Branchenempfehlung Strommarkt Schweiz

ICT Continuity

(Information & Communication Technology Continuity)

Umsetzungsempfehlungen zur Gewährleistung der ständigen Disponibilität der Informatik- und der Kommunikationstechnologie zwecks Sicherstellung der Versorgung

ICT-Cont, Ausgabe 2011

Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Impressum und Kontakt

Herausgeber
Verband Schweizerischer Elektrizitätsunternehmen VSE
Hintere Bahnhofstrasse 10, Postfach
CH-5001 Aarau
Telefon +41 62 825 25 25
Fax +41 62 825 25 26
info@strom.ch
www.strom.ch

Autoren der Erstauflage 2011

Christian Angele	SGSW	DSV
Norbert Bachmann	Swissgrid/WL ICT-I	Swissgrid
Mattia Bardelli	AET	ESI
Reto Bondolfi	ewz/WL ICT-I	Regionalwerke
Jean-Michel Bovet	Romande Energie	Regiogrid
Lorenz Cairoli	EBM	Regionalwerke
Raymond Cettou	SIG	Swisspower
Nisheeth Singh	Swissgrid	Swissgrid
Adrian Schwammberger	AEW/WL ICT-I	Regionalwerke
Peter Waldegger	Axpo	Swisselectric

Beratung und Umsetzung

Dr. Adrian Marti	AWK
Reto Büttner	AWK

AWK Group AG
Leutschenbachstrasse 45
Postfach, CH-8050 Zürich
Tel. +41 44 305 95 11
www.awk.ch

Weitere Unterstützung
Werner Meier, Alpiq / Chef WL ICT-I-Energie
Ruedi Rytz, BWL
Sandfire AG, Bruchmattstrasse 12, CH-6003 Luzern

Projektleitung VSE
Peter Betz, Auftraggeber
Jean-Michel Notz, Projektleiter

Chronologie der Branchenempfehlung ICT Continuity

Februar 2011	Arbeitsaufnahme Arbeitsgruppe ICT Continuity
Juli 2011	Entwurf bereit zur Vernehmlassung
Sommer 2011	Vernehmlassung in der Branche
September-November 2011	Überarbeitung nach Vernehmlassung
7. Dezember 2011	Verabschiedung durch den VSE-Vorstand

Dieses Dokument ist ein Branchendokument zum Strommarkt

Druckschrift Nr. 1025d, Ausgabe 2011

Abkürzungen und Begriffe

Abkürzung	Beschreibung
BWL	Bundesamt für wirtschaftliche Landesversorgung
DSG	Bundesgesetz über den Datenschutz (Datenschutzgesetz)
ICT (IKT)	Informations- und Kommunikationstechnologie
Krise	Ungeplantes Verhalten der elektrischen Energieversorgung mit über 50 MWh nicht zeitgerecht gelieferter Energie
SCADA	Überwachen und Steuern technischer Prozesse (Supervisory Control And Data Acquisition)
Störung	Ungeplantes Verhalten der elektrischen Energieversorgung
StromVG	Bundesgesetz über die Stromversorgung (Stromversorgungsgesetz)
NZGE	Nicht zeitgerecht gelieferte Energie
VSE	Verband Schweizerischer Elektrizitätsunternehmen

Referenzierte Dokumente

Titel	Autor / Herausgeber	Datum [1]	Link / Datei
[1] Risikoanalyse, Bereich ICT-Infrastruktur, Sektor elektrische Energie	Bundesamt für wirtschaftliche Landesversorgung	18.01.2011	
[2] Transmission Code 2010	Swissgrid	23.11.2009	http://www.strom.ch/uploads/media/TC_CH_2010_de_01.pdf
[3] Distribution Code Schweiz	VSE	2011	http://www.strom.ch/uploads/media/DC_CH_2011_D.pdf
[4] Good Practice Leitfaden (2010)	Business Continuity Institute BCI	2010	www.thebci.org
[5] Empfehlungen für das Business Continuity Management (BCM)	Schweizerische Bankier Vereinigung SwissBanking	2007	http://www.swissbanking.org/11107_d.pdf
[6] Asut-Branchenempfehlung Business Continuity Management (BCM)	Schweizerischer Verband der Telekommunikation asut	2009	http://www.asut.ch/content/content_renderer.php?id=263&s=1&lan=1
[7] Technical Specification TS 62351-1. Power systems management and associated information exchange – Data and communications security	International Electrotechnical Commission IEC	2007 - 5	http://webstore.iec.ch/preview/info_iec62351-1%7Bed1.0%7Den.pdf
[8] Treatment of Information Security for Electric Power Utilities, Technical Brochure N°419	Cigré	Juni 2010	http://www.cigre.org/

[1] Oder die jeweils aktuellste Ausgabe.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

Das Stromversorgungsgesetz (StromVG) vom 23.03.2007 und die Stromversorgungsverordnung (StromVV) vom 14.03.2008 und 12.12.2008 haben den Schweizer Strommarkt für Endkunden mit einem Jahresverbrauch von grösser 100MWh pro Verbrauchsstätte geöffnet. 5 Jahre nach Inkrafttreten dieses Gesetzes sollen durch Bundesratsbeschluss auch Endverbraucher mit einem Jahresverbrauch von weniger als 100 MWh pro Verbrauchstätte vom diskriminierungsfreien Netzzugang Gebrauch machen können. Dieser Beschluss unterliegt dem fakultativen Referendum.

Im Sinne des Subsidiaritätsprinzips (StromVG Art.3 Abs. 1) wurde im Rahmen des Projekts Merkur Access II ein umfassendes Regelwerk für die Elektrizitätsversorgung im offenen Strommarkt durch Fachleute der Branche ausgearbeitet. Mit diesem Regelwerk steht der Elektrizitätswirtschaft eine branchenweit anerkannte Empfehlung zur Nutzung der Stromnetze und der Organisation des Energiegeschäftes zur Verfügung.

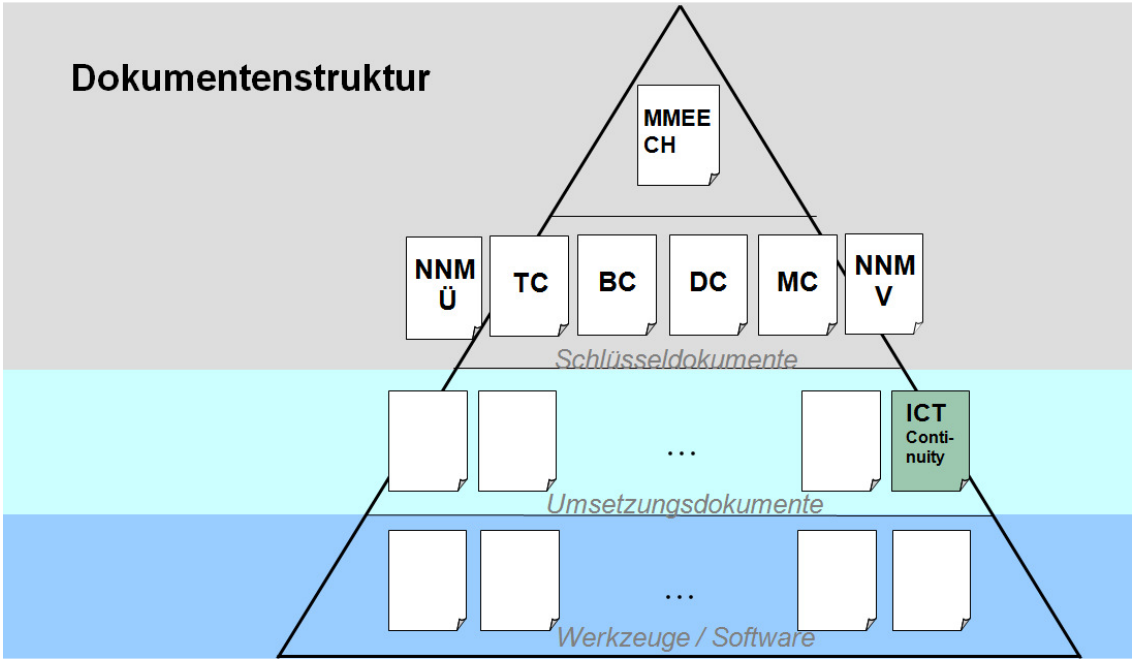
StromVG und StromVV verlangen die Erarbeitung von Richtlinien zu verschiedenen Sachverhalten durch die Netzbetreiber. Diese Aufgabe wurde im Rahmen der Branchendokumente erfüllt. Die entsprechenden Kapitel in den verschiedenen Dokumenten sind im Kapitel 7 des Marktmodells Elektrische Energie (MMEE) aufgeführt.

Das Netznutzungsmodell für die Verteilnetze (NNMV – CH), das Netznutzungsmodell für das Übertragungsnetz (NNMÜ – CH), der Transmission Code (TC – CH), das Balancing Concept (BC – CH), der Metering Code (MC – CH) und der Distribution Code (DC – CH) sind Schlüsseldokumente.

Abgestimmt auf diese zentralen Dokumente werden die Umsetzungsdokumente sowie die nötigen „Werkzeuge“ durch die Branche erarbeitet.

Das vorliegende Dokument ICT Continuity ist ein Umsetzungsdokument.

Weder Branchendokumente noch Richtlinien sind staatlich gesetztes Recht. Bei denjenigen Bestimmungen der Branchendokumente, welche als Richtlinien im Sinne vom Art. 27 Abs. 4 StromVV gelten, handelt es sich um Selbstregulierungsnormen. Behörden und Gerichte werden im konkreten Einzelfall die in den Branchenrichtlinien vorgeschlagene Lösung in der Regel übernehmen, es sei denn, sie erweise sich als nicht sachgerecht.
Die übrigen Branchendokumente sind grundsätzlich für diejenigen Beteiligten verbindlich, welche die Branchendokumente in einem konkreten Vertrag zum Vertragsbestandteil erklärt haben (sofern sie nicht zum Beispiel gegen die Stromversorgungsgesetzgebung verstossen).
Im Übrigen handelt es sich dabei um Branchenempfehlungen.



1. Zusammenfassung

(1) Mit den sich rasant entwickelnden Informations- und Kommunikationstechnologien (IKT, resp. ICT) entstehen für die Elektrizitätsunternehmen ungeahnte technische Möglichkeiten, aber auch neue Herausforderungen und Risiken. Für die Bewältigung unvorhergesehener Ereignisse in vernetzten Systemen ist es entscheidend, dass alle wichtigen Akteure koordiniert vorgehen und die Systemeigner der Branche die nötigen Vorkehrungen zur Ereignisbewältigung präventiv gemeinsam festlegen.

(2) Dazu wird in der vorliegenden Branchenempfehlung ein ICT Continuity Management (ICT-CM) Minimalstandard definiert, der sich in die ICT Continuity Strategie, die Business Impact Analyse, ICT Continuity Pläne, ICT Continuity Reviews, ICT Continuity Tests und die kontinuierliche Verbesserung strukturiert. Dieser Minimalstandard beinhaltet Analysen, Vorgaben und Anweisungen, die von jedem Elektrizitätsunternehmen schriftlich festgehalten werden sollen.

(3) Für die kritischen ICT Infrastrukturen der Elektrizitätsunternehmen werden konkrete Handlungsempfehlungen formuliert. Diese Branchenempfehlung dient der Krisenprävention. Die kritischen ICT Infrastrukturen der Elektrizitätsunternehmen sollen so ausgelegt werden, dass pro Ereignisfall möglichst nie eine Energiemenge von 50 MWh oder mehr nicht zeitgerecht geliefert wird (NZGE) [1].

(4) Diese Empfehlung gilt für die Branche in den Netzebenen 1 bis 4 als „Best Practice“. Auf tieferen Netzebenen angesiedelte Branchenteilnehmer sollen diese Empfehlung wo immer möglich stufengerecht umsetzen. Siehe auch dazu Abbildung 2, Seite 11.

(5) Die Rechtskommission des VSE (REKO) hält in seiner Stellungnahme zum Dokument fest, dass dadurch, dass das Dokument zum Branchendokument erhoben wird, es zum Massstab wird, an welchen sich Behörden und Gerichte in einem Eintretensfall halten werden. Die Netzbetreiber sind gut beraten, wenn sie sich an sämtliche im Dokument enthaltenen Vorgaben halten und dies auch nachvollziehbar festhalten (Beweissicherung).

2. Ausgangslage und Zielsetzung

(1) Mit den sich rasant entwickelnden Informations- und Kommunikationstechnologien (IKT, resp. ICT) entstehen für die Elektrizitätsunternehmen ungeahnte technische Möglichkeiten, aber auch neue Herausforderungen und Risiken. Bereits ein kleiner Systemfehler oder ein äusseres Ereignis kann aufgrund der immer engeren Vernetzung über die Unternehmens- und Branchengrenzen hinaus zum Zusammenbruch von ICT-Systemen mit gravierenden Folgen führen. Wegen der immer fortschreitenden Zentralisierung der Leitsysteme wächst das potentielle Schadensausmass bei Störungen in diesen Systemen.

(2) Die aktuellen technischen Entwicklungen der Stromversorgungsinfrastruktur sind stark geprägt durch die kommunikative Vernetzung und Steuerung von Stromerzeugern, Speichern, elektrischen Verbrauchern und Netzbetriebsmitteln in Energieübertragungs- und –verteilungsnetzen der Elektrizitätsversorgung. Die Schaffung intelligenter Stromnetze (engl. Smart Grids) führt zu neuen Verwundbarkeiten der Elektrizitätsunternehmen, ausgelöst beispielsweise durch:

- die bidirektionale Kommunikation zu Endgeräten (Smart Meters),
- über immer grössere Netzgebiete zusammengeschlossene Leitsysteme,
- die nur schwache Authentifizierung der Nutzer der Leitsysteme,
- ungenügende Schulung der Mitarbeiter.

(3) Der stetig fortschreitende Einzug netzwerkfähiger und fernwartbarer Infrastruktur wird die Attraktivität für Angriffe von aussen, z.B. durch Hacker erhöhen.

(4) Ebenfalls ist eine zunehmende Brisanz der Datenschutzproblematik[2] zu erwarten, verstärkt durch einen vermehrten Anfall von Kundendaten, insbesondere im Bereich Smart Metering.

(5) Die zwingend notwendige hohe Sicherheit moderner Energieleitsysteme wird erreicht durch:

- ein integriertes und ganzheitliches Sicherheitskonzept,
- klar definierte und getrennte Sicherheitsdomänen (Security Domain Model),
- eine Strategie der mehrstufigen Verteidigung (verhindern, entdecken, verteidigen und wiederherstellen),
- Standardisierung (nur umfassend geprüfte und für die Stromversorgung geeignete Technologien verwenden),
- durch die Etablierung einer glaubwürdig, durch das Management gelebten Sicherheitskultur und Schulung,

(6) Für die Bewältigung von unvorhergesehenen Störfällen in vernetzten Systemen ist es entscheidend, dass alle wichtigen Akteure koordiniert vorgehen und die nötigen Vorkehrungen vorgängig festgelegt werden.

(7) Ziel dieser Empfehlung ist es, Rahmenbedingungen zu schaffen, um Unterbrechungen der Geschäftstätigkeit entgegenzuwirken, die kritischen Geschäftsprozesse vor den Auswirkungen wesentlicher Ausfälle der ICT Infrastruktur zu schützen und ihre Fortführung sicherzustellen. Der wichtigste und kritischste Geschäftsprozess der Elektrizitätsunternehmen ist die Versorgung der Kunden mit elektrischer Energie. Dabei muss die Personensicherheit des Betriebs- und Unterhaltspersonals sowie von unbeteiligten Dritten stets gewährleistet sein.

(8) Diese Empfehlung soll die Basis für entsprechende Planungen und für die Vorbereitung auf die Bewältigung von ICT Störungen bilden, so dass negative Auswirkungen auf die Versorgungssicherheit verhindert oder zumindest vermindert werden können.

(9) Die Branchenempfehlung ist möglichst unabhängig vom jeweiligen Stand der Technik erarbeitet worden, da sich dieser rasch ändert. Die Anwendung der Branchenempfehlung hat individuell auf das eigene Unternehmen angepasst zu erfolgen. Unterstützung für die konkrete Umsetzung der Branchenempfehlung findet sich in der in Kapitel 8 aufgeführten Literatur.

[2] Siehe StromVG Art 10 und DSG

3. Geltungsbereich

(1) Die vorliegende Selbstregulierung des VSE richtet sich an die Netzbetreiber. Insbesondere betroffen sind die Eigentümer und Betreiber der Netzebenen 1 bis 4 (siehe Kapitel 4.2 und Abbildung 2). Diese Empfehlung wird von der Branche, insbesondere für Netzebenen 1 bis 4 als „Best Practice“ angewandt.

(2) Auf tieferen Netzebenen angesiedelte Branchenmitglieder sind angehalten, diese Empfehlung wo immer möglich ebenfalls stufengerecht umzusetzen. Betreiber der Netzebenen 5 bis 7 haben sicherzustellen, dass sie durch die vernetzten Leitsysteme keine Störungen auf den höheren Netzebenen verursachen.

(3) Dem Datenschutz ist auf den tieferen Netzebenen besonders Rechnung zu tragen.

(4) Diese Selbstregulierung enthält Empfehlungen (“Best Practice”) zur Ausgestaltung eines unternehmensspezifischen ICT Continuity Managements. Dabei ist auf die Besonderheiten der jeweiligen Ausgangslage, insbesondere der Risikosituation der einzelnen Unternehmungen, zu achten.

4. Einbettung

4.1. Dokumentenstruktur VSE

(1) Die vorliegende Branchenempfehlung ist als Umsetzungsdokument in die Dokumentenstruktur VSE zum Strommarkt Schweiz eingebettet.

(2) TC (Transmission Code) und DC (Distribution Code) beinhalten die technischen Regeln zu einem sicheren Netz- und Systembetrieb. Die vorliegende Branchenempfehlung ist auf der Ebene der Umsetzungsdokumente eingeordnet. Siehe auch das Vorwort zu diesem Dokument.

4.2. Definition eines relevanten Ereignis (Krise)

(1) Für das Übertragungsnetz sind meldepflichtige Ereignisse (Transmission Code [2] und Betriebsführungshandbuch Swissgrid) definiert.

(2) Für das Verteilnetz ist im Distribution Code Schweiz [3] Kapitel 2.2.3 resp. 3.5 Netzqualität Ziffer (6) wird für städtische Netze (über 10‘000 Anschlüsse) der Zielwert von maximal 4 Stunden Versorgungsunterbruch pro Ereignis bei einem Endverbraucher festgehalten. Solche Versorgungsunterbrüche sollen nur sehr selten vorkommen, wie in [3] Kapitel 3.5 Netzqualität Ziffer (7) mit den Kennzahlen SAIFI und SAIDI beschrieben wird.

(3) Ein solcher Ausfall von über 10‘000 Anschlüssen während über 4 Stunden wird deshalb als Krise bezeichnet. Bei einer geschätzten durchschnittlichen Leistung eines Anschlusses von 1250 W (ohne Grossverbraucher) entspricht dies einer Ausfallleistung von 12.5 MW und einer nicht zeitgerecht gelieferter Energie (NZGE) von 50 MWh.

(4) Die Zielwerte vom Distribution Code [3] Kapitel 2.2.3, resp. 3.5 werden auf Ereignisse innerhalb eines Verteilnetzes beschränkt. Ereignisse mit sehr geringer Wahrscheinlichkeit werden ausgenommen, z.B. frequenzabhängiger Lastabwurf, Naturkatastrophen oder Terrorismus.

(5) Im Transmission Code [2] sind keine zulässigen Ausfallzeiten quantifiziert.

(6) Somit besteht keine Vorgabe über die zulässige Häufigkeit von Ausfällen aufgrund solcher Ereignisse.

4.3. Domänenmodell Informationssicherheit

(1) Der notwendige hohe Grad an Sicherheit moderner Energieleitsysteme wird durch klar definierte und getrennte Sicherheitsdomänen (Security Domain Model) erreicht:

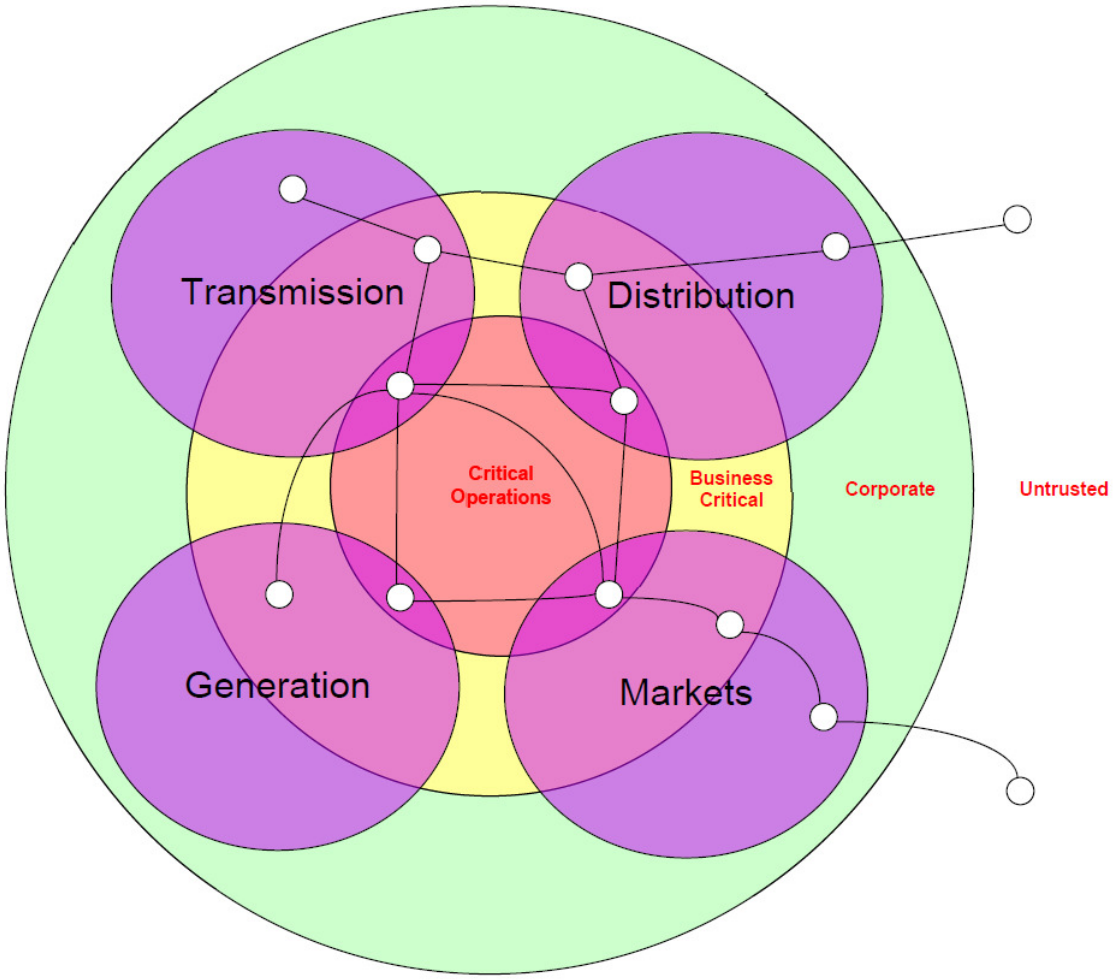


Abbildung 1: Domänenmodell Informationssicherheit (aus [8])

Schutzstufe (bezogen auf den Betrieb)	Domäne	Farbe in Abbildung 1	Beispiele
niedrig	offen (Untrusted)	weiss	Lieferant/Hersteller, Netzwerke Dritter, Internet
mittel	vertraulich (Corporate)	grün	Büro ICT (allgemein)
hoch	geschäftskritisch (Business Critical)	gelb	Büro ICT (Finanzen und Personal)
sehr hoch	betriebskritisch (Critical Operations)	rot	Prozess ICT

Tabelle 1: Übersicht Schutzstufen

4.4. Relevante Netzebenen

(1) Aus dem in Kapitel 4.2 definierten relevanten Ereignisses (Krise) lassen sich die relevanten Netzebenen ableiten.

- Störungen in den Netzebenen 1 bis 4 können zu einer Krise mit einer nicht zeitgerecht gelieferten Energie (NZGE) von über 50 MWh führen. Solche Störungen sollen stufengerecht bewältigt werden.
- Die Netzebenen 5 bis 7 sind insofern betroffen, als dass dort sichergestellt werden muss, dass diese nicht Ursache für Störungen auf den höheren Netzebenen sind. Dabei müssen insbesondere die vernetzten Leitsysteme berücksichtigt werden, mit der Gefahr einer Verschleppung eines Virus oder eines Hackerangriffes.

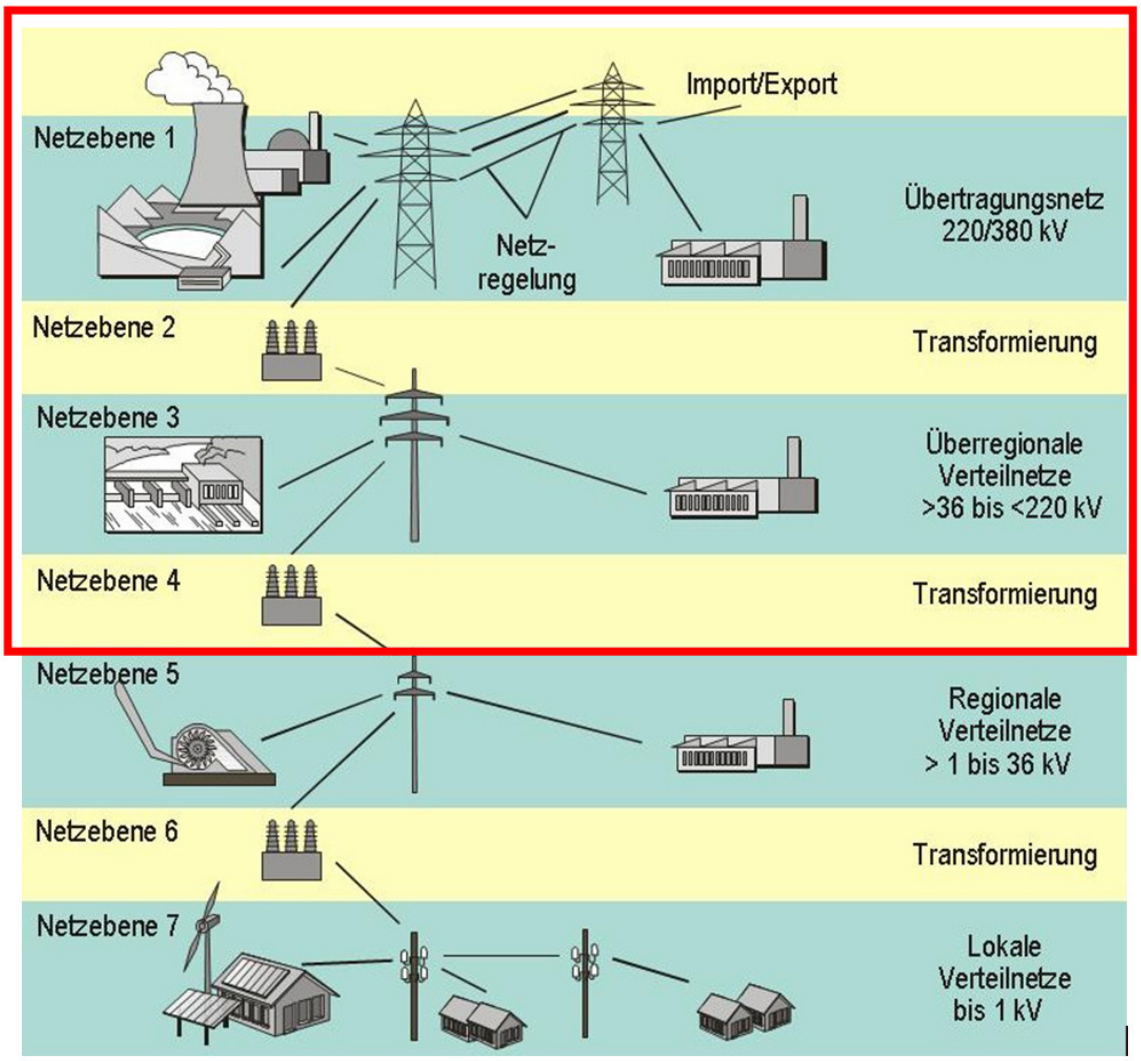


Abbildung 2: Relevante Netzebenen

4.5. Relation zur Risikoanalyse, Bereich ICT-Infrastruktur, Sektor Energie der wirtschaftlichen Landesversorgung

(1) Die Risikoanalyse [1] bildet eine wesentliche Grundlage für die vorliegende Branchenempfehlung. Die Analyse bestätigt, dass potenzielle Schäden im Bereich der Übertragungsnetze am grössten sind, da sich dort Instabilitäten über grosse Gebiete verbreiten können.

(2) In der Risikoanalyse [1] wurden folgende kritische Risiken identifiziert. Diese kritischen Risiken wiederspiegeln die aktuelle Topologie der Leitsysteme der Elektrizitätsunternehmen (Siehe Abbildung 3):

- Ausfall zentrales Netzleitsystem / Netzleittechnik (SCADA),
- Ausfall kritischer Applikation der Netzführung,
- Ausfall Rechenzentrum,
- Ausfall Telekommunikationstechnik und Infrastruktur,
- Ausfall Stationsleittechnik (Unterwerke und Kraftwerke).

(3) Da die geschätzten Eintrittswahrscheinlichkeiten der Risiken keine Aussage über den Zeitpunkt des Ereigniseintritts zulassen, ist ein aktives Management der identifizierten Risiken notwendig.

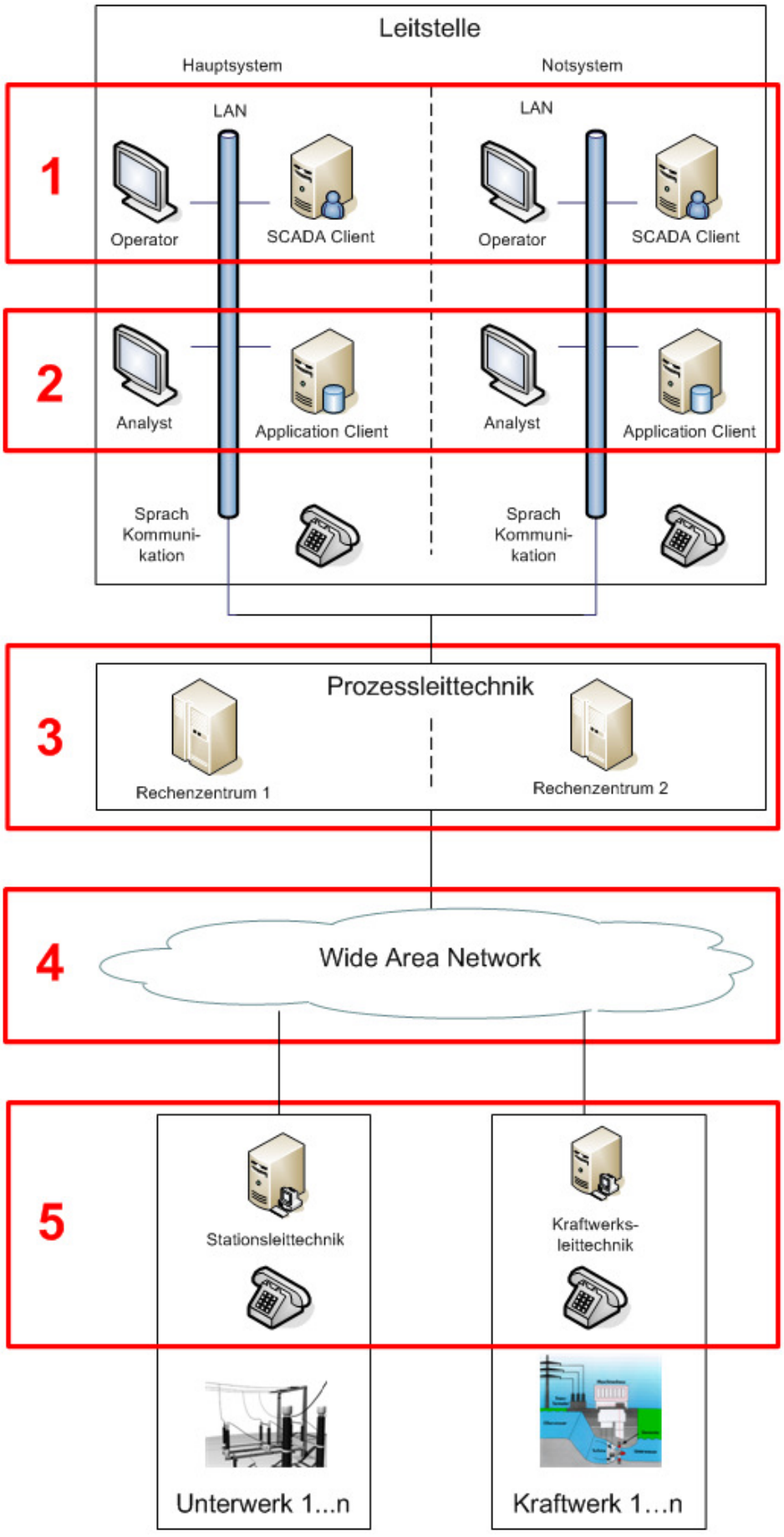


Abbildung 3: Kritische Infrastrukturen in Leittechnik, Daten und Sprachkommunikation

5. Anwendungsbereiche/Szenarien

(1) Die Elektrizitätsunternehmen haben alle potentiell relevanten Szenarien zu berücksichtigen, welche für das eigene Unternehmen oder für die Branche zu einer Krise führen können. Dabei wird – wie unter Kapitel 4.2 hergeleitet - unter einer „Krise“ ein ungeplantes Verhalten der elektrischen Energieversorgung mit über 50 MWh nicht zeitgerecht gelieferten Energie verstanden. Die Bewältigung kleinerer „Störungen“ mit weniger als 50 MWh nicht zeitgerecht gelieferter Energie ist nicht Gegenstand dieser Empfehlungen.

(2) Die Entstehung von Krisen kann unterschiedlichste Ursachen haben.

(3) Mögliche unabwendbare Ursachen für Krisensituationen sind beispielsweise:

- „unfallartige” Ereignisse wie z.B. Brand oder Explosion,
- Naturkatastrophen wie z.B. Überschwemmung oder Erdbeben,
- Fahrlässigkeit von Betriebspersonal,
- Ausfall von Personal, z.B. aufgrund Pandemie,
- Ausfall der Gebäudetechnik und/oder der Energieversorgung (z.B. Elektrizität),
- Ausfall von IT Systemen oder Infrastrukturen (Hardware- oder Software-Fehler),
- Ausfall von Kommunikationssystemen oder Telecom-Providern,
- Ausfall von externen Lieferanten (vgl. Outsourcing / Cloud Computing) wie z.B. Informationsprovider.

(4) Mögliche vorsätzliche Ursachen für Krisensituationen sind beispielsweise:

- Verärgerter Mitarbeiter,
- Vandalismus,
- Industriespionage, Terrorangriff oder Sabotage (z.B. Sprengung oder Vandalismus),
- Cyber-Attacke (z.B. Virus oder Hackerangriff).

(5) Es ist Aufgabe jedes einzelnen Unternehmens, im Rahmen des ICT Continuity Management seine spezifische Bedrohungssituation zu identifizieren. Die identifizierten Bedrohungen (Szenarien) bilden zusammen mit der Business Impact Analyse die Basis zur Erstellung der ICT Continuity Pläne (siehe Absatz 6.3).

(6) Eintretende Ereignisse können beispielsweise zur Folge haben, dass Mitarbeitende und/oder Infrastrukturen (v.a. Führungsinfrastruktur, Telekommunikation, Gebäude bzw. Arbeitsplätze) für unternehmenskritische Funktionen nicht mehr einsatzfähig sind. Ebenso können Probleme bei IT-Dienstleistungen oder Infrastruktur-Anbietern dazu führen, dass es zu nicht tolerierbaren Versorgungsausfällen kommt. Ein besonderes Augenmerk ist auf Kettenreaktionen und gegenseitige Abhängigkeiten zu richten, so beispielsweise der Ausfall der zur Wiederherstellung der Stromversorgung benötigten Telekommunikation aufgrund eines Stromausfalls.

(7) Das ICT Continuity Management muss die Einhaltung gesetzlicher, regulatorischer, vertraglicher und interner Vorschriften auch im Krisenfall sicherstellen.

6. Empfehlungen: ICT Continuity Management (ICT-CM) Minimalstandard

Vorbemerkungen

(1) Zu Beginn der Einführung eines erfolgreichen ICT Continuity Managements werden ein Betrachtungsbereich (Scope) definiert und eine Leitlinie (Policy) erstellt, die durch die Unternehmensleitung freigegeben werden müssen. Diese Leitlinie beschreibt die Eckpfeiler des ICT Continuity Managements und stellt den Auftrag der Unternehmensleitung zur Umsetzung dar. Im Rahmen des Programmmanagements werden auch Budgets und Personal für die Implementierung und Aufrechterhaltung des ICT Continuity Managements bereitgestellt. Durch die Unternehmensleitung sollen sowohl ein Verantwortlicher für die Erarbeitung und Umsetzung der Leitlinie als auch ein oder mehrere Verantwortliche für die Implementierung der erforderlichen Massnahmen benannt werden.

(2) Zur Sicherstellung der Einbettung des ICT Continuity Managements in die Unternehmenskultur und somit in die Unternehmensstrukturen werden alle Phasen des Lebenszyklus durch Schulungen und Awareness Massnahmen für die beteiligten Mitarbeiter begleitet. Diese Massnahmen sollen den Know How-Aufbau und die Akzeptanz fördern.

(3) In der ersten Phase werden die Anforderungen ermittelt, die ein unternehmensweites Business Continuity Management (BCM) an die IT stellt. Durch die Geschäftsbereiche wurden idealerweise maximal tolerierbaren Ausfallzeiten für Anwendungen und Systeme ermittelt. Im Rahmen der ICT Continuity müssen gestützt darauf Wiederherstellungsprioritäten und -zeiten festgelegt werden. Im Anschluss wird ein Soll-/Ist-Abgleich mit bereits umgesetzten Massnahmen des ICT Continuity durchgeführt (Gap-Analyse). In der Gap-Analyse werden sowohl technische als auch organisatorische Massnahmen betrachtet, wie zum Beispiel das von Mitarbeitern mit entsprechenden Kenntnissen für ICT Continuity Teams als auch Massnahmen zur Erhöhung der Verfügbarkeit von Anwendungen und Systemen.

(4) Es gibt ein breites Spektrum von potenziellen Angreifern, die sich hervorragend mit Technologien zur Transmission und Distribution sowie zur Steuerung und Kontrolle bei Übertragungs- und Verteilnetzen und entsprechenden Angriffsmethoden auskennen. Zu diesen Schwachstellen kommen funktionale Software-Fehler, die zu unvorhergesehenem Fehlverhalten führen können ebenso wie mögliche Hardware-Defekte und Netzwerkausfälle.

6.1. Business Impact Analyse

(1) Jede Unternehmung bestimmt ihre kritischen Ressourcen und Prozesse und erstellt eine Business Impact Analyse. Darin werden für die geschäftskritischen Prozesse die jeweiligen Auswirkungen beim Eintritt dieser Szenarien beurteilt.

(2) Diese Beurteilung schliesst auch gegenseitige Abhängigkeiten zwischen den Geschäftsbereichen (vor-/nachgelagerte Prozesse) und Abhängigkeiten von externen Anbietern (Outsourcing) mit ein.

(3) Mit Fokus auf Ausfälle von volkswirtschaftlicher Relevanz wurde die Risikoanalyse [1] erstellt. Darin sind kritische Infrastrukturen (Ressourcen) identifiziert. Dies soll als Ausgangspunkt für die unternehmensspezifische Business Impact Analyse verwendet werden. Zur Sicherstellung der ICT-Continuity wird der Fokus auf die Informations- und Kommunikationstechnik (ICT) des Unternehmens gelegt.

(4) Die Business Impact Analyse beinhaltet mindestens folgende Ergebnisse:

- Identifikation der Prozesse und Hilfsprozesse, welche eine Schlüsselrolle in der Erbringung der Dienstleistung des Unternehmens haben,
- die maximal tolerierbare Zeitspanne bis zur Wiederherstellung der geschäftskritischen Prozesse,

- den Mindestumfang der (Ersatz-)Ressourcen (Gebäude, Mitarbeitende, IT/Daten, externe Anbieter), die im Krisenfall verfügbar sein müssen, um den gewünschten Wiederherstellungsgrad zu erreichen.

(5) Oftmals werden im Rahmen der Durchführung einer Business Impact Analyse gleichzeitig mit der Verfügbarkeit auch die Anforderungen der Prozesse an die Vertraulichkeit und Integrität erhoben.

(6) Die Häufigkeit der Aktualisierung der Business Impact Analyse richtet sich insbesondere nach der Risikosituation der jeweiligen Unternehmung.

6.2. ICT Continuity Strategie

(1) Die ICT Continuity Strategie legt das grundlegende Vorgehen fest, mit dem das Unternehmen seine in der Business Impact Analyse festgelegten Ziele zur Wiederherstellung erreichen will. Im Rahmen der Strategiedefinition sind auch die relevanten dargelegten Szenarien zu definieren, auf welche die Planung auszurichten ist.

(2) Diese Strategie muss in schriftlicher Form vorliegen.

(3) Insbesondere bei kritischen Prozessen, die wesentliche Dienstleistungen für unsere Gesellschaft bereitstellen, müssen die daraus resultierenden Gefährdungen umfassend und realistisch betrachtet werden.

(4) Ziel muss es sein, dass sich IT-spezifische Gefährdungen nicht negativ auf die gesteuerten Prozesse auswirken. Bei bestehenden Systemen muss auf eine bestmögliche Absicherung geachtet werden. Soweit möglich, besonders aber bei neuen Systemen, sollten zusätzlich Sicherheitseigenschaften implementiert werden, die die informationstechnischen Risiken weiter reduzieren. Dabei dürfen neu implementierte Lösungen keine weiteren Gefährdungen oder Single Points of Failure in die Systeme einführen.

6.3. ICT Continuity Pläne

(1) Ein Resultat der Business Impact Analyse ist die Identifikation der Prozesse und Hilfsprozesse, welche eine Schlüsselrolle in der Erbringung der Dienstleistung des Unternehmens haben. Die Wiederherstellung der Funktionsfähigkeit der ICT-Systeme zur Durchführung der geschäftskritischen Prozesse hat aus Sicht ICT-Continuity oberste Priorität im Krisenfall.

(2) Für diese als geschäftskritisch identifizierten ICT-Systeme sind ICT-Continuity Pläne zu erstellen, welche die für die Wiederherstellung notwendigen Vorgehensweisen beschreiben.

(3) Entsprechende Pläne enthalten mindestens:

- Beschreibung des Anwendungsfalls (auslösendes Szenario),
- Vorgehensweise bzw. Massnahmenkatalog mit Prioritäten, notwendige Ersatzressourcen,
- Krisenorganisation mit Zuständigkeiten und Kompetenzen.

(4) Es sind regelmässige Zeiträume vorzugeben, in denen die ICT Continuity Pläne zu aktualisieren sind. Wesentliche Änderungen in der IT-Architektur oder im Geschäftsbetrieb können ebenfalls eine Überarbeitung der Pläne erforderlich machen.

6.4. ICT Continuity Reviews

(1) ICT Continuity Reviews beinhalten eine Bestandsaufnahme der relevanten Planungsdokumente und eine Bewertung, ob die Dokumente den definierten Prüfkriterien entsprechen. Es wird empfohlen, konsistente Prüfkriterien sowie klare Prozesse zur Überwachung und Behebung offener Punkte zu definieren.

6.5. ICT Continuity Tests

(1) Mit ICT Continuity Tests werden die Umsetzung der Planung und die Fähigkeit der Krisenmanagement-Organisation überprüft. Schwerpunkte sowie die Periodizität der einzelnen Tests sind in Abhängigkeit der Risikobeurteilung (vgl. Business Impact Analyse) festzulegen. Tests sollen realitätsnah und angepasst an die Risikosituation erfolgen. Durch Zusammenführen der Testergebnisse und insbesondere auch durch koordinierte Tests der Prozesseigner und der ICT-Verantwortlichen kann die Fähigkeit des Unternehmens zur Bewältigung von Krisensituationen gestärkt werden.

(2) Es wird empfohlen, die einzelnen Testaktivitäten in Form einer systematischen Testplanung zu koordinieren, die Berichterstattung einheitlich zu regeln sowie einen Prozess für die Überwachung und Behebung von Schwachstellen festzulegen. Insbesondere gibt ISO 27002 wertvolle Hinweise zu den möglichen zu schützenden und zu testenden Domänen.

(3) Es ist ein Test-/Übungsplan zu erstellen und von der Unternehmensleitung freizugeben. Neben dem korrekten Hinweis zur Dokumentation ist auch dringend zu empfehlen, dass bereits in der Planung die möglichen Risiken der Durchführung dokumentiert und der Unternehmensleitung mitgeteilt werden. Damit ist unter anderen die Frage angesprochen, was bei einer Übung passieren und wie die Übungsteilnehmenden darauf vorbereitet sind. Beispielsweise können durch die Verwendung einer isolierten Test-Umgebung und Daten-Backups Risiken bei der Testdurchführung vermieden werden.

(4) Die geplanten Übungen und Tests müssen in Zusammenarbeit mit den Geschäftsbereichen durchgeführt werden. Dabei sollten bei jeder Übung die Ziele für die jeweiligen Geschäftsbereiche und für das ICT Continuity Management festgelegt und überprüft werden. Der Test von einzelnen technischen Ressourcen – losgelöst von den Übungen der Geschäftsbereiche – wird lediglich als unterstützende Massnahme empfohlen. Wie auch bei anderen Standards (zum Beispiel BS 25999, BSI 100-4) wird empfohlen, dass sich der Schwierigkeitsgrad und die Komplexität der Übungen im Laufe der Zeit steigern sollen; vom Schreibtisch-Test bis hin zum physischen Live-Test der gesamten End-to-End-Kette einer Anwendung unter Berücksichtigung aller Ressourcen und Anwender. Nach der Festlegung der Mindestanforderungen an einen Test-Auftrag, hier ICT Continuity Tests genannt, gibt die Phase „Standard“ Hinweise zur Testdurchführung. Im Anschluss an diese Phase werden die Mindestinhalte in einem Bericht aufgeführt, der dem Auftraggeber der Übung zugestellt wird.

(5) Um sicherzustellen, dass alle Dokumente zum ICT Continuity laufend aktuell gehalten werden, stellt der Standard Anforderungen an Massnahmen zum Änderungsmanagement und zur Kontrolle aller ICT Continuity Management-relevanten Aufzeichnungen und Dokumente. Für das Management-Review des ICT Continuity Managements sind ähnliche Anforderungen wie der BS 25999 für BCM empfehlenswert. Als Beispiel sind hier angeführt:

- **Input**: Interne Service Level, Ergebnisse von relevanten Audits, Umsetzungsstatus von präventiven und korrektiven Massnahmen.
- **Output**: Angepasste Budgetanforderungen, ggf. angepasster Scope, Massnahmen zur Anpassung von Strategien oder Verfahren.

(6) Insbesondere wird die Durchführung von SCADA-Penetrationstests empfohlen. Für eine erfolgreiche Durchführung eines Penetrationstests, der den Erwartungen des Auftraggebers entspricht, ist eine klare Zielvereinbarung unerlässlich. Falls Ziele angestrebt werden, die nicht bzw. nicht effizient erreicht werden können, sollte der Tester in der Vorbereitungsphase deutlich darauf hinweisen und alternative Vorgehensweisen wie z. B. eine IT-Revision oder IT- Sicherheitsberatung empfehlen. Die Ziele des Auftraggebers, die mit einem SCADA-Penetrationstest erreicht werden können, lassen sich in vier Gruppen einteilen:

- Erhöhung der Sicherheit der technischen Systeme,
- Identifikation von Schwachstellen,
- Bestätigung der IT-Sicherheit durch einen externen Dritten,
- Erhöhung der Sicherheit der organisatorischen und personellen Infrastruktur.

(7) Im Ergebnis eines IT-Penetrationstests sollte daher nicht nur eine Auflistung vorhandener Schwachstellen vorhanden sein, sondern möglichst auch konkrete Lösungsvorschläge für deren Beseitigung aufgeführt werden.

(8) Im Rahmen eines SCADA Penetrationstests sollten dann auch logische IT-Sicherheitsmassnahmen wie z. B. Passwörter als auch physische Massnahmen wie Zutrittskontrollsysteme geprüft werden. Häufig werden nur logische Sicherheitsmassnahmen geprüft, da diese erstens grösstenteils aus der Ferne über das Netzwerk getestet werden können und somit weniger Aufwand erforderlich ist und zweitens die Wahrscheinlichkeit für Angriffe auf logische IT-Sicherheitsmassnahmen als ungleich grösser angesehen wird.

6.6. Kontinuierliche Verbesserung

(1) ICT Continuity Management ist ein iterativer Prozess. Resultate von durchgeführten Übungen und Tests, aber auch die Auswertung relevanter Ereignisse sollen zur kontinuierlichen Verbesserung des ICT Continuity Managements genutzt werden.

(2) Als solche Verbesserungen könnten die folgende Massnahmen zählen:

- Aufbau einer nationalen geschützten Vulnerability-Datenbank, deren Informationen regelmässig an Betreiber der Netzebenen 1-4 verteilt werden. Die Datenbank enthält im Sinne von Good und Best Practice Informationen zur Erkennung, der Abwehr und dem Umgang mit Gefährdungen von Komponenten, die für kritische Infrastrukturkomponenten bzw. kritische Geschäftsprozesse der Schweizer Stromübertragungs- und -verteilnetze benötigt werden. Zum Aufbau der Datenbank empfiehlt sich die enge Abstimmung mit den relevanten Aufsichtsstellen und Sicherheitsbehörden,
- Einrichtung eines nationalen Cyberlagebildes ENERGIE als Führungsinstrument mit entsprechenden Schnittstellen zu bestehenden Instrumenten und Plattformen des Austauschs cybersicherheitsrelevanter Informationen (z.B. MELANI, elektronische Lagedarstellung) sowie zu neuen Initiativen (z.B. nationale Cyber Defense-Strategie),
- Wirtschaftliche Anreize zur nationalen Entwicklung von technologischen und strategischen Technologien, um den „unbekannten Dritten“ keine Einblicke in die Strukturen und Systeme zu ermöglichen sowie – gestützt auf die Vulnerability-Datenbank – auch Aufbau einer genormten Devices-Datenbank („Sicherheitsgütesiegel“).

7. Handlungsempfehlungen zur Umsetzung ICT-CM Minimalstandard

7.1. Einleitung

(1) Die Handlungsempfehlungen sind entsprechend den in Kapitel 4.5, Abbildung 3, identifizierten kritischen Infrastrukturen strukturiert. Für verschiedene Infrastrukturen werden passende Handlungsempfehlungen formuliert.

(2) Die kritischen Infrastrukturen der EVUs sind gegen Ausfälle wie in Kapitel 4.2 definiert zu schützen.

(3) Auf nationaler Stufe mit ca. 7 GW Leistung ist eine unüberwachte Zeitspanne von 25 Sekunden unkritisch. Eine stufengerechte Verfügbarkeit kann mit entsprechenden Redundanzen (Notsysteme) gelöst werden.

(4) Für ein Verteilnetz mit ca. 500 MW Leistung ist eine unüberwachte Zeitspanne von 6 Minuten unkritisch; für ein einzelnes Unterwerk mit ca. 50 MW Leistung ist eine Stunde unkritisch. Je kleiner die Anschlussleistung, desto eher sind auch nichttechnische Massnahmen (Personaleinsatz) geeignet, Störungen zu beheben.

(5) Wie in Kapitel 4.3 eingeführt ist ein mögliches Konzept zur Sicherung der kritischen Infrastrukturen der Elektrizitätsunternehmen die Schaffung von Sicherheitsdomänen, welche durch kontrollierte Übergänge voneinander separiert sind.

(6) Die gesamte ICT Infrastruktur und die ICT Systeme müssen eine der jeweiligen Netzebene, insbesondere der Netzebenen 1 bis 4 angepasste Autonomiezeit im normalen und gestörten Netzbetrieb aufweisen.

(7) Die kritischen Applikationen sollen auf eigenen ICT Infrastrukturen und ICT Systemen betrieben werden.

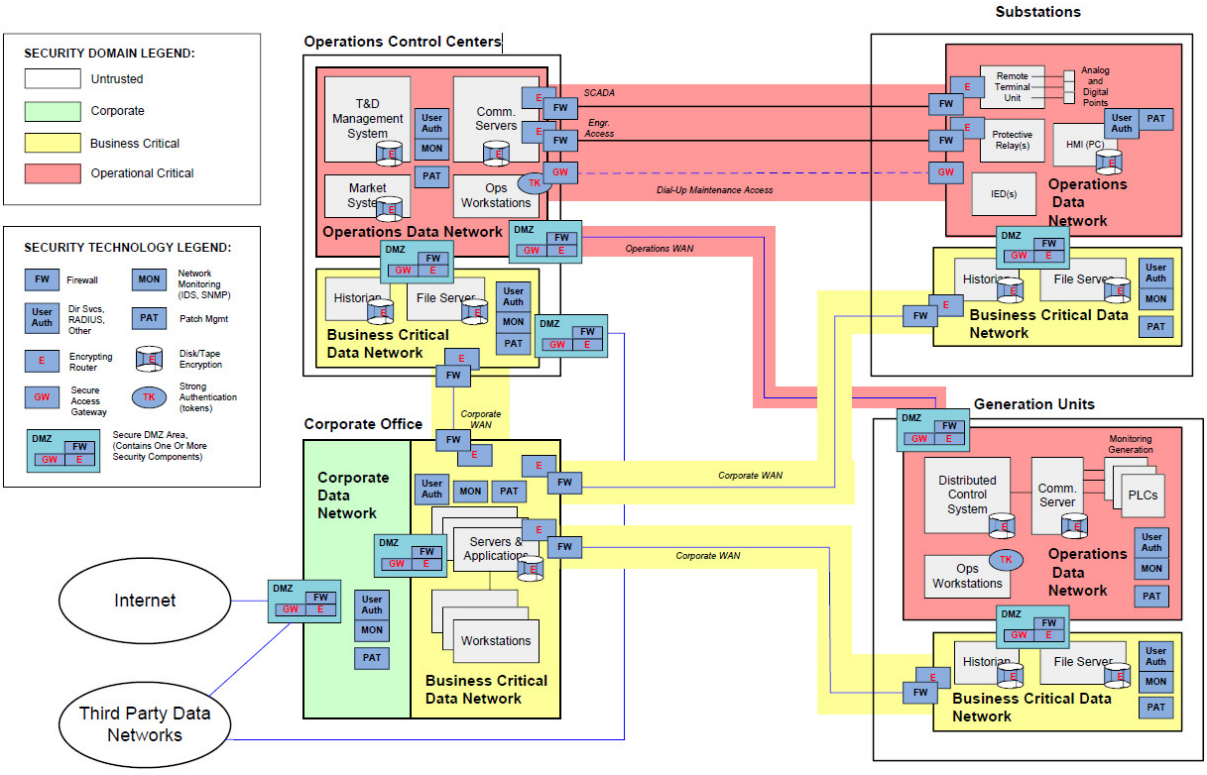


Abbildung 4: Beispiel sicherheitsorientierte ICT, Schaffung von Sicherheitsdomänen (Quelle [8])

(8) Zur Aufrechterhaltung der Leistungsfähigkeit müssen die Zuverlässigkeit und die Sicherheit (Integrität) von Bauteilen oder Komponenten, die bereits verbaut wurden, ohne dass die Unternehmen davon überhaupt Kenntnis haben, ausreichend geprüft und evaluiert werden.

(9) IT-spezifische Gefährdungen dürfen sich nicht negativ auf die gesteuerten Prozesse auswirken. Bei bestehenden Systemen muss auf eine bestmögliche Absicherung geachtet werden. Besonders bei neuen Systemen sollten zusätzliche Sicherheitseigenschaften implementiert werden, die die informationstechnischen Risiken weiter reduzieren. Dabei dürfen neu implementierte Lösungen keine weiteren Gefährdungen oder Single Points of Failure in die Systeme einführen.

(10) Es ist in jedem Fall den folgenden Punkten besondere Beachtung zu schenken:

a. Möglichst keine externen Zugänge (z. B. Internet, Intranet, Wartung) zum Prozesssteuerungsnetzwerk,
b. Unvermeidbare externe Zugänge müssen aufgrund des in der Regel sehr hohen Schutzbedarfs der Prozesssteuerungssysteme äußerst restriktiv ausgelegt und überwacht werden,
c. Technische Beschränkung des Netzwerkverkehrs auf den von den Steuerungssystemen benötigten Umfang; starke Segmentierung der Steuerungsnetze (zum Beispiel durch spezifische Sicherheits-Gateways (Firewalls)); restriktives Management der erlaubten Kommunikationsbeziehungen,
d. Systeme und Komponenten der Prozesssteuerung sollten:
    - nur die zum Betrieb notwendigen Leistungsmerkmale bieten (insbesondere keine Funktionalitäten, die ein Risiko für die Prozesssteuerung darstellen),
    - robust gegenüber Störungen und Angriffsversuchen sein,
    - über sichere systemspezifische Authentifizierungsmechanismen verfügen.
e. Langfristige Verfügbarkeit von Ersatzteilen, Updates und Systemwartung – entsprechend der Lebensdauer der Prozessinfrastruktur; möglichst offene Migrationspfade,
f. Möglichkeiten zum Einspielen von notwendigen Patches (was insbesondere bei Systemen mit 24/7/365-Anforderungen oft eine Herausforderung darstellt); eine schnelle Verfügbarkeit von getesteten Sicherheits-Patches sollte ein Kriterium bei der Auswahl des Herstellers der Prozessleittechnik sein.

7.2. Zentrales Netzleitsystem / Netzleittechnik (SCADA)

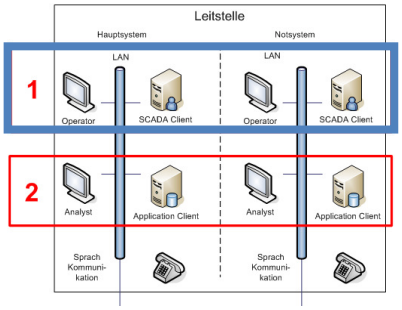
7.2.1. Quantifizierte Vorgabe

(1) Die pro Ereignis auf Stufe Netzleitsystem / Netzleittechnik (SCADA) nicht zeitgerecht gelieferten Energie (NZGE) soll 50 MWh nicht übersteigen.

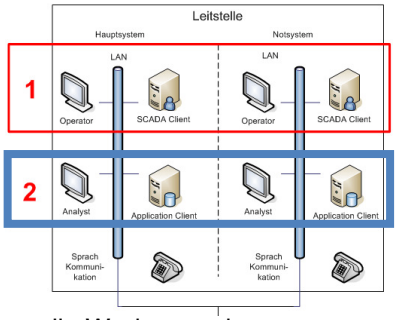
7.2.2. Empfehlung

(1) Das Netzleitsystem soll vollständig funktional redundant ausgelegt sein. Das redundante System soll örtlich getrennt in einer anderen Geländekammer platziert werden.

(2) Bei Netzleitsystem / Netzleittechnik (SCADA) mit geringer Anzahl gesteuerter Werke können alternative Massnahmen eingesetzt werden (z.B. eine geringere örtliche Trennung, Führung von Notalarmen auf weitere dezentrale Standorte oder eine rasche Steuerung vor Ort).



7.3. Kritische Applikationen der Netzführung



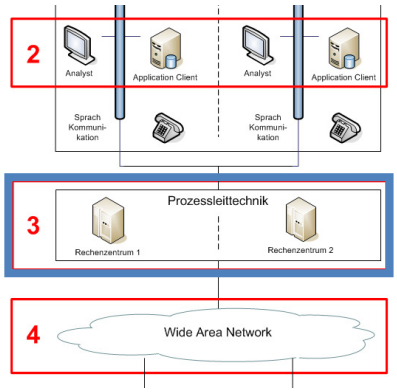
7.3.1. Quantifizierte Vorgabe

(1) Die pro Ereignis auf Stufe kritische Applikation unanalysiert (z.B. ohne (n-1) Sicherheitsrechnung) gelieferte Energie soll 50 MWh nicht übersteigen.

7.3.2. Empfehlung

(1) Die Verfügbarkeit der kritischen Applikationen soll den Anforderungen entsprechend verfügbar ausgelegt werden. Zudem sollen manuelle Workarounds zur Verfügung stehen.

7.4. Rechenzentrum



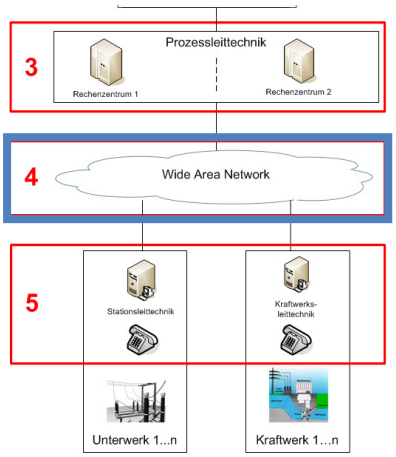
7.4.1. Quantifizierte Vorgabe

(1) Die pro Ereignis auf Stufe Rechenzentrum nicht zeitgerecht gelieferten Energie (NZGE) soll 50 MWh nicht übersteigen.

7.4.2. Empfehlung

(1) Rechenzentren sollen vollständig funktional redundant ausgelegt und möglichst verteilt auf zwei unterschiedliche Geländekammern platziert werden. Bei geringer Anzahl gesteuerter Werke können alternative adäquate Massnahmen eingesetzt werden.

7.5. Telekommunikationstechnik und Infrastruktur



7.5.1. Quantifizierte Vorgabe

(1) Die pro Ereignis auf Stufe Telekommunikationstechnik und Infrastruktur nicht zeitgerecht gelieferten Energie (NZGE) soll 50 MWh nicht übersteigen.

7.5.2. Empfehlung

(1) Alle Kraft- und Unterwerke der Netzebenen 1 bis 4 sollen physikalisch redundant über getrennte Telecom Trassen angebunden sein. Die Prozess ICT (SCADA) muss von der Büro ICT[3] und der kommerziellen ICT[4] mindestens logisch, besser physisch getrennt sein. Es soll zwischen den verschiedenen ICT Nutzungen nur (z.B. durch Firewalls) kontrollierte Übergänge geben. Die Netzzu-

[3] z.B. SAP oder MS Office

[4] z.B. verkaufte Bandbreite an Telecom Provider oder FTTH

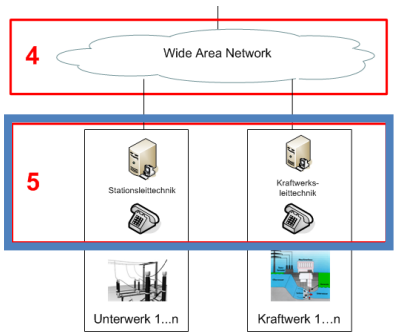
gänge sind mit Sicherheitsmassnahmen gemäss dem Stand der Technik (z.B. Authentifizierung und Verschlüsselung) auszurüsten.

(2) Eine stufengerecht gesicherte Sprachkommunikation (EW-Telefonnetz, rotes Telefon, Betriebsfunk usw.) muss verfügbar sein. Alle Kommunikationswege müssen über eine geeignete Selbstüberwachung (Watch Dog) verfügen, sodass ein Unterbruch umgehend erkannt und behoben werden kann.

7.6. Stationsleittechnik (Unterwerke und Kraftwerke)

7.6.1. Quantifizierte Vorgabe

(1) Die pro Ereignis auf Stufe Stationsleittechnik Netzebene 1 bis 4 nicht zeitgerecht gelieferten Energie (NZGE) soll 50 MWh nicht übersteigen.



7.6.2. Empfehlung

(1) Eine manuelle Feldsteuerung vor Ort muss möglich sein. Für komplexe Anlagen wird ein Vorort Bedienplatz im Werk empfohlen. Die Interventionszeit des Pikettdienstes ist gemäss der quantifizierten Vorgabe für jedes Werk auszulegen. Die internen Netzwerke und der externe Zugriff (z.B. Pikett oder Lieferanten) sollen mit Sicherheitsmassnahmen gemäss dem Stand der Technik (z.B. Authentifizierung und Verschlüsselung) ausgerüstet werden. Ersatzmaterial aller kritischen Komponenten ist bereitzuhalten.

8. Weitere Literatur

(1) Folgende Dokumente können die Stromversorgungsunternehmen bei der Umsetzung der vorliegenden Branchenempfehlung unterstützen:

Titel	Autor / Herausgeber	Datum	Link / Datei
IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management	ISO/IEC 27002	2008	http://de.wikipedia.org/wiki/ISO/IEC_27002
Security for Information Systems and Intranets in Electric Power Systems, Technical Brochure N°317	Cigré	April 2007	http://www.cigre.org/
Viking Project	EU financed Framework 7 Collaborative STREP Project	Nov. 2008 bis Okt. 2011	http://www.vikingproject.eu
Gefährdungsanalyse der WL	Bundesamt für wirtschaftliche Landesversorgung BWL	Mai 2010	http://www.bwl.adadm.ch/themen
Critical infrastructure protection for the smart grid	Accenture	2010	http://www.accenture.com/us-en/Pages/insight-critical-infrastructure-protection-smart-grid.aspx
Reliability Standards for the Bulk Electric Systems of North America	NERC - North American Electric Reliability Corporation	2008 - 2011	http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf
Meeting NERC CIP requirements with Cooper Power Systems IED Integration and Automation Solutions	Cooper Power Systems	März 2009	http://compliance.npcc.org/Documents/TFE%20Library/Cooper%20Power%20Systems%20-%20IED%20Intergration%20-%20Meeting%20NERC%20CIP%20requirements.pdf
ITIL Service Design	IT Infrastructure Library (ITIL)	2007	http://de.wikipedia.org/wiki/ITIL_V3_Service_Design

Tabelle 2: Unterstützende Dokumente für die Umsetzung der Branchenempfehlung

(2) Im Rahmen der Cyber Defense Strategy Schweiz wird der Bund eine gesamtheitliche Strategie des Bundes gegen Cyber-Bedrohungen ausarbeiten. Wegen der drastischen Auswirkungen bei einem grossräumigen Ausfall kommt der Stromversorgung dabei eine zentrale Bedeutung zu. Dabei geht es vor allem um ein Konzept, welches beschreibt, wie sich die (staatlichen und privaten) Betreiber von kritischen Infrastrukturen gegen Cyber-Attacken wappnen.

(3) ISO 27002 beinhaltet wertvolle Hinweise zu den möglichen zu schützenden und zu testenden Domänen:

- Domäne ISO 27002 9- Physische und umgebungsbezogene Sicherheit, Objektive ISO 27002 9.1 et 9.2
- Domäne ISO 27002 10- Betriebs- und Kommunikationsmanagement, Objektive ISO 27002 10.1, 10.5, 10.6 et 10.10
- Domäne ISO 27002 11- Zugangskontrolle Objektive ISO 27002 11.1, 11.2 et 11.6
- Domäne ISO 27002 12- Beschaffung, Entwicklung und Wartung von Informationssystemen: Objektive ISO 27002 12.2 et 12.5
- Domäne ISO 27002 13- Umgang mit Informationssicherheitsvorfällen: Objektive ISO 27002 13.1