swissgrid

Swissgrid AG
Bleichemattstrasse 31
Postfach
5001 Aarau
Schweiz

T +41 58 580 21 11
info@swissgrid.ch
www.swissgrid.ch

VB C1: Lastenheft Generalplanerleistungen Phase 1

Ausschreibung: Generalplanerleistungen
Projektbezeichnung: Physischer Schutz Unterwerke

Datum 30.Oktober 2019

Verfasser Swissgrid AG

swissgrid

Inhalt

Abbildungs- und Tabellenverzeichnis

1. Einleitung

Vorliegendes Lastenheft ist die verbindliche Arbeitsgrundlage für alle Projektbeteiligten im Projekt "Physischer Schutz Unterwerke". Es wird im Rahmen der SIA Phasen weiterentwickelt.

1.1 Zweck des Lastenheftes

Das Lastenheft (LH) definiert die bauherrenseitigen Anforderungen an die Generalplanerleistung und an das Projekt, welche im Rahmen der Projektbearbeitung zu berücksichtigen sind.

1.2 Freigabe und Pflege

Das Lastenheft ist Basis der Submission der Generalplanerleistung und der späteren Umsetzung. Die Pläne der Ausschreibung sind Teil des Lastenheftes.

2 Das Projekt "Physischer Schutz Unterwerke"

2.1 Einleitung / Ausgangslage

Die Swissgrid AG hat alleiniges oder gemeinschaftliches Eigentum an ca. 120 Unterwerken über die gesamte Schweiz verteilt. Ab Januar 2013 hat Swissgrid die Unterwerke von den vormaligen rund 20 Eigentümern übernommen. Die Rechte von Swissgrid am Grund, auf dem die Unterwerke stehen, sind unterschiedlich ausgestaltet: Swissgrid ist teilweise Grundeigentümerin, teilweise besitzt sie ein Baurecht und teilweise ein obligatorisches Nutzungsrecht.
Die Unterwerke sollen bezüglich Sicherheit (physischer Schutz vor unberechtigtem Zutritt, mutwilliger Beschädigung und Beeinträchtigung der Stromversorgungssysteme), Entwicklungsabsichten und Immobilienstrategie baulich auf das neue geforderte Niveau gebracht werden.
Alle Unterwerke wurden auditiert, diverse Unterlagen liegen pro Objekt vor, und die bestehenden Sicherheitsstandards der jeweiligen Unterwerke sind bekannt.
Ziel: Alle Unterwerke sicherheitsmässig auf einheitlichen Stand bringen.

In einem ersten Schritt sollen 10 der bestehenden ca. 120 Unterwerke in der Gesamtschweiz den neuen Sicherheitsstandards /-anforderungen des physischen Schutzes angepasst werden.
Die Namen der 10 ausgewählten Unterwerke wird in der Phase II bekanntgegeben.

2.2 Zielsetzung

Der mandatierte Generalplaner soll die Ziele und Anforderungen der Bauherrschaft planen und umsetzen. In einem ersten Schritt sollen vorerst 10 Unterwerke den neuen geforderten Sicherheitsstandards baulich angepasst werden.
Parallel soll eine Art Baukasten-Tool für Sicherheitsmaßnahmen erstellt werden, um die weiteren Unterwerke den neuen Sicherheitsstandards anpassen zu können.

2.2.1 Absichten der Swissgrid

Die Swissgrid will durch den physischen Schutz der Unterwerke und der entsprechenden Prozesse sicherstellen, dass

- die Branchenstandards eingehalten werden;
- die Risiken bedarfs- und zeitgerecht adressiert werden;
- sie sich auf ein Schutzniveau zubewegt, welches im Branchenvergleich als vorbildlich (best practice) für ein sicheres, effizientes und leistungsfähiges Netz anerkannt wird;
- die übergeordneten Unternehmensziele der Integralen Sicherheit erreicht oder übertroffen werden;
- die Massnahmen des physischen Schutzes mit den übrigen Prozessen und Systemen der Swissgrid abgestimmt sind, dabei ist auch zu definieren welche Alarme wo zu bearbeiten sind.

2.3 Erläuterung

Das Schweizer Übertragungsnetz umfasst 6700 Kilometer Leitungen, 12 000 Masten, 125 Unterwerke mit 146 Schaltanlagen sowie 41 Verbindungen ins Ausland. Es besteht sowohl aus 380-Kilovolt- als auch aus 220-Kilovolt-Leitungen: Während Erstere grösstenteils für den Import und Export von Strom genutzt werden, speisen die grossen Schweizer Kraftwerke ihre Energie mehrheitlich in das 220-Kilovolt-Netz ein. Die Spannung in Kilovolthöhe ist im Übertragungsnetz nötig, um Energie möglichst verlustarm über weite Strecken zu transportieren.

Bis die von den Kraftwerken produzierte Energie für die Endverbraucher nutzbar ist, wird die Spannung über sieben Netzebenen auf 400 und 230 Volt reduziert. Zu diesen Ebenen gehören neben der Höchst-, Hoch-, Mittel- und Niederspannungsebene drei verbindende Transformationsebenen.

Die in Unterwerken untergebrachten Schaltanlagen sind Knotenpunkte zwischen Leitungen. Hier wird die Energie auf eine tiefere Spannungsebene transformiert und in die unteren Netzebenen weitergegeben. Ausserdem trennen und verbinden die Netzleitstellen von Swissgrid in den Schaltanlagen Leitungen durch Schalthandlungen und lenken damit die Energieflüsse.

Der elektrische Strom kommt über die Leitung an der „Stromkreuzung“ an und fließt durch ein Schaltfeld weiter zu einem Transformator. Dort erfolgt in der Regel die Transformation auf eine andere Spannungsebene. Auf der neuen Spannungsebene kann der elektrische Strom durch eine vom Unterwerk abgehende Leitung weiter bis zum nächsten Unterwerk oder direkt zu einem Verbraucher transportiert werden.

Zu einem Unterwerk gehören neben den aktiv an der Stromleitung und Spannungsumwandlung beteiligten Geräten, den sogenannten Betriebsmitteln, auch Gebäude. Die wichtigsten sind das Betriebsgebäude und Relaishäuser, in denen die Technik für die Steuerung und Überwachung der Betriebsmittel untergebracht ist.

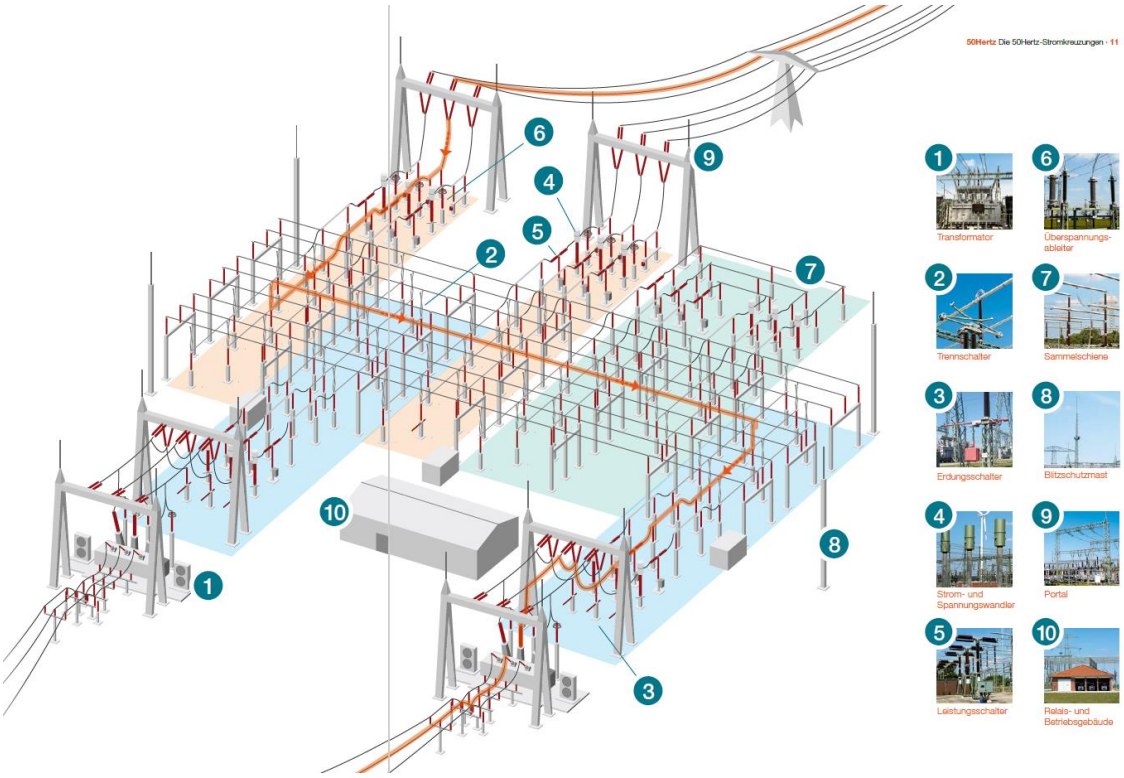


Abbildung 1: Schema eines Unterwerks: Quelle 50Hertz

Der elektrische Strom erreicht das Unterwerk über eine ankommende Leitung, die zum Leitungstrennschalter mit Erdungsschalter führt. Er bildet die Verbindung zwischen Leitung und Schaltanlage. Als Nächstes folgen der Strom und Spannungswandler in einem Gerät für Überwachung und Schutz. Der Leistungsschalter ist das zentrale Element eines Schaltfeldes. Er schaltet den Strom ein und aus, sowohl unter normalen Bedingungen als auch im Fehlerfall. Das Schaltfeld ist über die Sammelschienentrennschalter an alle Sammelschienen angeschlossen.

Die unterschiedlichen Sammelschienen können über ein Kupplungsschaltfeld miteinander verbunden werden. An den Sammelschienen sind die Trafoschaltfelder angeschlossen. Der Transformator verbindet die unterschiedlichen Spannungsebenen. An seiner Unterspannungsseite folgt ein weiteres Transformatorschaltfeld, die abgehende Leitung geht von dort zum nächsten Unterwerk.

3 Leistungsumfang

3.1 Leistungsumfang

Ausschreibungs- und Vertragsgegenstand ist die Erbringung aller notwendigen Planerleistungen sowie sämtlicher Spezialisten- und Koordinationsleistungen (Grundleistungen nach SIA 102, 103, 105, 106 und 108 und besonders zu vereinbarenden Leistungen inklusive Gesamtleitung nach SIA 112; SIA Ordnungen Stand 2014) für das beschriebene Bauvorhaben in der Funktion eines Generalplaners.
Der Generalplaner hat sämtliche zur Erreichung der von Swissgrid definierten Ziele erforderlichen Planerleistungen zu erbringen und zu verantworten.

Der Leistungsbereich umfasst die Erarbeitung und Vervollständigung und die Erarbeitung der SIA Teilphasen 31 (Vorprojekt Vervollständigung, Validierung und Konkretisierung pro UW) bis und mit Teilphase 41 (Ausschreibung, Offertvergleich, Vergabeantrag). Sofern sich Swissgrid nicht für ein „TU-Modell“ entscheidet, umfasst das Generalplanermandat ausserdem die Teilphasen 51 bis 53. Der Generalplanerzuschlag ist im zu offerierenden Honorar enthalten.

Betreffend Vertrag gilt die Verständigungsnorm SIA 112 «Modell Bauplanung» (Ausgabe Nov. 2014) im Rahmen der Ausschreibung als Verständigungsbasis. Der Generalplanervertrag wird auf Basis der entsprechenden Honorarordnungen für die einzelnen Disziplinen erstellt (SIA HO 102/103/105/106/108). Die Vertragsvorlage befindet sich in den Ausschreibungsunterlagen.

Der Generalplaner offeriert für die Vervollständigung der Vorprojektphase (Phase 31) und für die Erarbeitung der Phasen 32 (Bauprojekt) bis 53 (Inbetriebnahme, Abschluss) ein Honorar, das teilweise als Festhonorar und teilweise nach Zeitaufwand ausgestaltet ist. Die Teilphasen werden durch Swissgrid phasenweise ausgelöst.

Phase 1 Strategische Planung	Teilphase 11	Bedürfnisformulierung, Lösungsstrategien
Phase 2 Vorstudien	Teilphase 21	Definition des Bauvorhabens, Machbarkeitsstudie
	Teilphase 22	Auswahlverfahren
Phase 3 Projektierung	Teilphase 31	Vorprojekt
	Teilphase 32	Bauprojekt
	Teilphase 33	Bewilligungsverfahren
Phase 4 Ausschreibung	Teilphase 41	Ausschreibung, Offertvergleich, Vergabeantrag
Phase 5 Realisierung	Teilphase 51	Ausführungsprojekt
	Teilphase 52	Ausführung
	Teilphase 53	Inbetriebnahme, Abschluss

Variante „TU-Modell“:
Swissgrid behält sich vor, für die Phase 5 Realisierung einen Totalunternehmer zu beauftragen (sog. „TU-Modell“). Falls Swissgrid auf ein „TU-Modell“ umstellen möchte, teilt sie dies dem Generalplaner bis spätestens …. schriftlich mit. In diesem Fall entfällt die Pflicht des Generalplaners zur Erbringung von Generalplanerleistungen für Phase 5. Entschädigungsansprüche infolge der Reduktion des Leistungsumfangs stehen dem Generalplaner keine zu. Die vom Generalplaner mandatierten Subplaner und Fachplaner werden beim „TU-Modell“ dem Totalunternehmer überbunden, der anstelle des Generalplaner in sämtliche (Sub-)Planerverträge eintritt; es ist Aufgabe des Generalplaners, in

die Verträge mit seinen Subplanern eine Vertragsbestimmung aufzunehmen, die einen solchen Parteiwechsel vorbehaltlos ermöglicht.

Unterstützung bei der Erstellung von Konzepten für Betrieb und ICT sowie Erarbeitung von Prozessen

Die Einführung der neuen Sicherheitssysteme auf den Unterwerken mit Anschluss der Sicherheitszentrale bedingt die Erstellung neuer Prozesse und Betriebskonzepte und eine Zuordnung der Alarme und Informationen an die entsprechenden Swissgrid-internen Stellen. Zur Umsetzung möchte Swissgrid aus Gründen knapper eigener Ressourcen und zusätzlicher fachlicher Expertise auf externe Unterstützung zurückgreifen. Der Generalplaner sichert zu, dass er über ausgewiesene Erfahrung im Bereich Einführung solcher Systeme und über die entsprechenden Projektkoordinationsfähigkeiten verfügt. Der Generalplaner hat ein entsprechendes Angebot zu erstellen vgl. auch Ziffer 8 und 10.

3.2 Optionale Leistung: QS-Berater

Bei der Umstellung auf das „TU-Modell“ steht der Beauftragte (Generalplaner) Swissgrid auf deren Wunsch als QS-Berater zur Verfügung. Zu den Hauptaufgaben des Beauftragten als QS-Berater gehören insbesondere:

- Sicherstellen, dass Ausführung gemäss Bestellung (Ausschreibungsunterlagen für Bauunternehmen) erfolgt
- Die Schwergewichte des QS Mandates werden vor der Realisierung von Swissgrid festgelegt.

Ergänzungen und Präzisierungen der vom Beauftragten zu erbringenden Leistungen durch Swissgrid bleiben vorbehalten.

3.3 Optionale Leistung: Digitalisierung der UWs

Es sind historisch gewachsene Planunterlagen von den Unterwerken vorhanden 2D. Vektorisierte Daten der UWs sind nicht vorhanden. Auf Verlangen von Swissgrid hat der Generalplaner zu prüfen, ob sich aus Extrakten von vorhandenen Ortho-Fotos eine digitale Planungsgrundlage erarbeiten oder PDF-Dokumente als Planhintergrund verwenden lassen. Alternativ oder ergänzend kann Swissgrid verlangen, dass der Generalplaner eine 3D Neu-Erfassung der 10 Unterwerke anbietet, welche dann von Swissgrid betrieben werden und als neue Planungsgrundlage dienen könnte.

Ergänzungen und Präzisierungen der vom Beauftragten zu erbringenden Leistungen durch Swissgrid bleiben vorbehalten.

4 Grundlagen

4.1 Rechtliche Rahmenbedingungen

Die Planung und Realisierung des Projekts hat nach den aktuellen Gesetzen, Normen und Standards sowie nach dem anerkannten Stand der Technik zu erfolgen. Werden Gesetze und Normen im LH genannt dient dies ausschliesslich der Präzisierung der Bauherrenanforderungen und stellt keine abschliessende Aufzählung dar. Bei der Planung muss der gesamte Lebenszyklus des Unterwerkes / Gebäudes beachtet werden, insbesondere die Phasen Bau, Inbetriebnahme und Betrieb.

5 Richtlinien, Normen und Weisungen

5.1 Allgemein

Grundsätzlich gelten die eidgenössischen und die kantonalen Gesetze, Verordnungen, Richtlinien, Standards und Normen.

5.1.1 Allgemeine Grundlagen

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

5.1.2 Relevante spezifische Rechtsgrundlagen

- Bundesgesetz über die wirtschaftliche Landesversorgung (LVG), 8. Oktober 1982 (Stand 1. Jan. 2013)
- Bevölkerungs- und Zivilschutzgesetz (BZG), 4. Oktober 2002 (Stand 1. Januar 2012)
- Energiegesetz (EnG), 26. Juni 1998, (Stand 1. Januar 2014)
- Energieverordnung (EnV), 7. Dezember 1998, (Stand 1. Januar 2014)
- Stromversorgungsgesetz (StromVG), 23. März 2007 (Stand 1. Juli 2012)
- Stromversorgungsverordnung (StromVV), 14 März 2008 (Stand 3. Juni 2013)
- Energiestrategie 2050, BFE
- Relevante Weisungen der ElCom, 1/2013, 14. November 2013

5.1.3 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 Energie BFE*
  – Strategie Stromnetze, Ittigen, 2013
  – Grundlagen Energieversorgungssicherheit, Ittigen, März 2012
- *Bundesamt für Bevölkerungsschutz BABS*
  – Arbeiten SKI-Inventar, Bern, 2014
  – Leitfaden SKI, Bern, 2014
  – Risikobericht 2012, Katastrophen und Notlagen Schweiz, Bern 2013

5.1.4 Relevante Vorarbeiten der Branchen / Branchenverbände

- *Verband schweizerische Elektrizitätsunternehmungen (VSE)*
  – Branchenempfehlung Strommarkt Schweiz, ICT-Continuity, Aarau, Dezember 2011
  – Branchenempfehlung „Physischer Schutz Unterwerke“, Aarau, 2019
- *Bundesamt für Sicherheit in der Informationstechnik (BSI, D)*
  – IT-Grundschutz-Kataloge, 2016

5.2 Bau- und Gebäudetechnik

Wo in den Normen der SIA Anforderungen festgelegt sind, gelten die Zielwerte als Mindestanforderung (SIA 380/4, SIA 382/1).
Sämtliche einschlägigen Normen und Vorschriften des SIA, EN SN Normen, SUVA, Fachverbände, VKF, Vernehmlassungen, SWKI-Richtlinien, Vorschriften der Materialhersteller, geltende Gesetze, kantonale und örtliche Gesetze, usw. sind zu berücksichtigen.

Die Gebäudetechnik stellt einen integralen Teil dar und darf nicht losgelöst als Spezialdisziplin betrachtet werden. Generell sollen wartungsarme Systeme mit bewährter Technologie verwendet werden. Die Zugänglichkeit der Installationen für Wartung, Unterhalt und Nachinstallation muss gewährleistet sein.

6 Vorgaben und Schutzziele

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

Die Liste der nachfolgenden möglichen physischen Bedrohungen ist zu berücksichtigen:

Bedrohung gegen Infrastrukturen, beispielsweise:
- 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
- Einwirken von Kleindrohnen auf kritische Infrastrukturen
- Brandanschlag auf kritische Infrastruktur (Bsp. Trafo)

Für die Thematik „Physischer Schutz Unterwerke“ sind folgende Bedrohungs-Szenarien relevant:

1. Physische Angriffe zur Schwächung und Zerstörung von Infrastrukturen
2. Diebstahl von (betriebsrelevanten) Mitteln und Informationen
3. Unbefugter Zutritt
4. Vandalismus

6.1 Schutzziele

Mit der Definition der Schutzziele werden der jeweilige – unternehmensabhängige – Umfang und teilweise auch die Höhe des zu erreichenden Schutzgrades festgelegt.

Nachfolgend werden die 3 relevanten Schutzziele für den geplanten Schutz eines Unterwerkes dargestellt.

6.1.1 Kennen, benennen und überwachen der kritischen Bereiche

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

6.1.2 Schutz und Abschreckung / Verzögerung von Tätern

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.

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, verunsichert und/oder vertrieben werden.

6.1.3 Detektion und Nachvollziehbarkeit von Zutritten

Ziel ist es, jeden Zutritt zu einem Unterwerk 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 Nachvollziehbarkeit der Zutritte sicherzustellen.

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.

6.2 Kritikalität der Anlagen und Sicherheitslevels

Der Begriff Kritikalität bezieht sich in dieser Betrachtungsweise auf die Bedeutung des Unterwerkes bezüglich des Gesamtnetzes resp. der Bedeutung hinsichtlich der Gewährleistung der Versorgungssicherheit.

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

6.3 Sicherungslevels

Für die Planung und Umsetzung der Schutzmassnahmen für die ersten 10 Unterwerke (und die der nachfolgenden Unterwerke) wird der Schutzgrad durch Swissgrid vorgegeben. Gegenstand der Planung sind jene Elemente eines UW, die im Eigentum von SG stehen. Andere Elemente, die sich im Eigentum eines anderen (z.B. Verteilnetzbetreiber) befinden, dürfen nur soweit in die Planung einbezogen werden, als Swissgrid dies schriftlich oder per E-Mail bestätigt hat.

Dieser Schutzgrad für die ersten 10 Unterwerke orientiert sich an der VSE Branchenempfehlung „Physische Sicherheit für Unterwerke Nr. PSU/d Ausgabe 2019“

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. Die entsprechenden Detailangaben werden von Swissgrid bereitgestellt. Unternehmervarianten sollen aber möglich sein.

6.4 Abgrenzungen

Naturgefahren (Erdbeben, Hochwasser, Erdrutsch, etc.) werden in diesem Dokument nicht bearbeitet.

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.

7 Physical Security

7.1 Schutzzonen

Basierend auf einer sicherheitsmässigen Zonenbetrachtung können auf einem Unterwerk unterschiedliche Schutzzonen definiert werden. Unter Berücksichtigung potentieller Schutzmassnahmen 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

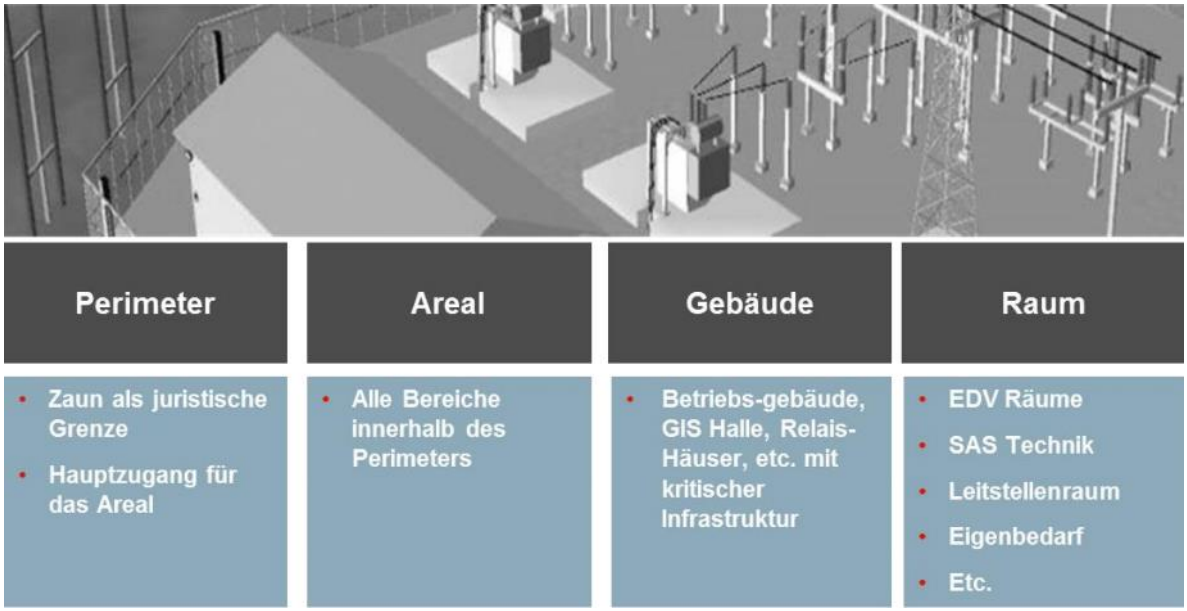


Abbildung 2: Schema Schutz-Zonen auf einem Unterwerk

7.2 Schutzmassnahmen pro Schutzzone

7.2.1 Zaun

Der Zaun stellt die 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 und dem Schutz von Drittpersonen. Diesbezüglich bestehen gesetzliche Vorgaben durch das Eidgenössische Starkstrominspektorat (ESTI).

Im Rahmen des vorliegenden Projektes ist ein Sicherheitszaun mit Untergrabschutz (Betonsockel) und 45 Grad-Ausleger (mit Schutzdraht) zu planen.

Gesamthaft kann mit einer Menge von etwa 10‘000 Laufmetern Zaun gerechnet werden.

Die Zaunspezifikation (inkl. Elemente wie Untergrabschutz und Übersteigschutz) erfolgt durch Swissgrid.

7.2.2 Perimeterdetektion

Zur Detektion des Perimeters werden „intelligente“ Thermalkameras eingesetzt. Diese Thermalkameras werden entlang der Arealgrenzen installiert und sind in der Lage, mittels einer intelligenten Analysesoftware, Eindringversuche zu erkennen und entsprechende Alarme (Reaktionen) auszulö-

sen. Diese Alarme sind an eine zentrale Stelle weiterzuleiten. Ziel der Massnahme ist es, potentielle Eindringlinge oder Angreifer frühzeitig zu erkennen.
Zur Verifikation der Alarme (und teilweise zur Arealüberwachung) werden PTZ-Kamerasysteme eingesetzt.
Es kann grob geschätzt mit folgenden Stück-Zahlen gerechnet werden (muss im Rahmen der Planung verifiziert werden):

Thermalkameras:	ca. 170
PTZ-Kameras:	ca. 70

Diese CCTV-Systeme sind über ein geeignetes LAN-System an die zentrale Rechnereinheit des Unterwerkes anzubinden. Zudem ist die erforderliche Stromversorgung sicherzustellen.

Die Definition der Anzahl, der Platzierung der Kameras und deren LAN-und Stromanbindung muss im Rahmen der Planung pro Unterwerk durch den GP vorgeschlagen und anschliessend zusammen mit Swissgrid festgelegt werden.

7.2.3 Hauptzugang Areal

Der Hauptzugang zum Areal (Perimeter oder Gebäudezugang, falls Gebäude den äusseren Perimeter darstellt) wird gehärtet und der Zutritt erfolgt über ein online Schliesssystem (Badgeleser). Das Zutrittskontrollsystem der Badgeleser muss mit dem heute bei Swissgrid eingesetzten System übereinstimmen. Gleichzeitig wird eine Video-Gegensprechanlage installiert. Weiter wird die Zahl der Arealzutritte reduziert. Im Idealfall steht so nur noch ein gesicherter und überwachter Zutritt auf das Gelände zur Verfügung.

7.2.4 Arealüberwachung

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 kommen zusätzliche Beleuchtungssysteme zum Einsatz.

Die Spezifikation der Video-Systeme wird von Swissgrid geliefert.

Für die Arealüberwachung ist mit ungefähr 10 weiteren PTZ-Kameras zu rechnen.

Zudem ist pro Unterwerk ein zusätzliches Beleuchtungssystem an kritischen Orten vorzusehen.

Mittels Lautsprechersystemen (ebenfalls im Bereich der kritischen Systeme) wird die Ansprechbarkeit möglicher Eindringlinge gewährleistet.

Die genaue Definition der Anzahl, der Platzierung der Kameras, der Licht- und Audiosysteme muss im Rahmen der Planung pro Unterwerk durch den GP erstellt und anschliessend zusammen mit Swissgrid festgelegt werden.

7.2.5 Gebäudehülle

Die Gebäudehülle (insbesondere Öffnungen) wird mittels geeigneter Materialien auf einem vorbestimmten Härtungsgrad gebracht. Dies erschwert das Eindringen von potentiellen Angreifern ins Gebäude.

Die Ausgestaltung und die Massnahmen sind pro Unterwerk mit Swissgrid abzustimmen.

7.2.6 Gebäudezugang

Nebst der Gebäudehülle werden auch die Zugänge in das Gebäude gesichert. Davon betroffen ist hauptsächlich der zu definierende Hauptzugang ins Gebäude. Idealerweise wird die Anzahl der Zugänge ins Gebäude auf das betrieblich notwendige Mindestmassreduziert. Des Weiteren sind bei den Massnahmen auch die Fenster in der Gebäudehülle miteinzubeziehen. Hier lassen sich geeig-

nete Massnahmen relativ einfach realisieren (Fenstergitter, Alarmkontakt, etc.). Sollte kein Arealzugang bestehen (Zaun) so übernimmt das Gebäude den Perimeterschutz, folglich gelten für den Zutritt die Regeln des Arealzuganges.
Die Ausgestaltung und die Massnahmen sind pro Unterwerk mit Swissgrid abzustimmen.

7.2.7 Raumüberwachung

Falls eine Raumüberwachung notwendig sein sollte, ist diese so zu planen und auszugestalten, dass die Alarme bei einem unbefugten Zutritt an eine zentrale Stelle weitergeleitet werden. Die Alarme werden danach gemäss Alarmierungsprozess an weitere Stellenübermittelt. 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).

7.2.8 Elemente

Falls auf einem Unterwerk der Schutz eines Racks oder Schaltschranks mit systemkritischen Elementen erforderlich werden sollte, so empfiehlt es sich, nebst den geforderten technischen Sicherungsmassnahmen das Rack/den Schrank in einer massiven Bauart einzukleiden (Bsp. massive Stahlverkleidung, keine sichtbaren Schrauben, etc.).

7.2.9 Elemente Zugang

Der Element Zugang bezieht sich auf das Schliesssystem der Racks oder der Schränke mit systemkritischen Elementen. Die unbefugte Öffnung des Elements soll durch ein geeignetes Schliesssystem ausgerüstet werden.

7.3 Anforderungen Physical Security

7.3.1 Allgemein

- Datensituation: Es besteht heute keine permanente Verbindung zwischen den eventuell vorhandenen Sicherheitstechniken auf Unterwerken und der Sicherheitszentrale;
  Die künftige Datenverbindung muss beidseitig erfolgen, das heisst eine Alarmsituation auf UW bewirkt Aufschaltung und Versand entsprechender Alarmsignale, im umgekehrten Fall muss die Sicherheitszentrale aktiv auf die installierten Geräte zugreifen können.

- Ein permanentes Übertragen von Kamerabildern ist nicht vorgesehen. Im Alarmfall oder falls von der SiZe (Sicherheitszentrale) gesteuert, folgt ein Aufschalten von vordefinierten Kameras.

- Standard auslösende Ereignisse sind beispielsweise unbefugte oder nicht kommunizierte Bewegungen über Arealgrenzen (Perimeterüberwachung) oder in Gebäude hinein oder innerhalb von Gebäuden in überwachten Bereichen.

- Grundsätzlich entsprechen die Anforderungen „Unterwerk“ denjenigen des Hauptsitzes Swissgrid in Aarau vorhandenen und bereits genutzten Cases. Die Bedienbarkeiten der Kamerasysteme sollten identisch sein.

7.3.2 Videoüberwachung Allgemein

- Anbindung an Sicherheitszentrale: Aufschaltungen (=Datenübertragung) bei Bedarf (=Alarmsignal [passiv], Herstellen der Verbindung aktiv durch SiZe); Aktoren in diesem Sinn sind entweder Sensoren wie eine intelligente Videoanalyse. Das heisst die Geräte detektieren einen Vorfall oder im umgekehrten Fall die SiZe

- Es ist pro Unterwerk mit schätzungsweise 25 Kameras zu rechnen (Thermal und PTZ, Videogegensprechanlage [VGSA] bei Eingang). Die genaue Stückzahl muss im Rahmen der Planung ermittelt werden. Bei Unterwerken mit grossem Umfang sind es deutlich mehr Kameras.

- Einsatz des gleichen Videomanagementsystems (VMS) wie in Aarau, um problemlose Anbindung an Sicherheitszentrale zu ermöglichen (IPS von Securiton)
- Diese Anzahl an Kameras macht eine „Multisite“-Architektur mit mehreren Verwaltungsbereichen des VMS erforderlich, um die Anbindung an die Sicherheitszentrale sicherzustellen
    - Multisite ist nach oben skalierbar und kann theoretisch unbegrenzt erweitert werden
    - Einzelne UW werden sinnvoll in Verwaltungsbereiche zusammengefasst, um Erweiterungen / Anbindungen weitere UW zu ermöglichen (Sinnvolle Obergrenze an Kameras für einen Verwaltungsbereich liegt bei ungefähr 150)
- Speicherung der Videodaten: 72h, mit der Option auf Erweiterbarkeit
- Speicherung der Daten erfolgt zentraler oder dezentral. Die geeignete Lösung muss im Rahmen des Projektes festgelegt werden. Aufschaltung der Videodaten erfolgt ausschliesslich in der Sicherheitszentrale sowie eines BCM-Standortes der SiZe.

7.3.3 Videoüberwachung Perimeterüberwachung

- Perimeterüberwachung wird durch lückenlose Überwachung mittels Wärmebildkameras ermöglicht. Alle ca. 50 Meter sind entsprechende Kameras vorzusehen. Die erforderlichen Positionen und Anstände sind durch den GP zu verifizieren resp. zu ermitteln.
- Alarmierung in SiZe bei Detektion (Alarmzonen entlang Perimeter)
- Aufschalten der Alarmierungsbilder (des detektierten Abschnittes) in SiZe
- Anwählen der individuellen Kameras zur Überprüfung, Zurückspulen im Rahmen der Datenschutzvorgaben, Zoom im Rahmen der technischen Möglichkeiten aus der SiZe
- Automatische Aktivierung und Ausrichtung von Arealüberwachungskameras bei Alarmen an Perimeter auf Alarmbereich, Aufschaltung auch dieser Bilder in SiZe

7.3.4 Videoüberwachung Arealüberwachung

- Arealüberwachung wird durch PTZ-Kameras (Pan-Tilt-Zoom) ermöglicht
- Arealüberwachung muss in der Lage sein, Perimeteralarme zu verifizieren (Übersicht Perimeterbereiche und [ausgewählte] Innenbereiche des Areals)
- Anwählen, vollständige Steuerung der PTZ-Kameras durch Sicherheitszentrale
- Zurückspulen der Videobilder im Rahmen der Datenschutzvorgaben

7.3.5 Zutrittskontrolle

- Verwaltung der Zutrittsrechte durch zentrale Stelle (SiZe) analog der bestehenden Zutrittsverwaltung mit kaba exos, einschliesslich (ad hoc) Vergabe und Entzug von Zutrittsrechten und -medien, Einsicht in Logbücher, etc.
- Zutrittskontrollsystem einschliesslich sämtlicher Geräte ist mit dem bestehenden System vollständig kompatibel oder entspricht diesem
- Direkte Steuerung der elektronischen Zutrittsmöglichkeiten (Freischaltung, Sperrung)
- Alarmierung in Sicherheitszentrale bei unbefugten oder unberechtigten Öffnungen (Türen zu lange Offen, elektronisch gesicherte Türen / Tore zu lange geöffnet)

7.3.6 Weitere Signale

- VGSA: Bei Klingeln wird Sicherheitszentrale kontaktiert und Videobild automatisch in SiZe aufgeschaltet

- Einbruchmeldeanlagen (EMA): können durch SiZe scharf / unscharf geschaltet werden. Weitere Funktionen werden im Laufe der weiteren Planung erarbeitet. Anbindung der SiZe (Steuerung der Informationen)

- Alarmgesichertes „Feuerwehr“-Rohr zur Aufbewahrung Schlüssel Notöffnung: Alarmsignal wird bei jeder Öffnung des Rohrs an Sicherheitszentrale versandt

- Lautsprecheranlage: optional (bei kritischen Unterwerken) sind auf dem Areal Lautsprecher verteilt, welche von der SiZe bedient werden können. Dies mittels vorbereiteter Textkonserven und individuellen Durchsagen

- Blitzlampen, spezielle Lampen: gelangen in sensiblen (kritischen) Bereichen zum Einsatz. Sind möglicherweise alarmgekoppelt (EMA) und müssten in diesem Fall einen Alarm auf der SiZe auslösen. Zudem müssen die Lichter von der SiZe aus bedienbar sein.

- Brandmeldeanlage (BMA): Überprüfung der Anbindung der bestehenden BMA (siehe auch Kap. 9) an die SiZe und allfällige Optimierung dieser. Wo eine BMA nicht vorhanden ist, muss eine BMA realisiert werden.

Allfällige zusätzliche Anforderungen sind im Rahmen des Projektes zu prüfen (Einbezug von Systembetrieb und Anlagenverantwortlichen).

7.3.7 Kurzzusammenfassung Ausrüstung

Elemente	Menge	Einheit
Zaun	ca. 10'000	Laufmeter
Thermalkameras	ca. 170	Stück
PTZ-Kameras	ca. 80	Stück
Beleuchtungssystem	1	pro UW
Lautsprechersystem	1	pro UW

Tabelle 1: Ausrüstungsliste

8 ICT-Infrastruktur Erwartete Kompetenzen und Lieferobjekte

Für die Umsetzung der Schutzmassnahmen müssen verschiedene ICT-Komponenten für Sicherheit und Überwachung (Video, Voice, Bewegungsmelder, Zutritt usw.) spezifiziert, aufgebaut und betrieben werden. Der GP verfügt über ICT-Fachplaner, die über die dafür notwendigen Kompetenzen und Erfahrungen verfügen.

Der Leistungsumfang der ICT-Fachplaner besteht aus folgenden Lieferobjekten:
- ICT-Konzepte
- Ausschreibung für ICT-Komponenten
- Leitung von Aufbau und Inbetriebnahme der ICT-Komponenten

ICT-Konzepte
Die ICT-Konzepte werden unter Mitwirkung von ICT-Engineers und Fachexperten von Swissgrid erstellt. Die ICT-Fachplaner sind für die Erstellung der ICT-Konzepte verantwortlich, wobei folgende Aufgaben wahrgenommen werden:
- Koordination von ICT-Engineers und Fachexperten
- Einbringen der eigenen Fachexpertise in Arealüberwachung mit ICT
- Inhaltliche Abstimmung der Beiträge
- Sicherstellen einer hohen Qualität der ICT-Konzepte (inhaltlich und formal)
- Mitarbeit und Unterstützung in der Erarbeitung von Inhalten
- Vorgaben bezüglich Vorgehensmethodik und Strukturierung
- Management-gerechte Ausarbeiten von Lösungsoptionen
- Einbringen des eigenen Netzwerkes für Referenzbesuche

Die Fachplaner sind dafür verantwortlich, dass die ICT-Konzepte einen Reifegrad erreichen, dass sie Swissgrid zur Genehmigung vorgelegt werden können.

Folgende ICT-Konzepte werden im Rahmen des Projektes erarbeitet:
- *ICT-Architektur*: Das Nutzungskonzept (siehe Kapitel 10.1) und die Architektur- und Security-Vorgaben von Swissgrid bilden die Grundlage für die abschliessende Definition der ICT-Architektur.
- *ICT-Spezifikation*: Mit Nutzungskonzept und ICT-Architektur als Grundlage werden sämtliche ICT-Komponenten spezifiziert. Es werden Gerätetypen, Funktionen, Leistungsmerkmale, Mengengerüste usw. ermittelt, auf deren Basis die Beschaffung der ICT-Komponenten erfolgen kann.
- *ICT-Betriebsmodell:* Prozesse und Aktivitäten für Betrieb und Wartung der ICT-Komponenten werden beschrieben.

Ausschreibung für ICT-Komponenten
Die ICT-Fachplaner erstellen die notwendigen Ausschreibungsunterlagen für die Beschaffung und den Aufbau der ICT-Komponenten. Die Ausschreibungsunterlagen werden von der Swissgrid abgenommen.

Leitung von Aufbau und Inbetriebnahme der ICT-Komponenten
Die ICT-Fachplaner übernehmen die Leitung für den Aufbau der ICT-Komponenten bis zu deren Inbetriebnahme. Dies beinhaltet auch sämtliche baulichen Massnahmen, die als Voraussetzung für die ICT-Komponenten gelten, wie z.B. Racks, Kabelkanäle, Vorrichtungen für Gehäuse usw.. Die ICT-Fachplaner stellen durch geeignete Qualitätssicherungsmassnahmen sicher, dass die ICT-Konzepte beim Aufbau berücksichtigt werden. Der Aufbau der ICT-Komponenten wird durch die Inbetriebnahme der Swissgrid abgenommen.

8.2 ICT-Architektur

8.2.1 Grundlagen

Die ICT-Architektur orientiert sich am verabschiedeten Standard „Grundschutz für Unterwerke betreffend Cyber Security (GS-UW Cyber)“. Darin wird postuliert, dass im Unterwerk ein neues LAN für ICT-Komponenten physischer Schutz (SPHY – Substation Physical Security LAN) getrennt von den bestehenden LAN (SOLAN für Sekundärtechnik, SBLAN für Zähler) aufgebaut wird.

Das Swissgrid WAN (GCN Grid Control Network) agiert als hochverfügbare Kommunikationsschicht zwischen Unterwerken und den geo-redundanten Rechenzentren und stellt für alle benötigten Kommunikationswege verschlüsselte Verbindungen zur Verfügung.

ICT-Komponenten für den physischen Schutz in Unterwerken werden an das zentrale Überwachungssystem, das heute in den Rechenzentren von Swissgrid in Betrieb ist (Securiton Alarm Management System - AMS), angebunden.

Das Zutrittssystem, das in den Unterwerken aufgebaut wird, ist standardmässig mit dem zentralen Swissgrid-Zutrittssystem von KABA zu integrieren.

Im Projekt müssen die Anforderungen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit definiert werden. Aufgrund dieser Anforderungen wird die Kritikalität des neuen LANs festgelegt, woraus in der Folge das System-Layout (z.B. Hochverfügbarkeit, Hardware-Sharing, etc.) abgeleitet wird.

8.2.2 Architektur-Übersicht und Scope

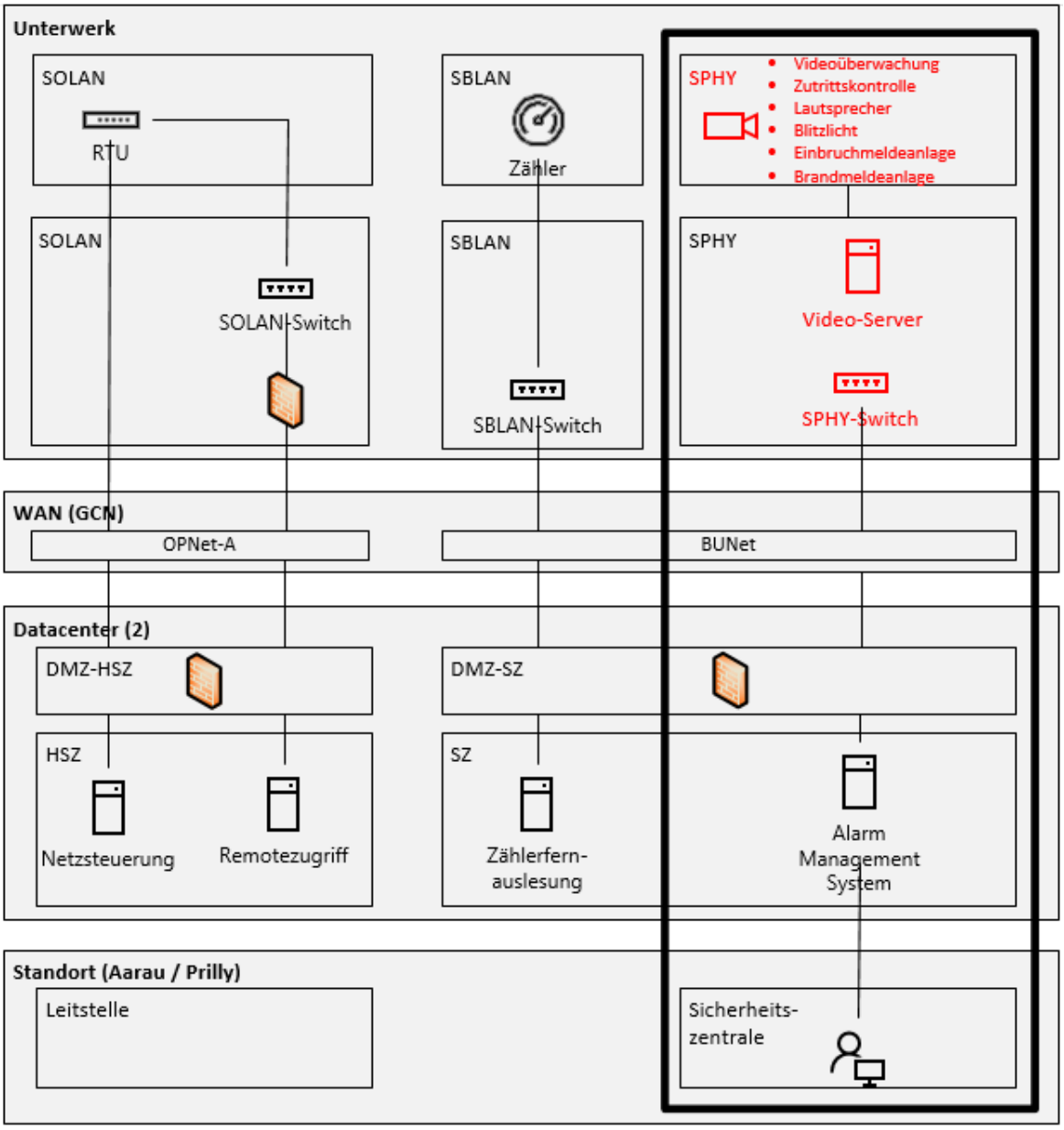


Abbildung 3: Schema Übersicht Architektur

Legende:

SOLAN	Substation Operations LAN
SBLAN	Substation Business LAN
SPHY	Substation Physical Security LAN
RTU	Remote Terminal Unit
LAN	Local Area Network
WAN	Wide Area Network
GCN	Grid Control Network
OPNet-A	Operations Network - A (WAN-Service)
BUNet	Business Network (WAN-Service)
DMZ	Demilitarized Zone
SZ	Secure Zone
HSZ	Highly Secure Zone

8.2.3 ICT-Prinzipien

Im Projekt werden folgende ICT-Prinzipien angestrebt:

- In den Unterwerken wird für SPHY eine minimal notwendige Infrastruktur aufgebaut, die einen überschneidungsfreien Betrieb mit anderen ICT-Installationen (SOLAN – Substation Operations LAN, SBLAN – Substation Business LAN) sicherstellt und einen möglichst tiefen Wartungsaufwand gewährleistet.
- Es ist anzustreben, dass für das WAN (GCN) und für das Rechenzentrum weder zusätzliche Infrastruktur noch erhöhte Komplexität resultiert.
- Aufbau und Betrieb von SPHY erfolgt nach einem einheitlichen Schema, das im Rahmen des Projektes ausgearbeitet wird. Das Schema kann Varianten enthalten, je nach den unterschiedlichen Gegebenheiten in Unterwerken. Ziel ist, dass ein Standard etabliert wird, der für sämtliche Unterwerke von Swissgrid angewendet werden kann.

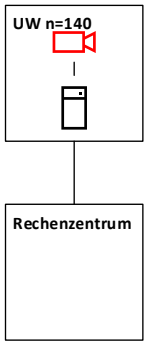
- Pro Gerätetyp (Kamera, Lautsprecher, Bewegungsmelder etc.) wird ein einheitliches Gerätemodell eingesetzt.

- Das SOLAN ist physisch isoliert und weist keine Verbindungen zum SBLAN und SPHY auf. Für den Fall, dass sich betriebliche Vorteile ergeben, können das SBLAN und das SPHY nur logisch segmentiert werden (VLAN – Virtual LAN).
- Wenn in Unterwerken Server-Komponenten benötigt werden (z.B. Mediaserver für Videostreaming), müssen diese in eigenständigen Racks aufgebaut werden.

8.2.4 Architektur-Optionen

Für die Anbindung der ICT-Komponenten für physische Sicherheit bestehen verschiedene Architektur-Optionen, die im Projekt unter der Federführung des GP untersucht werden. Dabei geht es insbesondere um die Frage, wo die Server-seitigen Komponenten der Security-Clients aufgebaut werden. Eine Server-Komponente ist beispielsweise ein Video-Server, der die Aufzeichnungen der Überwachungskameras vorhält.

Server-Komponenten in jedem Unterwerk



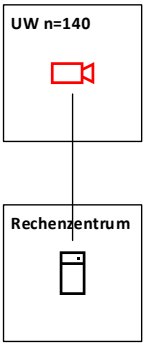
In jedem Unterwerk werden sämtliche Server-Komponenten aufgebaut.

Vorteile: Security-Clients können auch im Unterwerk gesteuert werden; durch lokales Caching von Video-Daten wird das WAN nur geringfügig zusätzlich belastet.

Nachteile: Es wird viel Infrastruktur im Unterwerk aufgebaut, die auch gewartet werden muss; Datenschutz-Problematik, weil Personendaten aus Videoaufzeichnungen im Unterwerk vorgehalten werden

Abbildung 4: Schema Komponenten in jedem UW

Unterwerk ohne Server-Komponenten



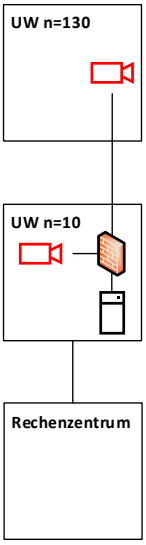
Im Unterwerk werden nur die Security-Clients aufgebaut. Sämtliche Server-Komponenten werden im Rechenzentrum aufgebaut. Sämtliche Signale werden direkt abgeführt und nicht lokal im Unterwerk vorgehalten.

Vorteile: Im Unterwerk muss nur eine minimale Infrastruktur aufgebaut werden; keine Datenhaltung im Unterwerk.

Nachteile: Enormes Datenaufkommen für das WAN und die Systeme im Rechenzentrum, das möglicherweise die Kapazitätsgrenzen übersteigt; keine lokale Steuerung von Security-Clients im Unterwerk.

Abbildung 5: Schema UW ohne Server-Komponenten

Server-Komponenten in Backbone-Unterwerken



In den meisten Unterwerken werden nur die Security-Clients aufgebaut. Die Server-Komponenten werden verteilt in wenigen Unterwerken (Backbone-UW) aufgebaut. Das WAN (GCN) besorgt das Routing der Signale vom Unterwerk in das Backbone-UW und vom Backbone-UW in das Rechenzentrum.

Vorteile: In den meisten Unterwerken muss nur eine minimale Infrastruktur aufgebaut werden. Die Netzauslastung wird durch den Aufbau der Knoten verteilt. Durch das lokale Caching in den Backbone-UW wird das Datenaufkommen beim Rechenzentrum geringer.

Nachteile: Das Routing im WAN (GCN) ist anspruchsvoll. Auch mit diesem Netzwerk-Layout ist nicht sichergestellt, dass die Kapazitätsgrenzen im WAN (GCN) nicht überschritten werden.

Abbildung 6: Schema Server-Komponenten in Backbone-UW

8.2.5 Anforderungen von Cyber Security

Die ICT-Komponenten für den physischen Schutz in Unterwerken unterliegen bestimmten Anforderungen bezüglich Cyber Security. Zur Gewährleistung einer sachgerechten Planung und Umsetzung der Anforderungen von Cyber Security ist eine entsprechend versierte Fachperson in die Konzipierung (Spezifikation), Planung und Realisierung miteinzubeziehen. Diese Anforderungen werden im Folgenden exemplarisch aufgeführt, damit sich der Generalplaner ein Bild machen kann, auf welchem Niveau die Cyber Security-Anforderungen umzusetzen sind:

- **NAC**: NAC (Network Access Control) wird in Unterwerken auf Basis von Zertifikaten eingesetzt (802.1x).
- **Remote Access**: Fernzugriff für Systems Mgmt erfolgt nur über dedizierte Systeme.
- **Security-Systeme**: Im SPHY sind keine zusätzlichen Systeme für IDS/IPS (Intrusion Detection Systems/Intrusion Prevention Systems) vorzusehen.
- **IP-Adressierung:** Swissgrid definiert einen Standard zur IP-Adressierung im Unterwerk.

- **Routing**: Erfolgt vom RZ über GCN auf einen dedizierten Switch im UW.

- **Physische Trennung der Netzwerke:** Die Netzwerke im Unterwerk sind dediziert nach Ihrer Funktion physisch getrennt.

- **Internet**: Die ICT-Komponenten im UW haben keine direkte Verbindung zum Internet.

- **Monitoring und Systems Management**: ICT-Komponenten für den physischen Schutz in Unterwerken werden zentral überwacht und gemanagt, wobei nur der Einsatz von sicheren Protokollen (z.B. SNMPv3) zugelassen ist.

- **Inventarisierung**: Im Unterwerk werden nur die von Swissgrid qualifizierten, freigegebenen und inventarisierten ICT-Komponenten installiert.

- **Zonenübergänge**: Swissgrid definiert die Übergänge von und in das Unterwerk sowie den Übergang zwischen den Netzwerk-Zonen.
- **Kryptographie und digitale Zertifikate**: Es werden, wo notwendig und sinnvoll, sicherheitstechnisch starke und sicher konfigurierte kryptographische Algorithmen, Verfahren und Mittel eingesetzt.

- **Malware-Schutz**: Technische Kontrollen zur Schadsoftware-Erkennung, Schadensbegrenzung und Wiederherstellung beschädigter Dateien und ICT-Systeme werden umgesetzt und gepflegt**.**

- **Patches und Updates:** Die Geräte/Systeme im Unterwerk werden zeitnah mit den vom Hersteller verfügbaren Patches und Updates nachgeführt.

- **Persönliche Accounts:** Der Zugriff auf Geräte/Systeme im Unterwerk der Swissgrid erfolgt - wo technisch möglich - mit persönlichen Accounts und Rollen, die dem Account gemäss Least Privilege-Prinzip zugewiesen sind.

- **Anbindung an Active Directory:** Alle ICT-Komponenten mit Ausnahme von Netzwerkelementen (Firewall und Switches) sind, soweit technisch möglich, an das Active Directory (AD) angebunden.

Backup-Management und Systemwiederherstellung: Zur schnellen Wiederherstellung von Daten und Services werden zyklische Sicherungen (Backups) erstellt.

Härtung von ICT-Komponenten
ICT-Komponenten für den physischen Schutz in Unterwerken werden nach technischer Möglichkeit gehärtet und sicher konfiguriert. Der IEEE Standard 1686 kann allgemein für die Härtung von ICT-Komponenten eingesetzt werden und beinhaltet folgende Massnahmen:

a) Standard-Accounts müssen deaktiviert oder gesperrt werden.

b) Die nicht benötigten Kommunikations-Ports, -protokolle, -verbindungen und -schnittstellen sowie Dienste und Anwendungen müssen deaktiviert, gesperrt oder entfernt werden. Beispielsweise Deaktivierung von USB-Ports, Webinterfaces, IPv6 und Modems.

c) Alle nicht benötigten Funktionen, die einen Ausbruch aus einem System, Dienst oder Anwendung ermöglichen, müssen entfernt, deaktiviert oder gesperrt werden.

d) Unnötige Benutzerkennungen (User-IDs) und -Zugänge/-Accounts müssen deaktiviert, gesperrt oder entfernt werden.

e) Die Berechtigungsvergabe an das Administrations-, Wartungs- und Supportpersonal muss restriktiv erfolgen (Least Privilege Prinzip).

f) Die systemeigenen Sicherheitsparameter müssen so konfiguriert werden, dass eine Erhöhung der Systemsicherheit erreicht wird (z.B. Aktivierung von Logging und Alarmierung).

g) Die Zugriffskontrolle muss technisch erzwungen werden:
   i. Die Administrations-Schnittstellen ohne Authentisierung (Stichwort: Autologin) müssen geschlossen/gesperrt sein
   ii. Die Sperrung der Administrations-Schnittstellen ohne Authentisierung muss technisch möglich sein.

h) Das automatische Sperren des Systems nach Benutzerinaktivität muss erzwungen werden.

i) Geräte mit kommerziellen Betriebssystemen müssen über ein Programm verfügen, welches nacherfolgreichem Integrationstest den Zustand des Systems einfriert. Besagtes Programm erlaubt nach dem Einfrieren keine unautorisierte Veränderung am System mehr. (Änderungen nur noch mit Admin-Account; Snapshot via Host-System nach Virtualisierung HMI– Human Machine Interface))

j) Anleitungen betreffend Härtung und sichere Konfiguration (sog. Hardening Guidelines) müssen vom Dienstleister/Lieferanten für jede ausgewählte ICT-Komponente definiert, dokumentiert und im Rahmen der bei Swissgrid etablierten Konfigurations-, Release- und Change Managementprozesse getestet und umgesetzt werden.

k) Anleitungen betreffend Härtung und sichere Konfiguration müssen jährlich durch Swissgrid auf Aktualität, Vollständigkeit und Wirksamkeit überprüft und bei Bedarf verstärkt, ausgetauscht oder ergänzt werden. Für jeden Gerätetyp müssen die umgesetzten Härtungsmassnahmen dokumentiert sein.

l) Eine vollständige Liste der installierten Firmware, Netzwerk-Komponenten, Software, und Applikationen inkl. Version (Build) muss jeder Lieferung einer ICT-Komponente durch den Dienstleister/Lieferanten beigelegt werden.

m) Die Hauptfunktionen (z.B. „Schutz“) eines Gerätes/Systems müssen immer gewährleistet werden, auch in Fällen, wo andere Funktionen des Gerätes/Systems gestört sind.

8.3 ICT-Betrieb

Aus Sicherheitsgründen will Swissgrid möglichst wenig verschiedenen Dienstleistern den Zutritt zu Unter-werken gewähren. Je nach Betriebsmodell soll der Betrieb von ICT-Komponenten in einen bestehenden Vertrag integriert werden. Im Betriebsmodell werden Störungsbehebung, Wartung und Austausch von ICT-Komponenten von einem Dienstleister durchgeführt. Dieser Dienstleister ist vertraut mit den Gegebenheiten im Unterwerken und entsprechend geschult.

ICT-Komponenten für den physischen Schutz in Unterwerken werden zentral von Swissgrid überwacht (Swissgrid Network Operations Center). Server-Komponenten in Unterwerken können remote administriert und gepatcht werden.

Im Projekt müssen die Anforderungen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit definiert wer-den. Über diese Anforderungen wird die Kritikalität des neuen LANs festgelegt, woraus in der Folge das System-Layout (z.B. Hochverfügbarkeit, Hardware-Sharing, etc.) abgeleitet wird.

9 Bauliche Anforderungen

9.1 Vorgaben zu Gebäude

9.1.1 Fassade/Dachhaut

Die Fassade/Dachhaut (insbesondere Öffnungen, wie Fenster und Türen) wird mittels geeigneter Massnahmen / Materialien (z. B. Fenstergitter, siehe auch Kap. 7.2.6) auf einem vorbestimmten Härtungsgrad gebracht. Dies soll das Eindringen von potentiellen Angreifern ins Gebäude erschweren.

Die Ausgestaltung und die Massnahmen sind pro Unterwerk mit Swissgrid abzustimmen.

9.1.2 Innenleben

Ist in einem Unterwerk der Schutz eines Racks oder Schaltschranks mit systemkritischen Elementen erforderlich, so sind nebst den geforderten technischen Sicherungsmassnahmen (siehe Kap.7 Physical Security) das Rack / der Schrank in einer massiven Bauweise einzukleiden (z.B. massive Stahlverkleidung, keine sichtbaren Schrauben, etc.).

Die Ausgestaltung und die Massnahmen sind pro Unterwerk mit Swissgrid abzustimmen.

9.1.3 Erdbebensicherheit (Statik) / baulicher Brandschutz

Die Gebäude sind auf Erdbebensicherheit/baulicher Brandschutz zu prüfen und gegebenenfalls zu ertüchtigen / den geltenden VKF Vorgaben anzupassen. Ersatzmassnahmen wie z.B Containerlösungen sind wenn nötig zu ergreifen.

Die Ausgestaltung und die Massnahmen sind pro Unterwerk mit Swissgrid abzustimmen.

9.1.4 Schadstoffe / Altlasten

Gebäudeschadstoffe
Hinweise auf mögliche Schadstoffvorkommen in Gebäuden gibt das interne Schadstoffkataster von Swissgrid. Bei weiterem Verdacht auf mögliche Schadstoffe sind zusätzliche Analysen (z.B. Schadstoffscreenings) durchzuführen.

Altlasten
Wo nötig sind die Unterwerksgebäude und evtl. Areale von Altlasten zu befreien.

10 BetriebsprozesseNutzungskonzept

Der GP erarbeitet mit der Unterstützung von Swissgrid im Projekt Use Cases, die insbesondere beschreiben, wie ICT-Komponenten für Sicherheit und Überwachung (Video, Voice, Bewegungsmelder, Zutritt usw.) eingesetzt und betrieben werden. Aus den Use Cases werden funktionale und nicht-funktionale Anforderungen abgeleitet, die die Basis bilden für das Layout der benötigten ICT-Komponenten. Darüber hinaus dienen Use Cases als Grundlage und Voraussetzung für das MSRL-Konzept. Die Dokumentation der Use Cases erfolgt in Anlehnung an den UML-Standard.

Use Cases dokumentieren systematisch und vollständig die Nutzung der ICT-Komponenten für Sicherheit und Überwachung, wie beispielsweise:

- wie das Unterwerk überwacht wird und von wem,
- von wo aus ICT-Komponenten gesteuert werden können (Sicherheitszentrale oder auch Unterwerk),
- wie eine Alarmierung zu erfolgen hat (Sicherheitszentrale, Leitstelle),
- wie lange Aufzeichnungen im Überwachungsfenster persistiert werden müssen,
- wer die ICT-Komponenten überwacht in Bezug auf Ausfall oder Sabotage etc.

10.1.1 MSRL-Konzept

Die Behandlung von Alarmen wird im Nutzungskonzept definiert. Der Generalplaner ist im Lead bei der Erstellung des MSRL-Konzepts. Die Swissgrid hat eine Beistellpflicht.

10.1.2 Alarm- und Informationsarten

Durch die neuen Sicherungssysteme werden verschiedene Arten von Informationen und Alarmen generiert. Dazu gehören (nicht abschliessend):

- Alarmmeldungen von den Detektionssystemen
- Alarmmeldungen von Zutrittsmedien
- EVAK
- Brandmelder
- Bewegungsmelder
- Etc.

Durch den Generalplaner ist eine Meldematrix (Alarmmatrix) mit den dazugehörigen Rollen und Verantwortung zu erstellen.

Die Informationen, Daten und Alarme sind in das bestehende Swissgrid-Datennetz zu integrieren und an eine zentrale Stelle zu liefern.

10.2 Zutrittsprozesse

Zutritte und deren nach- und vorgelagerten Prozesse werden an einer zentralen Stelle bei Swissgrid gesteuert und überwacht. Im Spezialfall des Unterwerks-Zutrittes gibt es eine enge operative Schnittstelle zwischen Sicherheitszentrale und Netzleitstelle.

Diese Prozesse sind während der Planung der Unterwerke zu definieren und im Rahmen der Umsetzung zu testen und gegebenenfalls zu optimieren und finalisieren.

Der Lead in diesem Thema liegt bei Swissgrid. Der Generalplaner wirkt unterstützend mit.

11 Natur und Landschaft Allgemein

Die Konzipierung (Spezifikation), Planung und Umsetzung der Schutzmassnahmen in den einzelnen Zonen hat unter Berücksichtigung und Einhaltung der geltenden Umweltschutzgesetzgebung zu erfolgen. In Ergänzung zu den in Kapitel 5 genannten rechtlichen Grundlagen sind hier folgende gesetzl. Vorgaben von besonderer Relevanz (nicht abschliessend):

- Bundesgesetz über den Umweltschutz (Umweltschutzgesetz, USG) vom 7. Oktober 1983 (Stand am 1. Januar 2018)
- Bundesgesetz über den Natur- und Heimatschutz (NHG) vom 1. Juli 1966 (Stand am 1. Januar 2017)
- Bundesgesetz über die Jagd und den Schutz wildlebender Säugetiere und Vögel (Jagdgesetz, JSG) vom 20. Juni 1986 (Stand am 1. Mai 2017)
- Tierschutzgesetz (TSchG) vom 16. Dezember 2005 (Stand am 1. Mai 2017)

Zur Gewährleistung einer ökologisch sachgerechten Planung und Bauabwicklung, insbesondere zur Berücksichtigung des vorsorgenden Biotop- und Artenschutzes, ist eine entsprechend ökologisch versierte Fachperson in die Konzipierung (Spezifikation), Planung und Realisierung (ökologische Baubegleitung) miteinzubeziehen.

Die Auswirkungen des Vorhabens auf die Umwelt sind in den jeweiligen Bewilligungsverfahren zu untersuchen und darzulegen. Der Beauftragte hat im Rahmen seiner Planung abzuklären, ob aufgrund früherer Plangenehmigungen Einschränkungen (z.B. Auflagen) bestehen, welche auf die aktuelle Planung einen Einfluss haben könnten. Allfällige Einschränkungen hat der Beauftragte von Anfang an in seiner Planung zu berücksichtigen.

11.2 Fauna

Im Sinne des Vorsorgeprinzips gemäss USG ist insbesondere darauf zu achten, dass die Fauna und ökologische Vernetzung im Perimeter und Areal sowie in den umgebenden Lebensräumen durch die Schutzmassnahmen keinen vermeidbaren Schaden oder eine vermeidbare Beeinträchtigung erleiden. Zu vermeiden sind insbesondere:

- Strukturen / Einrichtungen, welche Tiere gefährden können (Tierfallen wie z.B. scharfe Kanten, ungesicherte Bodenöffnungen, Verglasungen etc.)
- Strukturen / Einrichtungen, welche Lebensräume zerschneiden oder Wanderrouten blockieren (z.B. Gewährleistung Kleintierdurchgängigkeit des Zaunes)
- Strukturen / Einrichtungen, welche zu schädlichen Emissionen führen können (z.B. Lichtverschmutzung)

11.3 Flora

Im Sinne des Vorsorgeprinzips gemäss USG ist insbesondere darauf zu achten, dass:

- Eine Begrünung der Anlage (Areal und Gebäude inkl. Dach) und ein fachgerechter Unterhalt weiterhin möglich ist.
- Bei der Umsetzung der Schutzmassnahmen das Einbringen und Verschleppen invasiver, gebietsfremder Pflanzen (invasive Neophyten) verhindert wird.

11.4 Landschaft

Dem Orts- und Landschaftsbild ist Sorge zu tragen. Strukturen / Einrichtungen, welche das Landschaftsbild beeinträchtigen, sind auf ihre Zweck- und Verhältnismässigkeit zu beurteilen.

12 Glossar

BCM-Standort	Business Continuity Management Standort
CCTV-System	Closed circuit television system
GCN	Grid Control Network
GP	Generalplaner
ICT	Information and Communications Technology
LH	Lastenheft
MSRL	Mess-, Steuerungs- und Regelungstechnik
NDA	Non-disclosure agreement
PTZ-Kamera	Pan Tilt Zoom-Kamera (Schwenk-Neige-Zoom Kamera)
RZ	Rechenzentrum
SG	Swissgrid
SIA	Schweizer Ingenieur- und Architektenverein
SiZe	Sicherheitszentrale
SUVA	Schweizerische Versicherungsanstalt
SWKI	Schweizerische Verein von Gebäudetechnik-Ingenieuren
UW	Unterwerk
VKF	Vereinigung Kantonaler Feuerversicherungen