnen[14]. Eine grobe Abschätzung des Ausmaßes der jeweiligen Ursachen wird in Bezug auf die drei Ebenen des Energieversorgungssystems getroffen (vgl. Kapitel 3).

### *4.1.1 Naturereignisse*

Zu Naturgefahren gehören Extremwetterereignisse (Stürme, Hochwasser, Hitzewellen etc.), Waldbrände, seismische Ereignisse, Epidemien und kosmische Ereignisse.

Zwar sind das Ausmaß und die Eintrittswahrscheinlichkeit dieser Gefahren abhängig von der geographischen Lage, sie sind jedoch für die CIP der Energiesysteme von großer Bedeutung. Vor allem im Bereich der physischen Ebene befinden sich viele Elemente oberirdisch (Stromleitungen, Masten etc.) und sind somit vor allem für Extremwetterereignisse extrem anfällig.

Im November 2005 zeigte das ‚Münsterländer Schneechaos'[15] zum Beispiel, welchen Schaden Naturereignisse anrichten können, in diesem Fall starker Schneefall. 250.000 Menschen waren bis zu vier Tagen von der Stromversorgung abgeschnitten, da unter anderem 50 Strommasten unter der Last der Schnee- und Eisschichten zusammenbrachen.

### *4.1.2 Failure (technisch/ menschlich)*

Systemversagen, Unfälle und Havarien, Fahrlässigkeit und organisatorisches Versagen sind der Kategorie technischer bzw. menschlicher Failure zuzuordnen.

Auf Grund der steigenden Vernetzung und daraus resultierenden Komplexität von Stromnetzen nehmen auch in diesem Gefahrenbereich die Risiken für den Betrieb zu[16]. Am Beispiel des deutschen Stromnetzes und dessen Integration auf europäischer Ebene entstehen kontinuierlich neue Herausforderungen im Hinblick auf die organisatorischen Fähigkeiten der Betreiber im Bezug auf deren Koordinations- und Kooperationsfertigkeiten. Dies führt vor allem auf der obersten Ebene (‚Entscheidungsebene') zu einem erhöhten Risiko.

Dieses Risiko wurde am 4. November 2006 zur Realität, als es auf Grund von mangelnden Sicherheitsmaßnahmen zu einem größeren Stromausfall[17] in Europa kam. Ungefähr 15 Millionen Menschen waren bis zu eineinhalb Stunden ohne Strom. Auslöser war die planmäßige Abschaltung einer von E.ON betriebenen Hochspannungsleitung für die Ausschiffung eines Kreuzfahrtschiffes. Durch die Abschaltung kam es zu einer Überlastung einer Verbindungsleitung, welche durch ihre automatische Abschaltung kaskardenartige Ausfälle über ganz Europa hinweg provozierte.

Neben den verwaltungstechnischen Herausforderungen, ist die beschleunigte technologische Entwicklung unter anderem Auslöser für eine Vielzahl an Neuerungen. Dies führt zu ungleichen Aktualisierungen von Soft- oder Hardwarekomponenten, was wiederum zu einer Inkompatibilität untereinander führen kann [14]. Hinzu kommt das Risiko, dass das Personal nicht laufend für die neuen Entwicklungen geschult wird bzw. werden kann und die Elemente folglich fehlerhaft bedient werden könnten.

### *4.1.3 Kriminalität*

Sobald man Failure technischer oder menschlicher Art böswillig ausnutzt, kommt man in den Bereich der Kriminalität. Terrorismus, Sabotage, sonstige Kriminalität und (Bürger-)Kriege sind alles in allem schädigende Handlungen, die durch einen Menschen vorsätzlich ausgeführt werden.

Die zunehmende Interaktion zwischen IKT und Stromnetzen provoziert verstärkt Cyberattacken auf Energieversorgungssysteme. 53 Prozent aller Cyberattacken[18] sind auf den Energiesektor gerichtet. Eine Störung oder gar ein Ausfall der Energieversorgung würde weitreichende Konsequenzen auch in anderen Sektoren kritischer Infrastrukturen mit sich ziehen. Der Schutz vor virtuellen Anschlägen stellt folglich einen wichtigen Aspekt der nationalen CIP von Stromnetzen dar[19].

Das Bundesamt für Sicherheit in der Informationstechnik[20] identifizierte im Rahmen von Cyberangriffen die unberechtigte Nutzung von Fernwartungszugängen als eine der wichtigsten Bedrohungen. Wartungszugänge stellen die Schnittstelle eines IKT-Systems nach außen dar, sind aber jedoch heutzutage noch nicht ausreichend abgesichert.

Im Bereich der Stromnetze ist vor allem die Schnittstelle zwischen der physischen Ebene und den Kontrollzentren oftmals nicht ausreichend durch IT-Sicherheitsmaßnahmen geschützt. Die durch SCADA Systeme gesteuerte Schnittstelle stellt somit eine beliebte Angriffsfläche im Rahmen von Cyberattacken[21] dar. Wie E. Bompard et al.[12] schildern, sind die von SCADA Systemen verwendeten Kommunikationsprotokolle nicht durch Authen-

tifizierungs- oder Integritätsmechanismen geschützt. Dadurch ist es einem Angreifer zum Beispiel möglich Malware über Wechseldatenträger und Hardware einzuschleusen und auf die Datenflüsse zwischen den SCADA Systemen und den HMIs zuzugreifen. Damit kann er letztere mit irreführenden Informationen versorgen, um weitere Angriffe auf das Kontrollnetzwerk zum Beispiel zu verheimlichen.

Dieses Vorgehen und dessen enormen Auswirkungen rückten insbesondere durch den Wurm ‚Stuxnet'[22] an das Licht.

‚Stuxnet' adressierte ausschließlich Prozesssteuerungsrechner, auf denen die SCADA-Software ‚WinCC' von Siemens verwendet wurde. Sobald ein Angreifer über die Funktionen des SCADA Servers einer Prozesssteuerungsanlage verfügt, kann er nicht nur nicht autorisierte Befehle ausführen, sondern auch Datenkorruptionen durchführen oder das System anhalten.

## 4.2 Schutzmaßnahmen

Um Angriffen beziehungsweise Gefahren entgegenzuwirken, ist eine mögliche Herangehensweise durch drei Ansätze das Risiko einer Störung bzw. eines Ausfalls zu minimieren. Die Frage nach der Sicherheit eines Systems ist oberflächlich betrachtet die Voraussetzung für die Verlässlichkeit eines Systems und wird nicht getrennt untersucht. Im Folgenden werden die drei Prinzipien anhand von beispielhaften Lösungsansätzen für die analysierten Ursachen veranschaulicht.

### *4.2.1 Vermeidung der unmittelbaren Angriffswirkung*

Das Prinzip der Vermeidung der unmittelbaren Wirkung eines schädigenden Ereignisses beläuft sich auf den, teilweise präventiven, Schutz der Komponenten einer Infrastruktur. Am Beispiel des Energieversorgungssystems kann Ursachenvermeidung unter anderem physisch betrieben werden, zum Beispiel durch die Errichtung von Mauern gegen Hochwasser oder durch Blitzableiter an Stromleitungen. Dadurch kann vor allem Naturgefahren entgegengewirkt werden.

Um insbesondere menschliches Versagen zu vermeiden ist das ‚Vier-Augen'-Prinzip ein verlässlicher Ansatz. Zu beachten ist, dass die über die zweite Person ausgeführte Kontrolle ernstgenommen wird. Wenn dies gewährleistet werden kann, kann die Korrektheit organisatorischer Entscheidungen im Bereich der Koordinations- und Kooperationsplanung zunehmend verstärkt werden. Jedoch muss man bedenken, dass durch den zunehmenden Vernetzungs- und Technologisierungsgrad der Stromnetze die Komplexität auf ein Maß steigt, welches vom menschlichen Auffassungsvermögen nicht mehr vollständig erfasst werden kann. Folglich ist die zunehmende Unterstützung des ‚Vier-Augen-Prinzips' durch IT-Systeme unerlässlich.

Schutzmaßnahmen können und müssen auch virtuell umgesetzt werden. Im Rahmen der Kriminalitätsbekämpfung hat das Thema Cyber-Sicherheit aktuelle Brisanz. Eine Studie zeigt[21], dass heutzutage nur 17 Prozent der befragten Unternehmen ausreichende IT-Sicherheitsmechanismen implementiert haben. Wie bereits im Unterkapitel 4.1.3 erörtert, liegt eine besonders große Schwachstelle der Cyber-Ebene im Bereich der SCADA Kommunikationsprotokolle. In den letzten Jahren wurden einige Protokolle vorgestellt, welche die Anforderungen an ein sicheres SCADA System erfüllen. Einerseits muss die Integrität der übermittelten Sensor- wie auch Anweisungsdaten gewährleistet werden. Andererseits sind die Authentizität der Kommunikationspartner, wie auch die Vertraulichkeit der Serverdaten grundlegende Anforderungen. Die Arbeitsgruppe 15 des Technischen Komitees 57 der Internationalen Elektrotechnischen Kommission (IEC) veröffentlichte Standards für die Cyber-Security in Energieversorgungssystemen. Weitere Informationen zu den publizierten Maßnahmen in [23].

### *4.2.2 Redundanz und Dezentralisierung*

Die Verteilung der ausfallfähigen Elemente lässt sich durch zwei verschiedene Ansätze realisieren: der Redundanz einerseits und der Dezentralisierung andererseits.

Im Falle von Naturgefahren spielt die Redundanz eine wichtige Rolle. Ausschlaggebend hierfür ist das (n-1)-Kriterium. Dies besagt[24], dass im Falle des Ausfalls eines der n Versorgungswege die Versorgung ungestört fortgesetzt werden kann ohne dass dabei andere Elemente unzulässig belastet werden. Jedoch ist auch hier die steigende Vernetzung Grund für die Annahme, dass sobald zwei oder mehr Elemente gleichzeitig ausfallen, das (n-1)-Kriterium nicht mehr greift[25] und komplexere Prinzipien bei der Stromnetzplanung angewendet werden müssen.

Übergangselemente, zum Beispiel Haushaltsanschlüsse, Transformatoren sowie entsprechende Elemente im IT-Netzwerk, stellen in Stromversorgungseinrichtungen sogenannte Single Points of Failure (SPOF)[26] dar. Diese können im Falle eines Ausfalls zu erheblichen Störungen des Versorgungssystems führen. Durch redundante Geräte kann jedoch eine unterbrechungsfreie Versorgung gewährleistet werden[27]. Das redundante Gerät sollte hierbei zudem auf eine andere Art hergestellt worden sein, um die Wahrscheinlichkeit eines Ausfalls beider Geräte zu minimieren. In dem Falle eines Ausfalls des einen Gerätes kann durch die parallele Schaltung über Entkoppeldioden das andere Element einspringen ohne durch das defekte Gerät auch beschädigt zu werden.

Je dezentraler ein Energienetz aufgebaut ist, desto stabiler ist es nicht nur gegen Extremwetterereignisse, sondern im besonderen Maße gegen terroristische Angriffe. Beim Ausfall eines Kraftwerkes kann die Versorgung durch ein dezentralisiertes System trotzdem gesichert werden, da die Übertragungsnetze nicht nur von dem einen angegriffenen Kraftwerk abhängen[28]. Das Gesamtsystem wird somit robuster.

### *4.2.3 Unabhängigkeit*

Unabhängigkeit von der Stromversorgung über das herkömmliche Verteilnetz ist insbesondere in Bereichen, wie dem des Gesundheitswesens, wichtig. Für alle drei Gefahrenbereiche gibt es einen einstimmigen Ansatz als Schutzmaßnahme.

Unabhängige Stromversorgungssysteme (USV) sorgen dafür, dass stromabhängige Geräte weiterlaufen[29] und somit der Betrieb der Infrastruktur nicht gestört wird. Zusätzlich sollen USV in der Lage sein, kurzzeitige Unter- und Überspannungen abzufangen. Damit sind Krankenhäuser zum Beispiel in der Lage für einige Zeit ohne das öffentliche Stromnetz weiter zu arbeiten.

Das Zukunftskonzept ‚Smart Grid' stellt eine weitere Möglichkeit dar im Falle eines Totalausfalls ‚intelligent' mit den vorhandenen Ressourcen auszukommen. Verbraucher sind durch ‚Smart Grids' in der Lage als sogenannte ‚Prosumer' zu agieren. Das heißt Strom, welchen ein Verbraucher (‚Consumer') zum Beispiel durch eigene Photovoltaik-Anlagen produziert, kann er je nach

Marktsituation selbst verbrauchen. Im Falle eines Ausfalls kann somit ein ‚Prosumer' seinen eigenen Strom verbrauchen und ist somit im gewissen Maße nicht von der öffentlichen Stromversorgung abhängig.

## 5. FAZIT

Kritische Infrastrukturen umfassen die Gesamtheit aller lebensnotwendigen Systeme und sind durch den Staat zu schützen. Insbesondere das Energieversorgungssystem ist auf Grund der hohen Vernetzung der verschiedenen Elemente untereinander auf eine funktionierende Interaktion aller beteiligten Akteure, physisch wie auch virtuell, angewiesen.

Die Verletzlichkeit kritischer Infrastrukturen und im besonderen Maße die des Stromnetzes, ist auf Grund der wachsenden Interdependenzen und Technologisierung in den letzten Jahren stark gestiegen. Der Schutz kritischer Infrastrukturen ist zu einer gesamtgesellschaftlichen Aufgabe herangewachsen, die nicht nur durch technische Maßnahmen ausgeführt werden kann. Mit Rücksicht auf die Durchdringung aller Bereiche durch IKT sollte in Zukunft vor allem Wert auf die Stärkung der Cyber-Sicherheit gelegt werden, zum Beispiel durch sichere Kommunikationsprotokolle. Dies sollte nicht nur durch staatliche Initiativen unterstützt, sondern vor allem unternehmensintern umgesetzt werden.

## 6. REFERENCES


[1] *The Report of the President's Commission on Critical Infrastructure Protection* (Oct. 1997). http://fas.org/sgp/library/pccip.pdf (16.09.2014).

[2] OECD: Protection of 'Critical Infrastructure' and the role of investment policies relating to national securities (May 2008). http://www.oecd.org/investment/investment-policy/40700392.pdf (16.09.2014).

[3] Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html (20.09.2014).

[4] Department of Homeland Security: *National Infrastructure Protection Plan*. http://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf (18.09.2014)

[5] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: *Sektoren- und Brancheneinteilung Kritischer Infrastrukturen*.http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Downloads/Kritis/neue_Sektoreneinteilung.pdf?__blob=publicationFile (17.09.2014).

[6] Cavelty, M./ Suter, M.: *The Art of CIIP Strategy: Tacking Stock of Content and Processes*. Erschienen in: Critical Infrastructure Protection – Information Infrastructure Models, Analysis, and Defense. Springer Verlag, 2012.

[7] Deutscher Bundestag: *Unterrichtung durch die Bundesregierung - Rahmenprogramm der Bundesregierung „Forschung für die zivile Sicherheit (2012 bis 2017)"* (Jan. 2012). http://dip21.bundestag.de/dip21/btd/17/085/1708500.pdf (22.10.2014).

[8] Negenborn, R./ Lukszo, Z./ Hellendoorn, H. (Hrsg.): *Intelligent Infrastructures*. Springer Verlag, 2010.

[9] Institute for Energy and Transport (IET), Joint Research Center. http://ses.jrc.ec.europa.eu/non-experts-0 (18.09.2014).

[10] Fraunhofer ESK: *Smart Grid Communications 2020* (Nov. 2011).http://www.esk.fraunhofer.de/content/dam/esk/de/documents/SmartGrid_Studie_final-web.pdf (20.09.2014).

[11] Bundesregierung: *Anteil Erneuerbarer Energien wächst weiter* (Jan. 2014). http://www.bundesregierung.de/Content/DE/Artikel/2014/01/2014-01-13-bdew-energiebilanz-2013.html (22.10.2014).

[12] Bompard, E. et al.: *Cyber Vulnerability in Power Systems Operation and Control.* Erschienen in: Critical Infrastructure Protection – Information Infrastructure Models, Analysis, and Defense. Springer Verlag, 2012.

[13] Tranchita, C. et al.: *ICT and Power Systems: An Integrated Approach.* Erschienen in: Securing Electricity Supply in the Cyber Age. Springer Verlag, 2010.

[14] Bundesministerium des Innern: *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*. http://www.bmi.bund.de/cae/servlet/contentblob/598730/publicationFile/34416/kritis.pdf (17.09.2014)

[15] DWD, Deutschländer, T./ Wichura, B.: *Klimastatusbericht 2005: Das Mümsterländer Schneechaos am 1. Adventswochenende 2005* (Nov. 2005). http://www.dwd.de/bvbw/generator/DWDWWW/Content/Oeffentlichkeit/KU/KU2/KU22/klimastatusbericht/einzelne__berichte/ksb2005__pdf/15__2005,templateId=raw,property=publicationFile.pdf/15_2005.pdfT. (20.10.2014).

[16] Bundesministerium des Innern: *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement*. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf?__blob=publicationFile (17.09.2014).

[17] Bundesnetzagentur: *Bericht über die Systemstörung im deutschen und europäischen Verbundsystem am 4. November 2006* (Feb. 2007). http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/Berichte_Fallanalysen/Bericht_9.pdf?__blob=publicationFile&v=1 (20.10.2014).

[18] Softpedia, Kovacs, E.: *ICS-CERT Warns of Brute-Force Attacks Against Critical Infrastructure Control Systems* (Jun. 2013). http://news.softpedia.com/news/ICS-CERT-Warns-of-Brute-Force-Attacks-Against-Critical-Infrastructure-Control-Systems-364266.shtml (20.10.2014).

[19] Bundesministerium des Innern: *Schutz kritischer Infrastrukturen – Basisschutzkonzept* (Aug. 2005). http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2005/Basisschutzkonzept_kritische_Infrastrukturen.pdf?__blob=publicationFile (17.09.2014).

[20] Bundesamt für Sicherheit in der Informationstechnik: *Angriffsmethoden* (Apr. 2012). http://allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/angriffsmethoden/statistiken/ (22.10.2014).

[21] Cyber Risk Network, Ayers, E.: *Critical Infrastructure cyber risk scenarios not science fiction* (Jul. 2014).

http://www.cyberrisknetwork.com/2014/07/18/critical-infrastructure-cyber-risk/ (20.09.2014).

[22] Bundesamt für Sicherheit in der Informationstechnik: *Die Lage der IT-Sicherheit in Deutschland 2011* (Mai 2011). http://www.bsi.bund.de/SharedDocs/Downloads/DE/ (22.10.2014).

[23] International Electrotechnical Commission (IEC), Cleveland, F.: IEC TC 57 WG 15: IEC62351 Security Standards for the Power System Information Infrastructure. http://iectc57.ucaiug.org/wg15public/ (20.09.2014).

[24] Forschungsforum Öffentliche Sicherheit, Birkmann, J. et al.: *State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/ Stromausfall.* Freie Universität Berlin, 2010.

[25] *Grundsätze für die Planung des deutschen Übertragungsnetzes* (Mär. 2012). http://www.50hertz.com/Portals/3/Content/Dokumente/Anschluss-Zugang/Verteiler/Planungsgrundsaetze-120330.pdf (20.10.2014).

[26] Jüllig, R.: *Analyse zur IT-Sicherheit in Energieversorgungssystemen* (Mai 2013). http://www.f07.fh-koeln.de/imperia/md/content/personen/waffenschmidt_eberhard/abschlussarbeiten_auschreibungen/juellig_it_sicherheit_forschungsarbeit2013.pdf (18.09.2014).

[27] Energie und Technik – Lexikon. http://energie-und-technik.de/ (20.09.2014).

[28] B.KWK, Golbach, A.: *Fakten und Thesen zur Dezentralisierung der Stromerzeugung* (Jul. 2004). http://bkwk.de/ (17.09.2014)

[29] Elektronik Kompendium. http://www.elektronik-kompendium.de/sites/grd/0812171.htm (20.09.2014).



doi: 10.2313/NET-2015-03-1_09