Branchenempfehlung

Physische Sicherheit für Unterwerke

Netzebene 1 und tiefer (bei mit Netzebene 1 gemeinsam genutzten Unterwerken)

PSU – CH 2019

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

Telefon +41 62 825 25 25, Fax +41 62 825 25 26, info@strom.ch, www.strom.ch

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 Erstausgabe

Christian Brütsch	Repower	
Heinz Götschi	SBB Energie	ab Juni 2017
Beat Hanselmann	Stadtwerk Winterthur	
Robert Hauser	ewz	
Hans-Peter Mölbert	Swissgrid	
Lukas Petrig	Alpiq	
Theodor Pfister	BKW	
Beat Schüpbach	Swissgrid	Leiter der Arbeitsgruppe
Olivier Stössel	VSE / AES	Sekretär Ko EVU - TSO
Beat Stucki	SBB Energie	bis Juni 2017
Martin Wolf	CKW	
Roland Ziegler	Axpo	

Verantwortung Kommission
Für die Pflege und die Weiterentwicklung des Dokuments zeichnet die VSE-Kommission EVU - TSO verantwortlich.

Chronologie

Juli 2016 bis August 2018	Erarbeitung des Dokuments
November 2018 bis Februar 2019	Vernehmlassung
5. Mai 2019	Genehmigung im VSE Vorstand

Das Dokument wurde unter Einbezug und Mithilfe von VSE und Branchenvertretern erarbeitet.

Der VSE verabschiedete das Dokument am 05.05.2019.

Druckschrift Nr. PSU/d, Ausgabe 2019

Sprachliche Gleichstellung der Geschlechter.
Das Dokument ist im Sinne der einfacheren Lesbarkeit in der männlichen Form gehalten. Alle Rollen und Personenbezeichnungen beziehen sich jedoch sowohl auf Frauen wie auch auf Männer. Wir danken für Ihr Verständnis.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

Beim vorliegenden Dokument handelt es sich um ein Branchendokument des VSE. Es ist Teil eines umfassenden Regelwerkes für die Elektrizitätsversorgung im offenen Strommarkt. Branchendokumente beinhalten branchenweit anerkannte Richtlinien und Empfehlungen zur Nutzung der Strommärkte und der Organisation des Energiegeschäftes und erfüllen damit die Vorgabe des Stromversorgungsgesetzes (StromVG) sowie der Stromversorgungsverordnung (StromVV) an die Energieversorgungsunternehmen (EVU).

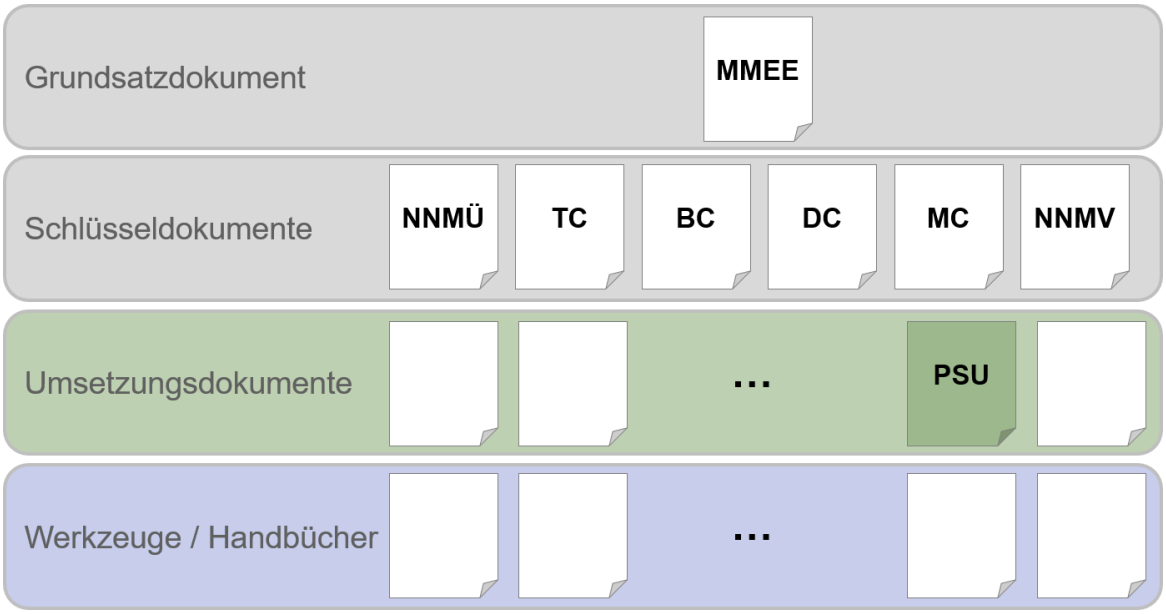
Branchendokumente werden von Branchenexperten im Sinne des Subsidiaritätsprinzips ausgearbeitet, regelmässig aktualisiert und erweitert. Bei den Bestimmungen, welche als Richtlinien im Sinne des StromVV gelten, handelt es sich um Selbstregulierungsnormen.

Die Dokumente sind hierarchisch in vier unterschiedliche Stufen gegliedert

- Grundsatzdokument: Marktmodell für die elektrische Energie – Schweiz (MMEE – CH)
- Schlüsseldokumente
- Umsetzungsdokumente
- Werkzeuge/Software

Beim vorliegenden Dokument Standard physische Sicherheit für Unterwerke handelt es sich um ein Umsetzungsdokument.

Dokumentstruktur



Summary

Basierend auf dem SKI-Leitfaden des Bundesamtes für Bevölkerungsschutz (BABS), wird im vorliegenden Dokument eine Wegleitung zur effizienten und effektiven Entwicklung von Sicherungsmassnahmen im Bereich der Unterwerke der Netzebenen 1 und tiefer (bei mit Netzebene 1 gemeinsam genutzten Unterwerken) dargestellt.

Gleichzeitig liefert das Dokument einen Überblick über die empfohlenen Minimalstandards im Bereich des physischen Schutzes von Unterwerken. Dieses Dokument kann aber auch als Leitfaden für den Schutz von Unterwerken ohne Netzebene 1 Anlagen dienen. Dies setzt aber voraus, dass die hierfür erforderlichen Vorarbeiten wie beispielsweise die Definition der Kritikalität der Anlagen und die Risikobetrachtung ebenfalls durchgeführt werden.

Ausgehend von einer umfangreichen Analyse bestehender Bedrohungen und den daraus abgeleiteten relevanten Gefährdungen, werden die daraus resultierenden Risiken (Eintretenswahrscheinlichkeit und mögliches Schadensausmass) ermittelt und dargestellt. Diese Analyse sollte für jedes Unterwerk oder für eine Gruppe gleichartiger Unterwerke durchgeführt werden.

In einem nächsten Schritt werden die Schutzziele entwickelt. Diese können je nach Unternehmung und Bedeutung der Anlage unterschiedlich sein.

Abgeleitet von diesen Schutzzielen werden anschliessend die geeigneten Massnahmen zur Reduktion der erkannten Risiken entwickelt.

So werden beispielsweise technische Lösungen für den Perimeterschutz eines Unterwerkes aufgezeigt. Dazu gehört insbesondere die Empfehlung, bereits beim Grundschutz elektronische Schliesssysteme einzusetzen.

Hierzu wird sinnvollerweise die Kritikalität eines Unterwerkes (Bedeutung der Anlage für das Gesamtnetz und damit für die Versorgungssicherheit) in die Planung mit einbezogen.

Die im Dokument formulierten Standards berücksichtigen zudem die unterschiedlichen regulatorischen und gesetzlichen Standards, welche ihren Ausdruck in der Definition des sogenannten Grundschutzes finden.

Weiter gehende Massnahmen, welche eine stärkere Berücksichtigung der Risikobetrachtung beinhalten, widerspiegeln sich in den Massnahmen „mittlerer“ und „hoher“ Schutz. Damit kann sichergestellt werden, dass die künftigen Investitionen und Massnahmen im Sicherheitsbereich risikogerecht eingesetzt werden.

In einem weiteren Schritt wird – nebst den bereits dargestellten technischen Lösungen – zudem auf die Bedeutung von betrieblichen und prozessualen Massnahmen (Awareness Schulungen etc.) hingewiesen.

Unter dem Wissen, dass nur eine integrale Sicherheitsbetrachtung eine wirkungsvolle und sinnvolle Gesamtlösung darstellen kann, wird zum Schluss des Dokumentes noch auf das Zusammenspiel der physischen Schutzmassnahmen mit denjenigen aus dem Bereich der Cyber Sicherheit hingewiesen.

Einleitung

Aufgrund der Entflechtungen in der Elektrizitätswirtschaft in den letzten Jahren hat sich die schweizerische Stromlandschaft auch bezüglich der Risikobetrachtung verändert. Mit der Übernahme des Übertragungsnetzes durch die nationale Netzgesellschaft entstand neu das Risiko eines Gesamtausfalles des Netzes, da beispielsweise die Steuerung des Übertragungsnetzes zentral vorgenommen wird. Dieses kumulative Ausfallrisiko bestand vorher in dieser Art nicht.

Erschwerend kommt hinzu, dass in den letzten Jahren ein Wandel hin zur Informationstechnologie stattgefunden hat, welcher auch neue Risiken mit sich bringt. Diese müssen durch die Energieunternehmen anerkannt, bewertet und behandelt werden, um den gesetzlichen Auftrag gemäss Stromversorgungsgesetz, Stromversorgungsverordnung oder dem Energiegesetz erfüllen zu können.

Durch das Bundesamt für wirtschaftliche Landesversorgung (BWL) hat eine Risiko- und Verwundbarkeitsanalyse des Teilsektors Stromversorgung durchgeführt. Dies führte (auszugsweise) zu folgenden Erkenntnissen:

- Entlang der gesamten Versorgungskette ist die Produktion von Strom in den Kraft- und Unterwerken heute weniger stark verwundbar hinsichtlich (IKT-) Gefährdungen als der Betrieb der Verteil- und Übertragungsnetze.
- Die Gefährdung durch Mitarbeitende, welche absichtliche oder unabsichtliche Fehlmanipulationen an kritischen Systemen vornehmen, ist ebenfalls signifikant und nimmt durch den Zentralisierungsprozess bei den Leitstellen weiter zu.
- Insgesamt wird die IKT-Verwundbarkeit der Stromversorgung in Zukunft weiter zunehmen.

Das Bundesamt für Bevölkerungsschutz (BABS) erarbeitete in enger Zusammenarbeit mit Betreibern kritischer Infrastrukturen einen sogenannten „Leitfaden SKI“, welcher den Betreibern kritischer Infrastrukturen eine methodische Vorgehensweise zu einem bedarfsgerechten Schutz ihrer Infrastrukturen liefert.

Zusammenfassend kann festgehalten werden, dass mit Ausnahme der Kernenergieanlagen, welche bereits heute weitreichenden regulatorischen Vorschriften des Eidgenössischen Nuklearinspektorats ENSI unterliegen, zum heutigen Zeitpunkt (rechtlich) kaum oder nur wenige verbindlichen Vorgaben bezüglich der physischen Sicherheit der Anlagen der Betreiber kritischer Strominfrastrukturen bestehen.

Das neue Landesversorgungsgesetz, welches per 01.06.2017 in Kraft getreten ist, gibt dem Bundesamt für wirtschaftliche Landesversorgung (BWL) neu jedoch auch die Kompetenz, subsidiär präventive Massnahmen zur Sicherstellung der Energieversorgung umzusetzen.

Diese fehlenden Vorgaben im Bereich der physischen Schutzmassnahmen sollen durch den hier vorliegenden Minimalstandard – welcher eine solche präventive Massnahme im Sinne des Landesversorgungsgesetzes ist - unter Berücksichtigung des SKI-Leitfadens des BABS geschlossen werden.

Das vorliegende Dokument wurde in der Folge in einer VSE Arbeitsgruppe erarbeitet. Dies mit dem Ziel, zwischen Übertragungsnetzeigentümer und den Netz- und Kraftwerkseigentümern der gemeinsamen Unterwerke einerseits ein verbindliches und akzeptiertes Branchendokument und andererseits einen konkretisierten Mindeststandard auf Basis eines Risiko-Assessments für die Schweizer Strombranche zu erarbeiten.

Hierbei sind Massnahmen zum physischen Schutz vor unberechtigtem Zutritt, mutwilliger Beschädigung und Beeinträchtigung der Stromversorgungssysteme zu definieren. Die Massnahmen gelten grundsätzlich

für Anlagen der Netzebene 1 und auch für Anlagen in tieferen Netzebenen, sofern diese baulich nicht von der Netzebene 1 getrennt sind oder nicht unabhängig von dieser betrieben werden können.

Grundsätzlich kann die Methodik des Dokuments auch für Unterwerke ausserhalb der Netzebene 1 angewendet werden.

1. Abgrenzung

(1) Aufgrund weitgehend fehlender gesetzlicher Grundlagen bezüglich physischer Schutzmassnahmen verfolgt diese Branchenempfehlung einen risikobasierten Ansatz, welcher sich am SKI-Leitfaden des BABS orientiert. Damit sollen die wesentlichen Risiken im Bereich der physischen Sicherheit adressiert werden. Ziel des Dokumentes ist es – insbesondere auch unter Berücksichtigung der speziellen Konstellation der Schnittstellen zwischen Übertragungsnetz und Verteilnetz - , den Sicherheitsverantwortlichen der Schweizer Energieversorgungsunternehmungen (EVU) eine Methodik und Anleitung zur Verfügung zu stellen, um die relevanten Sicherheitsrisiken bezüglich ihrer Unterwerke evaluieren und beurteilen zu können. Gleichzeitig werden verhältnismässige Sicherheitsmassnahmen erarbeitet, welche die wesentlichen Risiken bedarfsgerecht adressieren. Um diesen Prozess zu erleichtern, liefert das Dokument einen Überblick über aktuelle Umsetzungsmöglichkeiten. Hierbei wird die Bedeutung des zu schützenden Gutes mitberücksichtigt. Basierend auf diesen Empfehlungen werden Massnahmen für einen physischen Grundschutz definiert und einen erweiterten physischen Schutz exemplarisch dargestellt.

(2) Dies leistet einen wesentlichen Beitrag zur Erhöhung der Resilienz und dadurch zur Erhöhung der Versorgungssicherheit.

(3) Die Empfehlungen des vorliegenden Dokumentes stehen in einer engen Verbindung zu der VSE Branchenempfehlung „OT Grundschutz für kritische Infrastrukturen in der Stromversorgung“. Beide Branchenempfehlungen sollen sich gegenseitig unterstützen und nach Möglichkeit ergänzen.

(4) Bestehende Standards (wie beispielsweise ISO, NERC, und andere) werden für die Erarbeitung der Branchenempfehlung berücksichtigt. Gewisse darin enthaltenen Grundsätze oder Empfehlungen (Beispielsweise die Frage der Definition eines kritischen Anlagenteils) wurden in die Erarbeitung des vorliegenden Standards aufgenommen.

1.1 Inhaltliche Abgrenzung

(1) Die elektrische und betriebliche Sicherheit der Betriebsmittel des Stromnetzes sowie Fragestellungen hinsichtlich von Massnahmen zum Personenschutz und zur Arbeitssicherheit (diesbezüglich gelten die Bestimmungen der Starkstromverordnung, SUVA, UVG etc.) sind nicht Bestandteil dieser Branchenempfehlung.

(2) Das Dokument gilt für Unterwerke der Netzebene 1 und tiefer (bei mit Netzebene 1 gemeinsam genutzten Unterwerken). Diese grundsätzliche Methodik kann aber auch für Unterwerke in tieferen Netzebenen angewendet werden.

(3) Ebenfalls nicht Gegenstand des Dokumentes ist die Frage der Kostentragung. Hierzu wird auf die bestehenden regulatorischen und rechtlichen Grundlagen verwiesen.

(4) Naturgefahren, Tiere und Meteo-Risiken (Erdbeben, Hochwasser, Erdrutsch, etc.) werden in diesem Dokument nicht bearbeitet. Diese Themen sind im Rahmen der Baubewilligungsphase anhand der örtlichen Gegebenheiten und den gesetzlichen Bestimmungen zu klären.

1.2 Bestehende rechtliche Grundlagen und nationaler Kontext

1.2.1 Bezug zum nationalen Kontext

(1) Der Bundesrat hat am 27. Juni 2012 die nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) verabschiedet und das Bundesamt für Bevölkerungsschutz mit der Koordination bei der Umsetzung der Strategie beauftragt. Die nationale SKI-Strategie bezeichnet insgesamt 15 Massnahmen, mit denen die Widerstandsfähigkeit (Resilienz) der Schweiz im Hinblick auf Ausfälle und Störungen kritischer Infrastrukturen verbessert werden soll. Als zentrale Eckpfeiler sind etwa die Führung eines Verzeichnisses der kritischen Infrastruktur-Objekte und die Erarbeitung von Einsatzplanungen zur Unterstützung der Betreiber beim Schutz dieser Objekte im Falle von Katastrophen und Notlagen durch die Partner des Bevölkerungsschutzes und der Armee vorgesehen. Diese Strategie wurde mit Beschluss des Bundesrates vom 8. Dezember 2017 zur nationalen SKI-Strategie 2018-22 ersetzt. Der Leitfaden SKI des BABS sowie die Nationale SKI-Strategie können auf der Homepage des BABS heruntergeladen werden (www.babs.admin.ch).

(2) Ein weiterer Schwerpunkt stellt die Stärkung der Widerstandsfähigkeit der kritischen Infrastrukturen an und für sich dar. Diesbezüglich hat der Bundesrat die zuständigen Stellen (Fachbehörden, Betreiber Kritischer Infrastrukturen usw.) – im Rahmen der Nationalen SKI-Strategie, Massnahme M15 - beauftragt, die bestehenden Risiken zu überprüfen und bei Bedarf Massnahmen zur Stärkung der Resilienz der kritischen Infrastrukturen zu treffen. Das BABS hat diesbezüglich einen Leitfaden erarbeitet, der das methodische Vorgehen und die zu berücksichtigenden Aspekte beschreibt. Der Leitfaden wurde im Rahmen der Arbeitsgruppe SKI erarbeitet, in der die zuständigen Bundesstellen aus allen Departementen sowie die Kantone vertreten sind. Er wurde zudem einer fachlichen Konsultation bei Verbänden, Betreibern und kantonalen Konferenzen unterzogen. Im Rahmen eines Pilotprojekts wurde der Leitfaden anhand des Übertragungsnetzbetreibers Swissgrid umgesetzt. Die Umsetzung erfolgte dabei in Zusammenarbeit mit der Swissgrid und den zuständigen Fachbehörden (u.a. BFE, ElCom und BWL). Der SKI-Leitfaden orientiert sich dabei auch an den Arbeiten zur Definition und Umsetzung der nationalen Strategien zum Schutz kritischer Infrastrukturen und zum Schutz der Schweiz vor Cyber-Risiken.

(3) Der Schlussbericht "Pilotprojekt Leitfaden Swissgrid" beschränkt sich auf den Bereich des Übertragungsnetzes gemäss Stromversorgungsverordnung (StromVV). Anhand exemplarischer und beispielhafter Risiken werden Vorgehensweisen und daraus resultierende Sicherheitsstandards berücksichtigt. Ziel des Dokumentes ist es, den Unternehmen geeignete, risikobasierte Sicherungsansätze, abgestimmt auf die entsprechende unternehmensspezifische Situation aufzuzeigen.

1.2.2 Auslegeordnung über bereits bestehende gesetzliche Regelungen

(1) Gemäss Art. 8 StromVG sind die Netzbetreiber verpflichtet, ein „sicheres, leistungsfähiges und effizientes Netz“ zu gewährleisten. Dabei wird weder im StromVG noch in der StromVV präzisiert, welches Niveau an Sicherheit erreicht werden soll. Weiter kann zwar das Bundesamt für Energie BFE gemäss StromVV „technische und administrative Mindestanforderungen an ein sicheres, leistungsfähiges und effizientes Netz festlegen“, in Bezug auf den integralen Schutz des Netzes bestehen derzeit aber noch keine Bestimmungen.

(2) Seitens des ESTI (Eidgenössisches Starkstrominspektorat) werden verschiedene technische und betriebliche Regulatorien vorgegeben. Im Sicherheitsbereich sind ebenfalls gewisse Grundlagen in der Starkstromverordnung enthalten, wie beispielsweise die Definition der Mindestzaunhöhe.

1.2.2.1 Allgemeine Grundlagen

- Nationale Strategie Schutz kritischer Infrastrukturen SKI inkl. Umsetzungsplan
- Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS inkl. Umsetzungsplan

1.2.2.2 Relevante spezifische Rechtsgrundlagen

- Bundesgesetz über die wirtschaftliche Landesversorgung (LVG), 8. Oktober 1982 (Stand 1. Juni2017)
- Bevölkerungs- und Zivilschutzgesetz (BZG), 4. Oktober 2002 (Stand 1. Januar 2017)
- Energiegesetz (EnG), 26. Juni 1998, (Stand 1. Januar 2018)
- Energieverordnung (EnV), 7. Dezember 1998, (Stand 1. Januar 2018)
- Stromversorgungsgesetz (StromVG), 23. März 2007 (Stand 1. Januar 2018)
- Stromversorgungsverordnung (StromVV), 14 März 2008 (Stand 23. Mai 2018)

1.2.2.3 Relevante Vorarbeiten der Behörden

- **Bundesamt für wirtschaftliche Landesversorgung BWL**
  - Risikoanalyse Bereich ICT-Infrastruktur Sektor elektrische Energie (Leittechnik, Daten- und Sprach-kommunikation), Bern, 2011
  - Risiko- und Verwundbarkeitsanalyse des Teilsektors Stromversorgung
- **Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS)**
  - Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

- **Bundesamt für Bevölkerungsschutz BABS**
  - Arbeiten SKI-Inventar, Bern, 2014
  - Leitfaden SKI, Bern, 2014
  - Risikobericht 2012, Katastrophen und Notlagen Schweiz, Bern 2013

1.2.2.4 Relevante Vorarbeiten der Branchen / Branchenverbände

- **Verband schweizerische Elektrizitätsunternehmungen (VSE)**
  - Branchenempfehlung Strommarkt Schweiz, ICT-Continuity, Aarau, Dezember 2011
- **North American Electric Reliability Corporation (NERC)**
  - NERC CIP – Critical Infrastructure Protection, 2006 ff
- **Bundesamt für Sicherheit in der Informationstechnik (BSI, DE)**
  - IT-Grundschutz-Kataloge, 2016
- **Nationale Netzgesellschaft / VSE**
  - Vorgehen bei Last- und/oder Produktionsausfall grösser 400 MW, Frick, Januar 2013
  - Branchenvereinbarung Strommarkt Schweiz, Transmission Code 2013

2. Methodik

2.1 Methodische Vorgehensweise

(1) Das gewählte Vorgehen orientiert sich an den Grundlagen des Leitfadens SKI des Bundeamtes für Bevölkerungsschutz (BABS). Dieser Leitfaden wiederum orientiert sich an etablierten Konzepten und Standards in den Bereichen Risiko-, Kontinuitäts- und Krisenmanagement (z.B. ISO 31000, ISO 22301, BS 25999, ISO 27001). Der im Leitfaden abgebildete Regelkreis zum Schutz von kritischen Infrastrukturen wurde auf die Situation „Unterwerk“ adaptiert.

(2) Dies hat zur Folge, dass der Regelkreis um eine zusätzliche Betrachtungsgrösse (Kritikalität) ergänzt worden ist.

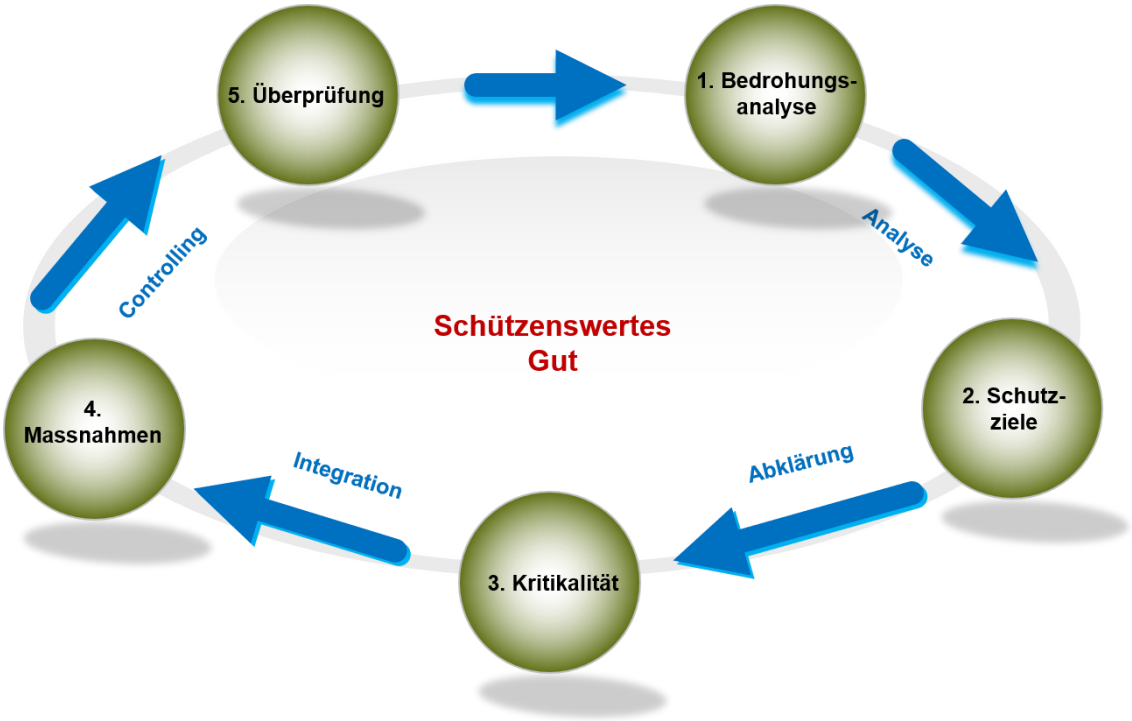


Abbildung 1 Regelkreis methodisches Vorgehen

2.2 Schritt 1: Bedrohungsanalyse

(1) Ziel der Bedrohungsanalyse ist es, mittels einer Analyse die kritischen Prozesse und Infrastrukturen auf einem Unterwerk zu identifizieren, eine Gefährdungsanalyse dafür durchzuführen und am Schluss eine priorisierte Liste der kritischen Funktionalitäten, Prozesse und Infrastrukturen als Grundlage für die Definition der Schutzziele zu erhalten.

(2) Voraussetzung für diese Tätigkeit sind klare Kenntnisse über die Bedeutung, Aufgabe und Funktionalität des betroffenen Unterwerks. Erst mit diesem Wissen kann beurteilt werden, welche Prozesse, Infrastrukturen etc. zwingend erforderlich sind um die Funktionalität des Systems Unterwerk gewährleisten zu können.

(3) In einem nächsten Schritt sind die kritischen Elemente eines Unterwerkes zu bezeichnen, deren Störung oder Ausfall zu einer Beeinträchtigung oder im Extremfall zu einem Ausfall des Unterwerkes führen könnten.

(4) Anschliessend werden relevante Gefährdungen identifiziert, die zu einer Störung oder einem Ausfall dieser kritischen Elemente führen können. Relevant ist eine Gefährdung dann, wenn diese die Funktionsfähigkeit des kritischen Elementes signifikant beeinträchtigen könnte.

(5) In einem nächsten Schritt sind für diese Gefährdungen spezifische Szenarien zu definieren, die mögliche Ereignisabläufe beschreiben. Für einzelne Gefährdungen können hierbei mehrere Szenarien ausgewählt resp. beschrieben werden (Gefährdungsbetrachtung).

(6) Nachfolgend werden für die jeweiligen massgebenden Szenarien die Risiken ermittelt und bewertet. Für eine graphische Darstellung ist die Erstellung einer Risikomatrix zu empfehlen. Hierbei findet die Einschätzung einer Eintretenswahrscheinlichkeit (W) und des aus dem Ereignis resultierenden Schadens (S) statt (siehe auch VSE-Dokument „Grundschutz OT in der Stromversorgung“).

(7) Mittels einer anschliessenden Quantifizierung der Risiken (Eintretenswahrscheinlichkeit x Schadensausmass) können die relevanten Bedrohungen Risiken monetär erfasst, beurteilt und dargestellt werden (Risikobetrachtung).

2.2.1 Gefährdungsbetrachtung

(1) Aufgrund fehlender gesetzlicher Vorgaben kann im Bereich der physischen Sicherheit ein umfassender Grundschutz nicht direkt abgeleitet werden. Deshalb orientiert sich dieses Dokument weitgehend an anerkannten „Best Practice – Ansätzen“.

(2) Um geeignete Schutzmassnahmen ermitteln zu können, ist es unabdingbar sich in einem ersten Schritt mit der Bedrohungssituation auseinander zu setzen.

(3) So verweist beispielsweise das BABS als Referenzereignis auf einen sogenannten „konventionellen Anschlag“ in Abgrenzung zu A-, B-, oder C-Anschlägen (BABS, Nationale Gefährdungsanalyse – Gefährdungsdossier Konventioneller Anschlag, 30. Juni 2015.)

(4) Konventionelle Anschläge (als mutwillige Aktionen gegen die physische Sicherheit) können in verschiedenen Ausprägungen und mehreren Bedrohungskategorien auftreten.

(5) Angelehnt an die Definition einer Bedrohungspyramide des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Deutschland, wurde eine entsprechende Bedrohungspyramide für physische Bedrohungen erstellt (Abbildung 2). Die Pyramide stellt mögliche Angreifer Gruppen dar, welche mit zunehmender Höhe der Pyramide professioneller hinsichtlich ihrer Bedrohungsebene wird. Die Spitze der Pyramide stellt folgerichtig ein staatlicher Akt (Krieg) dar.

(6) Treffen identifizierte Bedrohungen auf eine Schwachstelle (Sicherheitslücke), so entsteht ein Risiko für das zu schützende Gut. Diese Lücke kann entweder mit Schutzmassnahmen geschlossen oder aber das Risiko akzeptiert werden (Risikobereitschaft, siehe Kapitel 2.2.2.2).

(7) Bedrohungen gehen von verschiedenen Akteuren aus, welche unterschiedlichen Stufen von Wissen, Ausbildung, logistische Unterstützung, Ressourcen und Motivationen besitzen.

Abbildung 2 Bedrohungspyramide

Bedrohungsebene		Beschreibung	Schaden
B 1	Vandalen Gelegenheitstäter	Angreifer verfügen häufig über kein sehr fundiertes Wissen. Sie nutzen eine günstige Gelegenheit und sind auf kleine Delikte (Vandalismus) oder Diebstahl aus. Es kommen keine ausgefeilten Techniken oder Ressourcen zum Einsatz.	Gering
B 2	Aktivisten, Kriminelle	Personen, die gezielt versuchen Schwachstellen auszunützen um Delikte zu begehen (Diebstahl) oder setzen ihr Wissen für politische und ideologische Ziele ein (Aktivist).	Mittel
B 3	Professionelle Kriminelle Organisierte Aktivisten	Kriminelle, die entsprechende Geschäftsmodelle entwickeln, um mittels physischen -Angriffen Delikte zu begehen (Kupferdiebstahl) oder Anlagen zu blockieren. Sie sind in der Regel gut organisiert und verfügen über die notwendigen Ressourcen und Logistikunterstützungen.	Hoch
B 4	Terrorismus	Extreme physische Angriffe gegen bestehende Infrastrukturen unter hoher Gewaltanwendung mit dem Ziel zu zerstören oder ausser Betrieb zu setzen. Dazu zählt beispielsweise die Entführung von Personen oder der ballistische Angriff auf kritische Anlagen.	Sehr hoch
B 5	Staatlicher Akt	Kriegerische Handlungen von Fremd-Staaten. Dazu gehört beispielsweise der Beschuss durch Lenkwaffen oder mittels Artillerie.	Sehr hoch

Tabelle 1 Bedrohungsebene

(8) Es ist dabei nicht möglich, sich als Unternehmen gegen alle Akteure schützen zu können und somit alle Risiken aktiv mitigeren zu können. Gewisse Restrisiken bleiben bestehen und müssen durch das Unternehmen ausgewiesen, akzeptiert oder anderen Stellen zugewiesen werden.

(9) Die Umsetzung von Massnahmen richtet sich dabei nach der entsprechenden Bedrohungskategorie. Je höher die Kategorie, desto mehr Ressourcen (Geld, Know-how) sind nötig, um Angriffe zu verhindern oder die Auswirkungen beherrschen zu können.

(10) Es muss davon ausgegangen werden, dass Bedrohungen der Stufe B 4 und B 5 von einem Unternehmen allein nicht mehr bewältigt werden können. Bedrohungen im Bereich „Terrorismus“ und „Staatlicher Akt (Krieg)“ sind Aufgaben des Staates und können von den Unternehmen nicht ohne staatliche Unterstützung (beispielsweise Einsatz der Armee) bewältigt werden.

(11) Dies hat wiederum zur Folge, dass bei allen Anstrengungen seitens der Unternehmen immer eine Sicherheitslücke bestehen bleiben wird.

(12) Ob eine solche Lücke jedoch per se durch das Unternehmen akzeptiert wird, oder trotzdem Massnahmen getroffen werden (auch wenn die Zuständigkeit und Verantwortung beispielsweise beim Staat liegt) obliegt den Verantwortlichen des jeweiligen Unternehmens, welche einen entsprechenden Unternehmensentscheid vornehmen.

2.2.2 Risikobetrachtung

(1) Tritt eine identifizierte Bedrohung ein und es sind keine ausreichenden Schutzmassnahmen definiert worden, besteht für das schützenswerte Gut ein Risiko.

(2) Grundsätzlich besteht nun die Möglichkeit diese Sicherheitslücke zu schliessen (Umsetzung Schutzmassnahmen) oder aber das Unternehmen akzeptiert das (verbleibende) Risiko.

(3) Wie bereits erwähnt wird es nicht möglich sein alle Risiken zu mitgieren so dass immer ein Rest-Risiko bestehen bleiben wird. Diese Risikobetrachtung ist durch das jeweilige Unternehmen auszuweisen und zu bezeichnen.

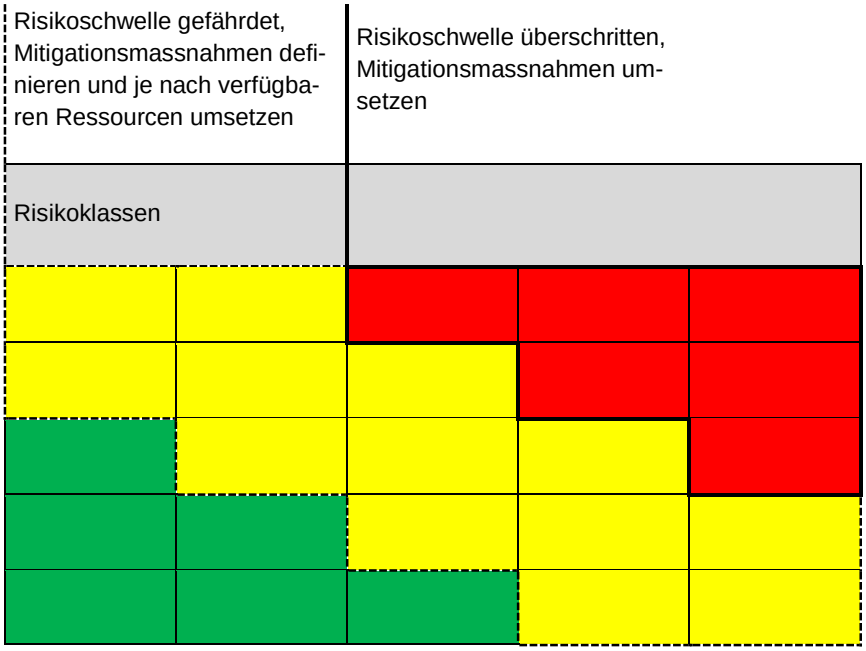
(4) In einem nächsten Schritt wird – basierend auf den in Kapitel 2.3 definierten relevanten Gefährdungen - die dazugehörige Risikobetrachtung durchgeführt.

(5) Dazu werden – bei der aktiven Durchführung der Risikoanalyse - pro Ereignis die Eintretenswahrscheinlichkeit (W) und das Schadensausmass (S) bezeichnet.

(6) Der Fokus liegt dabei auf einer Betrachtung der Schäden für die Bevölkerung und die Wirtschaft in der Schweiz, die sich aufgrund der Störungen im Übertragungsnetz, im vorliegenden Fall bei Unterwerken der Netzebene 1 und tiefer (sofern diese mit Netzebene 1 gemeinsam genutzt werden) ergeben würden.

(7) Die Darstellung der Risiken erfolgt im Rahmen einer Risikomatrix. Beispielhaft wird nachfolgend eine solche Risiko-Matrix dargestellt. Hierbei gibt es aktuell verschiedene Lösungsansätze bezüglich der Grösse einer solchen Risiko-Matrix. Idealerweise wird hierzu eine Risiko-Matrix verwendet, welche im jeweiligen Unternehmen verankert und akzeptiert ist.

(8) Beispiel einer möglichen Risikomatrix „Physische Sicherheit Unterwerke (Netzebene 1 und tiefer) mit exemplarischen Zahlenwerten:



Qualitative Einteilung	Häufigkeit pro Jahr	Häufigkeitsklasse	Risikoklassen				
Sehr wahrscheinlich	> 10	5					
Wahrscheinlich	1 - 10	4					
Möglich	0.1 - 1	3					
Denkbar	0.01 - 0.1	2					
Unwahrscheinlich	< 0.01	1					

Ausmassklasse	A	B	C	D	E
NE1: Finanzieller Schaden in MCHF	< 0.1	0.1 – 1.0	1 - 10	10 - 100	> 100
NE2-NE3: Finanzieller Schaden in MCHF	< 0.01	0.01 – 0.1	0.1 – 1.0	1 - 10	> 10
Schadensausmass	vernachlässigbar	klein	beträchtlich	ernsthaft	katastrophal

Tabelle 2 Beispiel Risikomatrix

(9) Allgemeine Erläuterungen
Die Risikomatrix ist pro Unternehmen selbständig zu befüllen und anschliessend zwischen den Partnern (bei gemeinsam genutzten Unterwerken) zu konsolidieren. In Abhängigkeit von der Netzebene und beispielsweise dem betroffenen Versorgungsgebiet des jeweiligen Unternehmens ergeben sich unterschiedliche Risiken. Dies betrifft insbesondere die Fragestellung des Schadensausmasses. Die Referenz der oben abgebildeten Risikomatrix bezieht sich auf die Netzebene 1. Aspekte der Personenschäden, der Versorgungssicherheit und des Reputation Schadens können als Ausmassklassen ergänzt und in der Risikobetrachtung berücksichtigt werden. Dies obliegt im Ermessen des Betriebsinhabers. Die Bedrohungen und deren Einteilung in den Risikoklassen sind regelmässig zu überprüfen und im Rahmen der Abstimmung mit den Partnern (auf dem Unterwerk) zu vereinbaren.

2.2.2.1 Risikobewertung, Risikoquantifizierung

(1) Der Leitfaden SKI des BABS schlägt vor, zu einem späteren Zeitpunkt des Prozesses, eine Kosten-Nutzen-Betrachtung der in Frage kommenden Massnahmen (Grenzkosten) durchzuführen. Zu diesem Zweck bietet es sich an, die Risiken zu monetarisieren und in einem späteren Schritt mit den Kosten von Massnahmen in ein Verhältnis zu setzen. Die Multiplikation der

Eintretenswahrscheinlichkeit respektive der Plausibilität mit den monetarisierten Schadenswerten ergibt die Risikowerte (in CHF / Jahr).

(2) Artikel 15 StromVG sieht vor, dass Auslagen für den Betrieb eines sicheren Netzes als Netzkosten angerechnet werden können. Es wird jedoch nicht weiter spezifiziert, welches Mass an Sicherheit beim Betrieb des Netzes erwartet wird.

(3) Weiter gilt es sich in diesem Prozessschritt mit der Frage auseinander zu setzen, ob pro Risiko die Eintrittswahrscheinlichkeit, das Schadenausmass oder beides gleichzeitig reduziert werden soll. Zudem ist in diesem Schritt zu klären, ob möglicherweise externe Vorgaben, regulatorische oder gesetzliche Aufgaben in die Beurteilung einfliessen müssen.

2.2.2.2 Risikobewältigung

(1) Dieser Prozessschritt stellt die Vorbereitungshandlung der später erfolgenden Massnahmendefinition dar. Ziel ist es hierbei, die jeweilige Risikobereitschaft des Unternehmens korrekt abzubilden.

(2) Hierbei gilt es Grundsatzfragen wie die Rechtmässigkeit von möglichen Massnahmen (Legalitätsprinzip) und die Bedeutung der Unternehmen als national kritische Infrastrukturen zu würdigen. So ist es durchaus möglich, dass auch Massnahmen, welche auf den ersten Blick per se wirtschaftlich nicht tragbar sind, diese aber den Schutzgedanken einer kritischen Infrastruktur entsprechen, umgesetzt werden können.

(3) Grundsätzlich bestehend verschiedene Möglichkeiten ein bestehendes Risiko zu reduzieren:
- Definition von Massnahmen zur Verminderung der Eintretenswahrscheinlichkeit
- Definition von Massnahmen zur Reduktion des Schadensausmasses
- Transfer eines Risikos (Versicherungslösung)

(4) Weiter besteht die Möglichkeit, ein Risiko zu akzeptieren (Risikoakzeptanz beispielsweise aufgrund des Entscheids des Unternehmens, die Eintretenswahrscheinlichkeit als minimalst anzunehmen).

(5) Es kann in diesem Fall durchaus sein, dass bestimmte Risiken erkannt werden, durch das betroffene Unternehmen bewusst zur Kenntnis genommen und akzeptiert werden. Dies kann unterschiedliche Gründe besitzen. Einerseits können wirtschaftliche Überlegungen im Vordergrund stehen, andererseits aber auch Fragen der Zuständigkeit (Bedrohungspyramide).

(6) Die Risikobereitschaft, stellt jenes Mass an Risiko dar, welches das jeweilige Unternehmen bereit ist zu tragen und welches durch das Unternehmen - trotz Kenntnis des Risikos – nicht mitigiert und von diesem akzeptiert wird.

(7) Für die Bestimmung der Risikobereitschaft sind neben Schutzzielen auch andere Ziele (beispielsweise Unternehmensziele) angemessen zu berücksichtigen.

(8) Grundsätzlich kann festgehalten werden, dass der gesamte Risikoprozess kontinuierlich und in regelmässigen Zeitabständen zu überprüfen ist.

2.3 Schritt 2: Definition der Schutzziele

(1) Mit der Definition von Schutzzielen (welcher Schutzgrad soll gegen welche potentiellen Angreifer Gruppen resp. Angriffsszenarien erreicht werden) wird der Zielerfüllungsgrad der zu treffenden Massnahmen vorgegeben. Dies erlaubt es eine Grenze zwischen akzeptierbaren und nichtakzeptierbaren Risiken festzulegen.

(2) Bei der Formulierung der Schutzziele stellt die Verfügbarkeit der kritischen Infrastrukturelemente einen sinnvollen Indikator dar. Die Ziele sind so zu wählen, dass eine minimale Ausfallzeit der kritischen Elemente resultiert.

2.4 Schritt 3: Kritikalität der Anlagen

(1) Wie bereits in Schritt 1 angesprochen, kommt der Bedeutung eines Unterwerkes resp. dessen kritischer Anlagenteil in Bezug auf das betrachtete Gesamtsystem einer entscheidenden Rolle zu. Unter diesem Blickwinkel ist vor Definition von lokalen Massnahmen (Einzelbetrachtung) eine Kritikalitätsbetrachtung durchzuführen (Gesamtbetrachtung).

(2) Der Begriff Kritikalität bezieht sich in dieser Betrachtungsweise auf die Bedeutung des Unterwerkes bezüglich des Gesamtnetzes resp. der Bedeutung hinsichtlich der Gewährleistung der Versorgungssicherheit (siehe auch Kapitel 3.4).

2.5 Schritt 4: Massnahmen: Grundschutz, erweiterter Schutz

(1) In der Erarbeitung des Schutzkonzepts sind Massnahmen (wie beispielsweise elektronische Zutrittssysteme, Härtung von Gebäuden etc.) zu evaluieren, die grundsätzlich in Frage kommen, um die festgestellten Risiken zu reduzieren bzw. um die Schutzziele einzuhalten. Generell sind Massnahmen zu treffen, die dem aktuellen Stand der Technik entsprechen, dazu dienen die Schutzziele zu erreichen und kostenwirksam optimiert sind.

(2) Je nach Ausgangslage, Bedrohungsart, Risiko oder Schutzziel können die Massnahmen im Bereich der Unterwerke in drei Kategorien eingeteilt werden:

2.5.1 Grundschutz

(1) Der Grundschutz ergibt sich aus den vielfältigen Vorgaben von Gesetzen und Verordnungen (beispielsweise Starkstromverordnung) sowie Standards (verpflichtende und freiwillige) und anerkannten „Best Practices“. Alle Massnahmen, die gemeinsam den Grundschutz bilden, werden auf Basis dieser Vorgaben festgelegt und aus etablierten Standards oder aus allgemein anerkannten „Best Practice“-Erfahrungen abgeleitet. Risikobetrachtungen werden bei der Ermittlung und Definition des Grundschutzes nicht angestellt.

(2) „Best Practices“ haben einen hohen Stellenwert, da sie auf bewährten Verfahren basieren und aufzeigen, wie andere Firmen der gleichen Problematik begegnen. Verpflichtende Gesetze sind in jedem Fall in den Grundschutz zu integrieren. Grundsätzlich sollen alle Empfehlungen des Grundschutzes bei allen Unterwerken umgesetzt werden.

2.5.2 Erweiterter Schutz (mittlerer und hoher Schutz)

(1) Neben dem Grundschutz, der das minimal notwendige Schutzniveau definiert, stellt die Risikobereitschaft das als sinnvoll erachtete Schutzniveau aus Sicht der Verantwortlichen dar. So wird

beispielsweise mittels einer Kritikalitätsbetrachtung die Bedeutung eines Unterwerkes für das Gesamtsystem berücksichtig. Ist das Unterwerk von besonderer Bedeutung (beispielsweise aufgrund seiner Bedeutung für das Gesamtnetz), das heisst besonders schützenswert, so wird ein Schutz der Kategorie „mittel“ oder „hoch“ empfohlen.

(2) Grundsätzlich lassen sich alle Massnahmen in zwei Kategorien einteilen:
- Vorbeugende Massnahmen, die das Schadensausmass oder die Eintretenswahrscheinlichkeit eines Risikos reduzieren. Dazu gehören ebenfalls kurative Massnahmen wie beispielsweise vorbereiten der Business Continuity-Massnahmen (BCM) und Prozesse.
- Vorbereitende Massnahmen, welche die Ausfallzeit einer kritischen Infrastruktur minimieren oder die Ereignisbewältigung unterstützt

(3) Nach Möglichkeit sollte darauf geachtet werden, nicht nur Massnahmen auszuwählen, die die Eintrittswahrscheinlichkeit verringern, sondern auch das Schadensausmass reduzieren. Hierbei gilt es zu beachten, dass die Reduktion des Schadensausmasses im Regelfall nur durch entfernen bzw. verringern des Gefahrenpotentials oder durch (passive) Abschirmung und beispielsweise eine ausreichende Lagerhaltung von kritischem Ersatzmaterial erreicht werden kann.

(4) Generell sind Massnahmen zu treffen, die dem aktuellen Stand der Technik entsprechen, dazu dienen die Schutzziele zu erreichen und kostenwirksam sind.

(5) Die Massnahmen sind in der Folge einer risikobasierten Kosten-Nutzen-Analyse zu unterziehen. Dies geschieht durch eine Gegenüberstellung der potenziellen Investitionen für die Massnahmen und der direkten sowie indirekten Kosten einer Beeinträchtigung der kritischen Infrastruktur.

(6) Grundsätzlich stellt sich in diesem Zusammenhang auch die Frage nach dem akzeptablen Restrisiko. Ein solches Risiko kann sich einerseits aus bewusst akzeptierten und anderseits aus falsch beurteilten oder nicht anerkannten Risiken zusammensetzen.

(7) Im Rahmen des Schutzes kritischer Infrastrukturen muss eine risikobasierte Kosten-Nutzen-Analyse folgende Kriterien erfüllen:
- Die Umsetzung der Massnahme(n) muss u.a. zum Erreichen des zuvor festgelegten Schutzziels beitragen.
- Der Nutzen der neuen bzw. angepassten Massnahmen muss die festgestellten Risiken für die kritische Infrastruktur senken bzw. die Ausfallszeit minimieren.
- Die Kosten der Massnahmen müssen betriebswirtschaftlich angemessen sein.

(8) Mit dieser Kosten-Nutzen Betrachtung wird sichergestellt, dass die effizientesten Massnahmen (Zielerreichung) vorgeschlagen werden.

2.6 Schritt 5: Überprüfung

(1) Damit die Qualität der Implementierung und die Wirksamkeit von getroffenen Massnahmen überprüft sowie Abweichungen korrigiert werden können, werden diese kontinuierlich überwacht und mit dem Grundschutz sowie der Risikobereitschaft abgeglichen. Das gewählte Schutzkonzept selbst ist in regelmässigen Abständen auf seine Wirksamkeit und Effizienz hin zu überprüfen.

(2) Zusätzliche Überprüfungen sind notwendig, nach
- der Umsetzung von Massnahmen,
- nach einem Krisenereignis,
- nach einer Erweiterung/Veränderung in der kritischen Infrastruktur sowie
- bei einer Änderung der Gefährdungslage.

(3) Diese Überprüfungen sind zu planen, durchzuführen und die Ergebnisse zu dokumentieren (siehe auch Kapitel 3.6).

3. Anwendung: Entwicklung Schutzmassnahmen Unterwerk

3.1 Vorgehen Anwendungsfall Unterwerk

(1) Das Vorgehen richtet sich grundsätzlich nach der in Kapitel 1 dargestellten Methodik. Diese basiert auf dem Vorgehensprozess des SKI-Leitfadens, welcher – angewandt auf die Thematik „Unterwerk“ - sich folgendermassen zusammenfassen lässt:

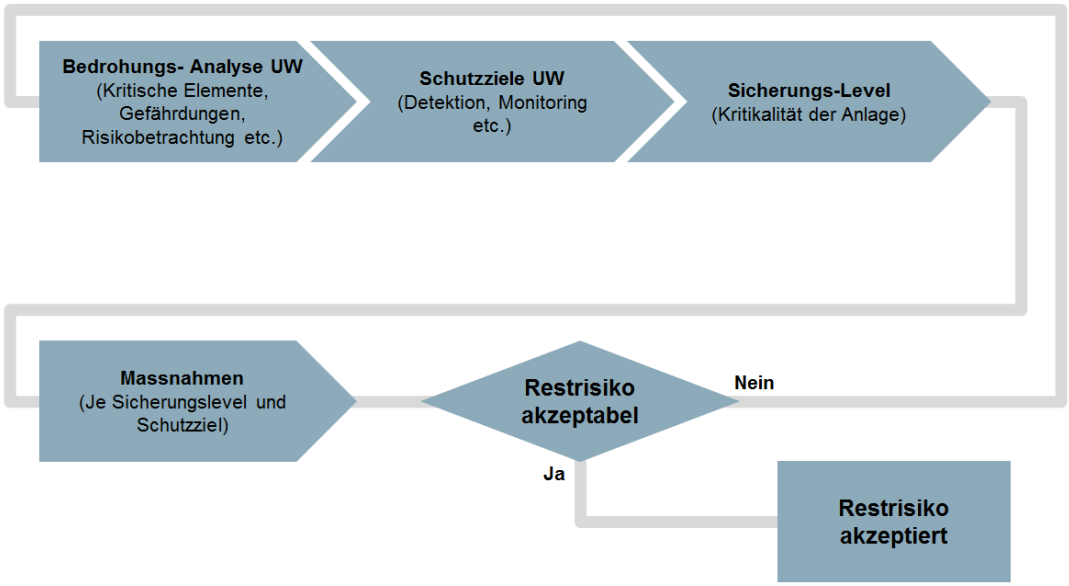


Abbildung 3 Prozessablauf zur Entwicklung geeigneter Schutzmassnahmen

3.2 Schritt 1: Bedrohungsanalyse

3.2.1 Identifikation kritischer Elemente eines Unterwerkes

(1) Zur Beurteilung der relevanten Gefährdungen werden in einem ersten Schritt diejenigen Elemente eines Unterwerkes identifiziert, welche als kritisch zu bezeichnen sind.

(2) Hierbei wird der Kritikalitätsbegriff folgendermassen definiert:

- Anlagenteile, welche bei einem Ausfall zu einer erheblichen Störung der Versorgungssicherheit und damit zu merkbaren Beeinträchtigungen der Bevölkerung und der Wirtschaft führen können
- Anlagenteile, welche nur sehr schwer oder mit einem sehr hohen zeitlichen Aufwand ersetzt werden können und deshalb das Risiko eines Versorgungsausfalles in sich tragen

Liste der kritischen Elemente auf einem UW (Liste nicht abschliessend)

Hoch kritische Elemente	Mittel kritische Elemente	Unkritische Elemente
Höchstspannungs-transformatoren*	Sammelschiene	Büro- und Aufenthaltsgebäude
Kontrollschaltkästen für Leistungsschalter	Isolatoren	Strassen und Wege
Kontrollrechner der Stations- und Feldleitsysteme	Leistungsschalter	Lager allgemeines Material
Messeinrichtungen, Schaltschränke	Kabeleinführungen	Parkplätze
Schutzgeräte	Überspannungsableiter	Lager hochwertiges Material
Schränke des Kommunikationsnetzwerks (WAN)	Messwandler	Werkstattbereiche
Kabeleinführungen Netzwerk Kommunikation (WAN)	Trenner	
Eigenbedarf		

Tabelle 3 Liste kritischer Elemente eines Unterwerkes

* inkl. ausgewählte Trafos anderer Netzebenen

(3) Die Kritikalität der Elemente ist im Rahmen der Erarbeitung des Schutz-Massnahmenkatalogs zu berücksichtigen. Im Fokus steht hierbei der Schutz der hochkritischen Elemente.

3.2.2 Relevante Gefährdungen und Risiken

(1) In einem nächsten Schritt werden – basierend auf der in Kapitel 2.2.1 dargestellten Bedrohungspyramide - die relevanten Gefährdungen und daraus abgeleitet Bedrohungen bestimmt.

(2) Als relevante Gefährdungen werden dabei Szenarien betrachtet, welche zu einer Störung oder einem Ausfall der kritischen Elemente auf einem Unterwerk führen können.

(3) Die Liste der nachfolgenden möglichen physischen Bedrohungen ist zu berücksichtigen:

(4) Bedrohung gegen Infrastrukturen:
- Einschleichen, unbefugter Zutritt
- Physische, zerstörerische Angriffe durch Einzelpersonen oder Gruppen
- Störung der Netzkommunikationssysteme und der Kommunikationsinfrastruktur
- Fahrzeugangriff oder Unfall-Impact
- Diebstahl von vertraulichen Informationen, Unternehmensvermögen und Sachmitteln (beispielsweise Anlagenteile, Metalle und Ausrüstungen)
- Kriminelle, elektronische Ablenkungs- und Abhörtechniken
- Vandalismus
- Drohnenangriffe auf kritische Infrastrukturen
- Brandanschlag auf kritische Infrastruktur (Bsp. Trafo)

(5) Bedrohungen gegen Personen:
- Kriminelles Social Engineering
- Anstellung von nicht überprüften Mitarbeitenden
- Physische und psychische Angriff gegenüber Mitarbeitenden
- Entführung

(6) In einem nächsten Schritt werden diese möglichen Gefährdungen in thematische Gruppen zusammengefasst und spezifische Szenarien definiert, die mögliche Ereignisabläufe beschreiben.

(7) Auf diese Weise werden insgesamt 6 übergeordnete Szenarien (siehe nachfolgende Tabellen) definiert. Bei der Festlegung und Beschreibung der Szenarien liegt der Fokus auf Ereignissen, die zu einer gravierenden Beeinträchtigung der Stromversorgung führen können. Ereignisse und Intensitäten, die keine solchen Konsequenzen nach sich ziehen würden, werden nicht betrachtet.

(8) Gleichzeitig wird das aus dem Szenario entstehende und zu berücksichtigende Risiko und dessen möglichen Auswirkungen beschrieben:

1. Physischer Angriff zur Schwächung und Zerstörung von Infrastruktur			
Bedrohung	**Bedrohungs-ebene**	**Beschreibung**	**Risiko**
Ungeplanter physischer Angriff	B1	Ungeplanter oder amateurhafter Angriff auf ein Unterwerk oder Teile eines Unterwerkes mit kleiner krimineller Energie. Als Hilfsmittel wird beispielsweise gängiges Einbruchswerkzeug eingesetzt.	Kleinere Beschädigungen von Anlagenteilen, Türen oder Fenster aufgebrochen, Zaun aufgeschnitten. Keine Störung des Netzbetriebs zu erwarten.
Geplanter physischer Angriff	B2	Organisierter und geplanter Angriff auf ein Unterwerk oder Teile eines Unterwerkes mit mittlerer oder hoher krimineller Energie. Spezialisierte Werkzeuge, Vorgehensweisen und spezifisches Wissen gelangen zur Anwendung.	Zielgerichtete Beschädigungen von hoch kritischen Elementen und in der Folge eine grosse Wahrscheinlichkeit einer Beeinträchtigung der Versorgungssicherheit.
Unfall oder Angriff mit Fahrzeug	B1, B2	Beschädigung von Assets durch einen Verkehrsunfall oder einen organisierten und geplanten Angriff. Als Angriffsmittel können schwere LKW oder PKW zur Anwendung gelangen.	Eher zufällige Beschädigungen, welche jedoch weitgehende Auswirkungen haben können. Risiko von auslaufendem Öl und damit Umweltschäden, Brandgefahr. Beeinträchtigung der Versorgungssicherheit beim Ausfall kritischer Anlagenteile.
Unfall oder Angriff mit ballistischen Waffen	B2, B3, B4, B5	Beschädigung von Assets oder Personen durch einen Unfall oder durch einen unorganisierten oder organisierten und geplanten Angriff mittels Waffen	Es muss von einer zielgerichteten Beschädigung von möglicherweise hoch kritischen Anlagenteilen durch ballistischen Beschuss ausgegangen werden. Bei Beschuss durch Hochenergie Waffen (Stufe Sturmgewehr und höher) muss mit erheblichen Schäden gerechnet werden. Gefahr für Ausfall von Anlagenteilen resp. des Unterwerkes hoch.
Angriff mit EMP-Geräten	B4, B5	Beschädigung von Assets durch den Einsatz von EMP-Geräten	Ein zielgerichteter Angriff mit EMP-Waffen führt zu einer Beschädigung des elektronischen Systems des Unterwerkes. Dies führt zu Ausfällen der Sekundärtechnik und der Kommunikationsinfrastruktur. Eine Steuerung des Unterwerkes ist nur schwer möglich. Risiko des Betriebsausfalles hoch.
Angriff mit Drohne	B2, B3, B4, B5	Erkundung oder Beschädigung von Assets durch den Einsatz von Drohnen oder anderen Fluggeräten	Im Extremfall kann es durch den Einsatz von Drohnen (Abwurf von Explosivstoffen) zu erheblichen Beschädigungen kritischer Anlagenteilen kommen. Dies wiederum kann zum Ausfall des UW führen.

2. Diebstahl von betriebsrelevanten Mitteln und Informationen			
Bedrohung	**Bedrohungs-ebene**	**Beschreibung**	**Risiko**
Diebstahl von betriebs-relevanten Informatio-nen	B1 bis B5	Diebstahl von betriebsrelevanten In-formationen, physischer oder elektro-nischer Art	Ungewollter, krimineller Informati-onstransfer kann zum Erkennen von Sicherheitslücken oder der be-stehenden Sicherheitsarchitektur führen. Dies wiederum ermöglicht potentiellen Angreifern einen ziel-gerichteten und effektiven Angriff. Erhöhtes Risiko für die Versor-gungssicherheit.
Diebstahl von nicht be-triebsrele-vanten Sachwerten	B1, B2	Diebstahl von Sachwerten wie bspw. Mobiliar, Werkzeuge, Büromaterial, nicht strategische Ersatzteile, Umbau-materialien, etc.	Schädigung des Unternehmens durch Vermögensverluste. Im Re-gelfall keine Auswirkung auf die Versorgungssicherheit.
Diebstahl von betriebs-relevanten Sachwerten	B1, B2, B3	Diebstahl von Sachwerten wie bspw. Spezialwerkzeuge, Betriebsmittel der in Betrieb stehenden Anlagen, strate-gische Ersatzteile, Erdgarnituren, etc.	Dies kann zu Einschränkung der Betriebsbereitschaft bis hin zu ei-nem Teil-Ausfall der Anlage führen.

3. Unbefugter Zutritt			
Bedrohung	**Bedrohungs-ebene**	**Beschreibung**	**Risiko**
Unbefugter Zutritt mittels Einbruchs	B1 bis B5	Eine Einzelperson oder Gruppe verschaffen sich mit Hilfsmitteln Zu-tritt in das Unterwerk, bspw. mittels Aufschneidens oder Übersteigen des Zaunes, aufbrechen einer Türe oder eines Fensters	Kleinere Beschädigungen von Anla-genteilen, Türen oder Fenster auf-gebrochen, Zaun aufgeschnitten. Keine Störung des Netzbetriebs zu erwarten. Risiko eines Personen-schadens durch unsachgemässes Betreten des Geländes.
Unbefugter Zutritt durch Einschlei-chen	B1, B2	Eine Einzelperson oder Gruppen verschaffen sich mittels „Anhängen an eine Gruppe“ (back tailing) oder anderen Einschleichprozessen Zu-tritt in das Unterwerk	Im Extremfall kleinere Beschädigun-gen von Anlagenteilen. Keine Stö-rung des Netzbetriebs zu erwarten. Risiko eines Personenschadens durch unsachgemässes Betreten des Geländes.
Unbefugter Zutritt durch Manipulatio-nen	B2, B3	Eine Einzelperson oder Gruppen verschaffen sich mittels Manipula-tion des Zutrittssystems oder durch einen gestohlenen Schlüssel Zutritt in das Unterwerk	Im Extremfall kleinere Beschädigun-gen von Anlagenteilen. Keine Stö-rung des Netzbetriebs zu erwarten. Risiko eines Personenschadens durch unsachgemässes Betreten des Geländes.

4. Innentäter			
Bedrohung	**Bedrohungs-ebene**	**Beschreibung**	**Risiko**
Geplante Insider Handlung	B2, B3, B4	Insider (internes oder externes Personal), welche über genügend Know-How verfügen, führen Angriffe und Manipulationen aus	Im Extremfall gezielte Beschädigungen und Ausschaltungen von kritischen Anlagenteilen, was zu einem Gesamtausfall des Systems führen kann. Hohes Risiko für die Anlagensicherheit.
Emotionale Fehlreaktionen	B2	Eine Einzelperson oder Gruppe führt durch eine emotionale Reaktion eine kriminelle Handlung aus	Im Extremfall Verletzung von Personen und/oder gezielte Beschädigungen und Ausschaltungen von kritischen Anlagenteilen, was zu einem Gesamtausfall des Systems führen kann. Hohes Risiko für die Personen- und Anlagensicherheit.

5. Physische und psychische Bedrohung von Personen			
Bedrohung	**Bedrohungs-ebene**	**Beschreibung**	**Risiko**
Kriminelles Social Engineering	B3, B4	Beispielsweise durch kriminelle Informationsbeschaffung und Aufklärungsarbeiten über kritische oder hochkritische Funktionen oder kritischen Applikationen und Anlagenteilen.	Ungewollter, krimineller Informationsgewinn und in der Folge Informationstransfer kann zum Erkennen von Sicherheitslücken oder der bestehenden Sicherheitsarchitektur führen. Dies wiederum ermöglicht potentiellen Angreifern einen zielgerichteten und effektiven Angriff. Erhöhtes Risiko für die Versorgungssicherheit.
Angriff gegen Personen	B3, B4	Eine Einzelperson oder Gruppe bedrohen gezielt Personen, bis hin zum physischen oder psychischen Übergriff mit dem Ziel relevante Informationen oder Zutritte zu erlangen	Im Extremfall Bedrohung und Verletzung von Personen und in der Folge eine gezielte Beschädigung und Ausschaltungen von kritischen Anlagenteilen, was zu einem Gesamtausfall des Systems führen kann. Hohes Risiko für die Personen- und Anlagensicherheit.
Entführung von Personen	B3, B4, B5	Eine Einzelperson oder Gruppe entführen Personen um Handlungen und/oder Informationen, welche sich negativ auf die Versorgungssicherheit auswirken, zu erpressen	Im Extremfall Bedrohung, Gefährdung und Verletzung von Personen und in der Folge eine gezielte Beschädigung und Ausschaltungen von kritischen Anlagenteilen, was zu einem Gesamtausfall des Systems führen kann. Hohes Risiko für die Personen- und Anlagensicherheit.

6. Vandalismus			
Bedrohung	**Bedrohungs-ebene**	**Beschreibung**	**Risiko**
Vandalismus in und um das Unter-werk	B1, B2	Finanzielle Schädigung durch Ver-unstaltung und/oder Beschädigung von Vermögenswerten durch Schmierereien oder kleinere physi-sche Beschädigungen	Setzt in der Regel das unbefugte Betreten des Areals voraus. Dies wiederum kann das Risiko von Per-sonenschäden (unsachgemässe Handlungen) mit sich bringen. Van-dalismus für sich alleine betrachtet im Normalfall kein Risiko für die Versorgungssicherheit.

3.3 Schritt 2: Schutzziele

(1) Mit der Definition der Schutzziele werden der jeweilige – unternehmensabhängige – Umfang und teil-weise auch die Höhe des zu erreichenden Schutzgrades festgelegt. Diese Definition bildet damit auch zu einem gewissen Grad die Maturität eines Unternehmens im Umgang mit Risiken aus physi-schen Bedrohungen des Unternehmens respektive dessen kritischen Anlagenteilen ab.

(2) Nachfolgend werden die 3 relevanten Schutzziele für den Schutz eines Unterwerkes dargestellt.

3.3.1 Schutzziel 1: Kennen, benennen und überwachen der kritischen Bereiche

(1) Ziel ist es, die systemkritischen Bereiche/Elemente zu kennen und zu benennen. Die einzelnen Ele-mente sollen hinsichtlich ihrer Kritikalität (Funktionieren des Gesamtsystems) eingeschätzt werden. Diese Bereiche/Elemente gilt es einerseits mit geeigneten Massnahmen zu schützen und anderer-seits auch zu überwachen, damit unautorisierte Zugriffe, Zutritte, verdächtige Aktivitäten oder Ein-griffe erkannt werden können.

3.3.2 Schutzziel 2: Schutz und Abschreckung/Verzögerung von Tätern

(1) Ziel ist es, sich vor Angriffen schützen zu können bzw. Angriffe möglichst frühzeitig zu verhindern. Ein weiterer Aspekt liegt in der Abschreckung von potentiellen Angreifern. Dies geschieht einerseits durch die Erkennbarkeit der getroffenen Massnahmen (Kameras) und/oder durch das Anbringen ent-sprechender Hinweis- und Warnschilder.

(2) Potentielle Angreifer sollen durch die Sicherungsmassnahmen signifikant in ihren Aktionen verzögert werden, so dass diese vor dem Eindringen auf das Gelände oder dem Anrichten von grösseren Schäden durch Interventionskräfte festgehalten oder durch akustische Alarmsignale gestört, verunsi-chert und vertrieben werden.

(3) In diesem Schutzziel wird auch die jeweilige Resilienz des Betriebs/Unterwerkes abgedeckt.

3.3.3 Schutzziel 3: Detektion und Nachvollziehbarkeit von Zutritten

(1) Ziel ist es, jeden Zutritt zu kritischer Infrastruktur (in diesem Fall dem Unterwerk und weiteren kriti-schen Anlageteilen) zu erfassen und zu kennen. Gleichzeitig soll man in der Lage sein zu erkennen, ob dieser Zutritt unautorisiert oder gerechtfertigt erfolgt. Mittels eines Auditprogramms ist die Nach-vollziehbarkeit der Zutritte sicher zu stellen.

(2) Des Weiteren sollen die nicht autorisierten Zutritte durch ein geeignetes Sicherheitssystem an eine zentrale Stelle weitergeleitet werden, damit die notwendigen, fallbedingten Massnahmen eingeleitet werden können.

(3) Nebst diesen „echten“ Schutzzielen sind drei weitere „betriebliche“ Ziele zu berücksichtigen:

3.3.3.1 Regelungen bezüglich Ausnahmesituationen (Baustellen, Unterhalt, etc.)

(1) Es muss sichergestellt werden, dass bei Ausnahmesituationen auf dem betroffenen Unterwerk oder Anlagenteil die notwendigen Anpassungen in der Sicherheitskonzeption geplant, erstellt und beim betroffenen Personal geschult werden. Die Detektion und Nachvollziehbarkeit der Zutritte darf dabei nicht eingeschränkt werden.

3.3.3.2 Sicherheitsprozesse sind bekannt, getestet und geschult

(1) Einführen und unterhalten eines gesamthaften Sicherheitssystems, welches für alle betroffenen Personen bekannt gemacht wird und inkl. allen notwendigen Prozessen geschult wird. Dabei ist sicherzustellen, dass die Sicherheitsorganisation die Prozesse nach Bedarf/gesetzlicher Regelung schult und die erforderlichen Nachweise dokumentiert und ablegt. Das gesamte Sicherheitssystem ist regelmässig auf dessen Funktionalität und Angemessenheit hin zu überprüfen. Dies im Rahmen eines standardisierten Ansatzes wie beispielsweise „Plan – Do – Check – Act“.

(2) Allfällige lage- und bedrohungsbedingten Anpassungen sind entsprechend vorzunehmen, zu dokumentieren und zu schulen.

(3) Unter Berücksichtigung des Umstandes, dass dem Faktor Mensch eine bedeutende Rolle zukommt, sind, basierend auf der bestehenden Sicherheitskonzeption, regelmässige Awareness-Schulungen durchzuführen. Die Etablierung einer gelebten Sicherheitskultur steht dabei im Vordergrund. Diese Schulungsprozesse resp. deren Erfolg sind regelmässig zu auditieren, dies im Sinne eines kontinuierlichen Verbesserungsprozesses. Die Ergebnisse sind zu dokumentieren und dienen – nebst anderen Informationen – als Grundlage für nachfolgende Analyseschritte.

3.3.3.3 Erfassung von Vorfällen und Ableiten von Massnahmen

(1) Das Erfassen von Vorfällen und den daraus abgeleiteten Massnahmen muss im gesamthaften Sicherheitssystem implementiert werden. Diese Datenbasis (beispielsweise eine Ereignisliste mit nachgelagerten Massnahmen) dient als Grundsteine einer laufenden und aktuellen Lagebetrachtung und fliesst in eine permanente Bedrohungsanalyse mit ein. Dabei ist sicher zu stellen, dass jeder Vorfall entsprechend der vorgängig definierten Kriterien erfasst und analysiert wird. Die daraus resultierenden Massnahmen sind nach deren Dringlichkeit (Risikoprozess) umzusetzen.

(2) Generell gilt, dass die Schutzziele die jeweilige Risikosituation und Kritikalität der zu schützenden Anlagen berücksichtigen. Wie die Massnahmen sind auch die Schutzziele regelmässig zu überprüfen und zu aktualisieren.

(3) Nachgelagert sind auch Aspekte der Reaktionsfähigkeit des Unternehmens auf festgestellte Überwachungsalarme darzustellen und periodisch zu überprüfen.

(4) Die Schutzziele dienen auch dazu in einer späteren Phase die Massnahmen auf deren Zielerfüllungsgrad hin zu beurteilen.

3.4 Schritt 3: Kritikalität der Anlagen und Sicherungslevels

(1) Sinnvollerweise berücksichtigt ein Schutzkonzept für kritische Anlagen und Elemente auch die Kritikalität der zu schützenden Anlagen und Anlagenteile hinsichtlich der Aufgabenerfüllung des Gesamtsystems.

(2) Die gleiche Betrachtungsweise gilt für die Gesamtzahl der zu schützenden Unterwerke und Schaltanlagen.

(3) Unter Berücksichtigung einer wirtschaftlichen Aufgabenerfüllung der Energieunternehmungen unter gleichzeitiger Berücksichtigung der Bedürfnisse der Versorgungssicherheit, kann davon ausgegangen werden, dass im Bereich der physischen Schutzmassnahmen nicht alle Unterwerke die gleiche Kritikalität einnehmen. Oder anders gesagt, unter Berücksichtigung der Netzwirkung der einzelnen Unterwerke gibt es unter-schiedliche Schutzbedürfnisse und Schutzgrade. So kann beispielsweise der Ausfall eines hochkritischen Unterwerkes die Stabilität des Gesamtnetzes gefährden, während der Ausfall eines unkritischen Unterwerkes keinerlei Gefahr für die (gesamte) Versorgungssicherheit darstellt.

(4) Mögliche Kriterien für eine Kritikalitätsberechnung sind:
- Bedeutung des Unterwerks aus Sicht Netzgesellschaft (Zahl der Spannungsebenen, Zahl der internationalen Linien, Zahl der nationalen Linien, Zahl der Transformatoren und deren Leistung, Anzahl Verbraucher etc.)
- Bedeutung des Unterwerks bezüglich dem Verteilnetz (Zahl der Transformatoren Richtung Verteilnetz und deren Leistung, Anzahl Verbraucher etc.))
- Sicht eines Kraftwerkes (Zahl der Generatoren, Höhe der Leistung, Zahl Pumpen, Bedeutung in Sachen Schwarzstartfähigkeit etc.)

(5) So sollen Unterwerke der Netzebene 1 und tiefer (bei gemeinsam mit Netzebene 1 genutzten Unterwerken) in Abhängigkeit von ihrer Bedeutung (Kritikalität) gehärtet werden. Dabei werden grundsätzlich drei Sicherungs-Stufen unterschieden (hoher Schutz, mittlerer Schutz und normaler Schutz). Die Härtungs-massnahmen orientieren sich an den, den Bedrohungsszenarien zu Grunde gelegten Angreifergruppierungen respektive den daraus abgeleiteten Bedrohungen und Risiken (siehe Kapitel „Relevante Gefährdungen“).

3.4.1 Sicherungslevel „Normaler Schutz“ (Grundschutz)

(1) Der Grundschutz stellt die Basislösung für alle Unterwerke der Netzebene 1 und tiefer (bei gemeinsam mit Netzebene 1 genutzten Unterwerken) dar.

(2) Die Auswirkungen eines Ausfalls des Unterwerkes auf die Gesamtverfügbarkeit des Netzes sind niedrig. Das Unterwerk soll daher nur gegen das Eindringen von niedrig motivierten Angreifergruppen, wie zum Beispiel Vandalen oder Gelegenheitsdieben, gesichert werden.

(3) Einschränkungen: Es erfolgt keine elektronische Überwachung des gesamten Geländes.

3.4.2 Sicherungslevel „Mittlerer Schutz“

(1) Die Auswirkungen eines Ausfalls des Unterwerkes auf die Gesamtverfügbarkeit des Netzes sind mittelschwer. Das Unterwerk soll daher zusätzlich gegen das Eindringen von mittel bis hoch motivierte Angreifer Gruppen, wie zum Beispiel organisierten Einbrechern (Kupferdiebe etc.), gesichert werden.

(2) Massnahmen: Zusätzlich zu der Basislösung wird in der „Mittel“-Lösung das gesamte Gelände überwacht und es ist eine Beobachtung des gesamten Unterwerkes möglich.

3.4.3 Sicherungslevel „Hoher Schutz“

(1) Die Auswirkungen eines Ausfalls des Unterwerkes auf die Gesamtverfügbarkeit des Netzes sind schwer bis katastrophal. Das Unterwerk soll daher zusätzlich gegen das Eindringen von hoch bis sehr hoch motivierte Angreifergruppen, wie zum Beispiel organisierte Kriminelle oder Aktivisten, gesichert werden.

(2) Massnahmen: Zusätzlich zu der „Mittel“-Lösung erfolgt eine doppelte Detektion in den sensitiven Aussenbereichen und die Überwachung der sensitiven Innenräume. Die Innenräume werden in Sicherheitszonen aufgeteilt. Die Zufahrtwege können überwacht werden.

(3) Generell sind die Anlagen dahinhegend zu konzipieren, dass sie eine möglichst hohe und angemessene Resilienz gegen jegliche Bedrohungsform aufweisen. Weiter sind auch betriebliche Massnahmen wie die Reaktionsfähigkeit auf eingehende Alarme angemessen vorzuhalten.

3.5 Schritt 4: Massnahmen

3.5.1 Schutz-Zonen

(1) Die nachfolgend dargestellte Schutz-Massnahmen orientieren sich an den in Kapitel 3.4 dargestellten Grundsätzen hinsichtlich der Kritikalität der Unterwerke und der sich darauf befindlichen kritischen Anlagenteile.

(2) Basierend auf einer sicherheitsmässigen Zonenbetrachtung können auf einem Unterwerk unterschiedliche Schutz-Zonen definiert werden. Unter Berücksichtigung potentieller Schutz-Massnahmen und der Analyse möglicher Bedrohungen und des Ablaufes eines theoretischen physischen Angriffes (von aussen gegen innen) werden sinnvollerweise folgende Schutzzonen unterschieden:

- Perimeter
- Areal
- Gebäude
- Raum mit Elementen
- Transformator

Abbildung 4 Schema Schutz-Zonen auf einem Unterwerk

3.5.2 Schutz-Massnahmen pro Schutz-Zone

(1) Pro Zone und Sicherungselement/Massnahme werden die unterschiedlichen – von der Kritikalität der Anlage beeinflussten – Sicherungsmassnahmen aufgeführt.

3.5.2.1 Zaun

(1) Der Zaun stellt die juristische Grenze des Areals dar und bietet zugleich physischen Schutz vor Gefahren auf der Anlage wie auch Schutz gegen Angreifer. Die Errichtung eines Zaunes dient auch der Abgrenzung gegenüber von Drittpersonen (Safety Aspekt). Diesbezüglich bestehen gesetzliche Vorgaben durch das Eidgenössische Starkstrominspektorat (ESTI).

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	Ausführung eines Zaunes gemäss Starkstromverordnung (Zaun Höhe und vorgegebene Maschenweite).	2
Mittlerer Schutz	Zum gesetzlich vorgegeben Zaun wird zusätzlich ein Übersteigschutz (Ausleger) installiert. Dieser kann zusätzlich mit einem Sicherheitsdraht (Stachel- oder Natodraht) gesichert werden.	2
Hoher Schutz	Zu den bereits vorgeschlagenen Massnahmen des erweiterten Schutzes kommt als Zusatzmassnahme die Ausführung eines Untergrabschutzes hinzu. Zudem können Massnahmen zur Verstärkung des Zaunes umgesetzt werden (beispielswiese Einsatz von verstärkten Zaunelementen etc.).	2

Tabelle 4 Schutzmassnahmen Zaun

Ausführungsbeispiele

Zaun mit Übersteigschutz

Zaun mit Untergrabschutz

Abbildung 5 Beispielbilder für Zaunlösungen

3.5.2.2 Anprallschutz

(1) Kritische Anlagenteile und Elemente – wie Transformatoren, Einspeisungen etc. - werden gegen die Einwirkung grober mechanischer Beeinträchtigung geschützt. Um den Aufbau von hoher kinetischer Energie zu unterbinden können beispielsweise an strategischen Punkten Blockaden oder Verengungen angeordnet werden. Diese können sich auch ausserhalb des Perimeters (Areal) befinden und so beispielsweise Zufahrtsstrassen und parallel verlaufende Strassen umfassen.

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	keine Massnahmen	
Mittlerer Schutz	Prüfung „weicher“ Massnahmen (Bsp. Leitplanken, Pfosten, etc.)	2
Hoher Schutz	Prüfung „harter“ Massnahmen (Bsp. Betonelemente, Poller, etc.)	2

Tabelle 5 Schutzmassnahmen Anprallschutz

Ausführungsbeispiel

Abbildung 6 Beispiel von Betonschutzelementen

3.5.2.3 Zaundetektion

(1) Mittel geeigneter Detektionsmassnahmen wird der äusserste Perimeter (im Regelfall der Zaun) des Geländes überwacht. Ziel der Massnahme ist es, potentielle Eindringlinge oder Angreifer frühzeitig zu erkennen. Dies geschieht mittels einer Detektion (Intelligenter Zaun, intelligente Kameras), welche erkennt, falls ein Angreifer versucht den Zaun zu übersteigen, zu durchschneiden oder sich sonst wie unerlaubt Zugang zum Areal zu verschaffen. Im Regelfall bedingt diese Massnahme eine nachgelagerte zentrale Überwachungseinrichtung, welche in der Lage ist auf Vorfälle geeignet zu reagieren.

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	keine Massnahmen	
Mittlerer Schutz	Perimeter Detektion: intelligente Überwachung des Zauns oder der Mauer mittels Sensoren oder Kamerasystemen.	1,2,3
Hoher Schutz	Zusätzlich zur Perimeter Detektion, welche je nach Ausbildungsform, möglicherweise nur das Auftreten eines Vorfalles detektieren, werden Bildsysteme verwendet, welche es erlauben den Alarmauslösungsgrund visuell zu identifizieren und im Bedarfsfall mögliche Eindringliche optisch zu verfolgen.	1,2,3

Tabelle 6 Schutzmassnahmen Zaundetektion

Ausführungsbeispiele

Videoanalyse am Zaun

Detektionssystem am Zaun

Abbildung 7 Beispiele von intelligenten Zaunsystemen

3.5.2.4 Hauptzugang Areal

(1) Um das Areal vor unbefugten Zutritten zu schützen wird dem Hauptzugang besondere Beachtung geschenkt. Der Hauptzugang kann sich hierbei direkt an einer Gebäudehülle befinden und muss nicht zwingend über einen Perimeterschutz (Zaun) erfolgen. Mittels separater Sicherung des Zuganges wird gleichzeitig die Zahl der Arealzutritte reduziert. Im Idealfall steht so nur noch ein gesicherter und überwachter Zutritt auf das Gelände zur Verfügung. Dem Arealzugang kommt in der gesamten Sicherheitsarchitektur eine bedeutende Rolle zu. Die Zutritte zum UW sollen eindeutig nachvollziehbar sein.

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	Der Einsatz eines elektronisches Schliesssystems ermöglicht es, Zutritte zu sperren und diese nach zu vollziehen	1,2,3
Mittlerer Schutz	Der Einsatz eines zentralen online Schliesssystems ermöglicht zusätzlich den direkten remote Zugriff. Dies erlaubt es online Zugriffe zu sperren oder freizugeben. Dies bedingt aber auch eine zentrale Verwaltungsstelle, welche die Rechte verwaltet und kontrolliert. Dies wiederum hat auch einen positiven Einfluss bezüglich der Personensicherheit.	1,2,3
Hoher Schutz	Zusätzlich zu der online Variante des Schliesssystems findet eine visuelle Überprüfung des Hauptzuganges mittels Kameras statt.	1,2,3

Tabelle 7 Schutzmassnahmen Hauptzugang Areal

Ausführungsbeispiele

Abbildung 8 Beispiele von Zutrittssystemen

3.5.2.5 Arealüberwachung

(1) Die Arealüberwachung stellt sicher, dass bei unbefugten Zutritten eine technische Überwachung und Nachverfolgung sichergestellt werden kann. Gleichzeitig leistet diese einen zusätzlichen Schutz bezüglich Arbeitssicherheit. Um die Sichtbarkeit zu verbessern gelangen auch zusätzliche Beleuchtungssysteme in den Einsatz.

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	keine Massnahmen zur Arealüberwachung	
Mittlerer Schutz	Installation von zusätzlichen Beleuchtungen an kritischen Stellen und punktuelle Kameraüberwachungen kritischen Arealbereiche	1,2,3
Hoher Schutz	Zusätzlich zum erweiterten Schutz findet eine systematische Arealüberwachung mittels Kameras statt. Die Beleuchtungssysteme werden zusätzlich mit einem Zufallsgenerator ausgestattet.	1,2,3

Tabelle 8 Schutzmassnahmen Arealüberwachung

Ausführungsbeispiele

Abbildung 9 Ausführungsbeispiele von Überwachungskameras

3.5.2.6 Gebäudehülle

(1) Die Gebäudehülle wird mittels geeigneter materialen auf einem vorbestimmten Härtungsgrad gebracht. Dies erschwert potentiellen Angreifern das Eindringen in das Gebäude durch die Gebäudehülle. Der Härtungsgrad ist abhängig von der Bedeutung des Unterwerkes für das Gesamtnetz und der topographischen Lage des Werkes. Von dieser Betrachtung ausgenommen sind die Zugänge in das Gebäude.

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	keine Massnahmen	
Mittlerer Schutz	Härtung der Gebäudehülle gemäss bestehender Normregelungen (Widerstandsklassen) in Abhängigkeit von der Kritikalität des Unterwerkes.	2
Hoher Schutz	Zusätzlich zur Härtung des Gebäudes erfolgt eine Detektion, Überwachung der Gebäudehülle	1,2,3

Tabelle 9 Schutzmassnahmen Gebäudehülle

Ausführungsbeispiele

Fenstergitter

Einbruchmeldeanlage

Einbruch-Sensor

Abbildung 10 Beispiele von Härtungsmassnahmen am Gebäude

3.5.2.7 Gebäude Zugänge

(1) Nebst der Gebäudehülle werden auch die Zugänge in das Gebäude gesichert. Davon betroffen ist hauptsächlich der zu definierende Hauptzugang in das Gebäude. Idealerweise wird die Anzahl der Zugänge in das Gebäude auf das betrieblich notwendige Mindestmass minimiert. Des Weiteren sind bei den Massnahmen auch die Fenster in der Gebäudehülle mit einzubeziehen. Hier lassen sich geeignete Massnahmen relativ einfach realisieren (Fenstergitter, Alarmkontakt, etc.). Sollte kein Arealzugang bestehen (Zaun) und das Gebäude damit den Perimeterschutz übernimmt, so gelten für den Zutritt die Regeln des Arealzuganges.

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	mechanische Schliessung	2
Mittlerer Schutz	Elektronisches Schliesssystem, Zutritte sperrbar und nachvollziehbar	1,2,3
Hoher Schutz	Zentrales online Schliesssystem mit Kameraüberwachung	1,2,3

Tabelle 10 Schutzmassnahmen Gebäude Zugänge

(2) Ausführungsbeispiele siehe Kapitel Hauptzugang Areal.

3.5.2.8 Raumüberwachung

(1) Die Raumüberwachung alarmiert bei einem unbefugten Zutritt eine zentrale Stelle. Die Alarme werden danach gemäss Alarmierungsprozess an weitere Stellen weitergeleitet. Der Berechtigte Zugang ist durch einen Code, Schlüssel oder einer Meldung an die zentrale Stelle zu autorisieren. Vorzugsweise sind die Zugänge zu diesen Räumen mit einer Kamera ausgerüstet (Nachvollziehbarkeit eines Alarms).

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	keine Massnahmen	
Mittlerer Schutz	Einbruchmeldeanlage (Bsp. Raum- und Zugangsüberwachung mit Sensoren)	1,2,3
Hoher Schutz	Zusätzlich mit Kameras überwacht	1,2,3

Tabelle 11 Schutzmassnahmen Raumüberwachung

(2) Ausführungsbeispiele Einbruchmeldeanlage und Kameras (Abbildungen 9 und 10).

3.5.2.9 Raumzugänge

(1) Schutz aller Zugänge eines Raumes. Davon betroffen ist der Hauptzugang und wenn vorhanden alle anderen Türen welche den Raum erschliessen. Vorzugsweise wird dem Raum ein Hauptzugang zugeteilt, welcher geschützt wird und die anderen Zugänge werden verschlossen.

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	keine Massnahmen	
Mittlerer Schutz	Mechanische Schliessung	2
Hoher Schutz	Elektronisches Schliesssystem, Zutritte sperrbar und nachvollziehbar	1,2,3

Tabelle 12 Schutzmassnahmen Raumzugänge

Ausführungsbeispiele

Abbildung 11 Ausführungsbeispiele von Raumschliesssystemen

3.5.2.10 Element

(1) Schutz eines Racks oder Schaltschrank mit systemkritischen Elementen. Nebst den empfohlenen technischen Sicherungsmassnahmen empfiehlt es sich, das Rack oder den Schrank in einer massiven Bauart zu bevorzugen/nachzurüsten (Bsp. massive Stahlverkleidung, keine sichtbaren Schrauben, etc.)

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	keine Massnahmen	
Mittlerer Schutz	Einbruchmeldeanlage (Bsp. Zugriffsüberwachung mit Sensoren)	1,2,3
Hoher Schutz	Zusätzlich mit Kameras überwacht	1,2,3

Tabelle 13 Schutzmassnahmen Element

(2) Mögliche Ausführungsbeispiele Einbruchmeldeanlage und Kameras (Abbildungen 9 und 10).

3.5.2.11 Element Zugang

(1) Der Element Zugang bezieht sich auf das Schliesssystem der Racks oder der Schränke mit systemkritischen Elementen. Die unbefugte Öffnung des Elements soll durch eine geeignete Schliessung ausgerüstet werden.

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	keine Massnahmen	
Mittlerer Schutz	Mechanische Schliessung	2
Hoher Schutz	Elektronisches Schliesssystem, Zugriff sperrbar und nachvollziehbar	1,2,3

Tabelle 14 Schutzmassnahmen Element Zugang

(2) Mögliche Ausführungsbeispiele Mechanische oder mechatronische Schlüssel, online Schliesssystem (Abbildung 11).

3.5.2.12 Trafo-Schutz

(1) Zu den kritischsten Elementen eines Unterwerkes gehören die Transformatoren. Insbesondere der ballistische Schutz (Einwirkung von Objekten mit hoher kinetischer Energie) stellt eine besondere Herausforderung dar. Als Schutzmassnahme kann der Transformator – unter Berücksichtigung der betrieblichen Anforderungen – beispielsweise ballistisch geschützt werden. Ein solcher Schutz ist aber extrem kostenintensiv und gilt es im Rahmen der Schutzzieldefinition zu hinterfragen und je Unternehmen zu klären.

(2) Sollte sich ein Unternehmen entschliessen, seine Transformatoren gegen kinetische Einwirkungen zu schützen, könnten folgende Klassierungen zu Anwendung gelangen.

Schutzklasse	Beschreibung der Schutzmassnahme	Schutzziele
Normaler Schutz	keine Massnahmen	
Mittlerer Schutz	Einhausung des Transformators (Beton-, Stein- oder Stahl-Lösungen)	1,2
Hoher Schutz	Einhausung inkl. Schliessung des „Daches“	1,2

Tabelle 15 Schutzmassnahmen Trafo-Schutz

(3) Ausführungsbeispiele Steinkörbe, Beton-Elemente oder Gitter-Varianten.

3.5.3 Erläuterungen zu den Schutz-Massnahmen

(1) Besitzt ein Unterwerk aufgrund seiner Lage oder baulichen Ausgestaltung über keinen Zaun (Beispiel: unterirdische GIS-Anlage), so kommt in der Planung der Massnahmen dem Thema „Zugang Gebäude“ die gleiche Bedeutung zu wie beim Thema „Hauptzugang Areal“.

(2) Je nach Typologie und Gestaltung eines Unterwerkes kann es auch zu Kombinationen von Massnahmen kommen.

3.6 Schritt 5: Überprüfung (Aktualisierungszyklus und Audit)

(1) Nach Abschluss der Planung, Konzeption und Umsetzung der Sicherungsmassnahmen gehen diese in den Normalbetrieb über. Aufgrund sich verändernder Rahmenbedingungen (Beispielsweise der Bedeutung eines Unterwerkes für die Stabilität des Gesamtnetzes) oder eine Veränderung der Bedrohungssituation beispielsweise im europäischen Energiesektor, macht es Sinn, die getroffenen Massnahmen in regelmässigen Abständen zu Überprüfen.

(2) Unter Berücksichtigung der eingesetzten technischen Sicherungsmittel (siehe Kapitel 2.5.2) macht es Sinn, die Gesamtkonzeption eines Unterwerkes in regelmässigen Abständen zu überprüfen. Die Prüfzyklen orientieren sich an den „Halbwertszeiten“ der getroffenen technischen Schutzmassnahmen.

(3) Sollte es aus betrieblichen Gründen zu einem Um- oder Neubau des Unterwerkes kommen, macht eine Überprüfung ebenfalls Sinn.

3.7 Investitionen

(1) Grundsätzlich besteht die Möglichkeit, jede der einzelnen Schutzmassnahmen und der daraus resultierenden möglichen Massnahmenkombinationen einer Kosten-Nutzen-Analyse zu unterziehen.

(2) Da sich die Mitigationswirkung der einzelnen Massnahmen im Anwendungsfall eines einzelnen Unterwerkes aber nur ungenügend darstellen lässt, wird in diesem Fall bewusst auf diese Anwendung verzichtet.

3.8 Awareness und betriebliche Massnahmen

(1) Technische Lösungen allein genügen jedoch nicht um die gewünschte Sicherheitsgewinne zu erzielen. Ergänzend braucht es klare und verbindliche prozessuale und organisatorische Massnahmen.

3.8.1 Bewusstsein der Mitarbeiter

(1) Die Mitarbeiter, Subunternehmer und Betreiber der Unterwerke müssen durch Schulungen auf mögliche Sicherheitsrisiken hingewiesen werden. Nebst den technischen Sicherungsmassnahmen braucht es auch betriebliche und prozessuale Leitlinien wie das Thema „Sicherheit“ auf einem Unterwerk zu handhaben ist. Hierzu sollten unternehmensspezifische Sicherheitsrichtlinien definiert werden. Dieses betrifft im Besonderen auch eine Sensibilisierung auf die möglichen Cyber Angriffswege und deren möglichen Schutzmassnahmen im Bereich physische Sicherheit.

(2) Schulungen, Überprüfungen des Wissenstandes und der Awareness sollten in regelmässigen Abständen durchgeführt werden.

(3) Im Fokus steht bei all diesen Massnahmen die Awareness Bildung der Mitarbeitenden. Dies mit dem Ziel eine eigentliche Sicherheitskultur mit dem entsprechenden Verständnis zu erarbeiten und zu festigen.

3.8.2 Definition und Prüfung von Zutrittsberechtigungen

(1) Analog zu der Vergabe von Administratorenrechte im Bereich der Cyber-Sicherheit, ist es sinnvoll, den Zugang zu kritischen Anlagenteilen zu regeln und Berechtigungen zu vergeben. Diese Berechtigung kann an verschiedene Bedingungen geknüpft sein. Dazu gehören beispielsweise:

- Nachweis über ausreichende Fähigkeiten und Kompetenzen
- Unbedenklichkeitsüberprüfungen wie eine Personensicherheitsüberprüfung

(2) Insbesondere bei kritischen Anlagen der Netzebene 1 und 3 kommt dem Thema der Personensicherheitsprüfung eine bedeutendere Rolle zu. Diesem Umstand trägt auch der Bund Rechnung, indem mit der Verabschiedung der Energiestrategie 2050 die rechtliche Grundlage geschaffen worden ist, eine solche Prüfung durch Bundesstellen vorzuschreiben und zu veranlassen.

3.8.3 Standortbesuche

(1) Mittels Standortbesuche resp. –Überprüfungen wird mittels Checkliste der Umsetzungsstand der Massnahmen geprüft. Gleiches gilt für die Einhaltung der betrieblichen Sicherheitsprozesse.

(2) Diese Überprüfungen bilden den zentralen Bestandteil eines kontinuierlichen Verbesserungsprozesses (KVP).

3.8.4 Reaktion auf Sicherheitsvorfälle

(1) Sicherheitsvorfälle und Angriffe lassen nicht gänzlich durch adäquate Schutzmaßnahmen vermeiden. Demzufolge müssen für den erfolgreichen Angriffsfall oder andere Sicherheitsvorfälle Notfallpläne

ausgearbeitet und erprobt werden. Diese verfügen in Abhängigkeit von der Kritikalität des Unterwerkes unterschiedliche Umfänge und Bearbeitungstiefen.

(2) Dazu gehören folgende Massnahmen:
- Definition von Notfallplänen und Wiederanlaufplänen (einschließlich Wissensdatenbank, Lessons-Learned und Kommunikationswege) in einem standardisierten Verfahren. Diese Pläne sind bekannt und geschult. Sowie vor Ort und in einem bezeichneten Raum rasch verfügbar.
- Test der Notfall-Pläne und Wiederanlauf-Pläne einmal jährlich. Bei den Tests kann es sich um Echte Tests“ handeln oder auch um Reviews der bestehenden Pläne und Grundlagen.

3.9 Physische Schutz-Massnahmen in Bezug zum Thema Cyber Sicherheit

(1) Die physischen Schutzmassnahmen haben nicht nur das Ziel, die primären Komponenten eines Unterwerkes zu schützen, sondern tragen gleichzeitig auch dazu bei, einen Schutz der kritischen Cyber Komponenten zu gewährleisten.

(2) Erst eine integrale Betrachtung des Themas „Sicherheit“ erlaubt es, effiziente und wirksame Schutz-Konzepte zu planen und umzusetzen.

(3) Insbesondere auf Unterwerken kommt dem Schutz der ICT-Komponenten durch physische Massnahmen eine wichtige Rolle zu (siehe auch VSE-Dokument „OT-Grundschutz in Unterwerken“). Dadurch kann beispielsweise sichergestellt werden, dass:
- Keine unbefugten Personen physischer Zugang zu sicherheitskritischen Orten erhalten
- Physikalische Veränderung, Manipulation, Diebstahl oder sonstige Entfernung oder Zerstörung bestehender Systeme, Infrastruktur, Kommunikationsschnittstellen, Personal oder physischer Standorte verhindert werden
- Unerlaubte Beobachtung von sensiblen Informationen durch visuelle Beobachtung, Notizen, Fotografien oder durch andere Mittel unterbunden werden
- Unerlaubte Einführung neuer Systeme, Infrastruktur, Kommunikationsschnittstellen oder anderer Hardware verhindert werden
- Unerlaubte Einführung von Geräten, die entworfen wurden, um Hardware-Manipulationen, Abhören oder andere schädliche Tätigkeiten durchzuführen mittels USB-Speichergerät, Wireless Access Points, Bluetooth oder anderen mobilen Technologien ausschliessen

(4) Die physische Sicherung beispielsweise des Kontrollzentrums bzw. Kontrollraumes reduziert die Wirkung vieler Bedrohungen. So haben Kontrollzentren und Kontrollräume häufig permanent angemeldete Arbeitsbereiche mit kontinuierlichem Zugriff auf primäre Steuerungsserver, wobei die Reaktionsgeschwindigkeit und die ständige Sicht auf die Anlage von grösster Bedeutung sind. Zudem werden in diesen Bereichen oft die Server selbst und andere kritische Computerknoten und Steuersysteme gehostet. Der Zugang zu solch kritischen Anlagenteilen sollte durch geeignete Massnahmen (physischer Art) geregelt werden und eine eindeutige Identifizierung und ein Monitoring erlauben. In vielen Fällen ist es erforderlich, eine Offsite-Notzentrale / Leitstelle zur Verfügung zu halten, damit die Steuerung sichergestellt werden kann, wenn die primäre Leitstelle unbrauchbar wird.

(5) Um die geeigneten Massnahmen zum Schutz der kritischen IT-Systeme auf einem Unterwerk treffen zu könne, bedarf es vorgängig einer klaren Analyse der kritischen IT-Komponenten und der möglichen Bedrohungsszenarien (VSE-Dokument „OT-Grundschutz auf Unterwerken“). Erst mit diesem Wissen kann ein effektiver Schutz etabliert werden.

(6) Weiter muss in der Erarbeitung und Umsetzung der physischen Schutzmassnahmen bedacht werden, dass bei der Verwendung von IT-basierten Sicherungssystemen (beispielsweise bei der Verwendung von IP-basierten Kameras), zusätzliche Angriffspunkte geschaffen werden, welche durch geeignete Cyber-Schutzmassnahmen abgedeckt werden müssen.

(7) Das VSE-Dokument „Grundschutz OT in der Stromversorgung“ regelt die erforderlichen Auflagen.

4. Abkürzungen

BABS	Bundesamt für Bevölkerungsschutz
BFE	Bundesamt für Energie
BWL	Bundesamt für wirtschaftliche Landesversorgung
ElCom	Eidgenössische Elektrizitätskommission
GIS	Gas isolierte Schaltanlage
ICT	Informations- und Kommunikationstechnologie
IKT	Informations- und Kommunikationstechnologie
MELANI	Melde- und Analysestelle Informationssicherung
SCADA	Supervisory Control and Data Acquisiton
SKI	Schutz kritischer Infrastruktur
UW	Unterwerk