Mindestanforderungen an die Informationstechnik des Anbieters für die Erbringung von Abschaltleistung

Fassung vom 23.01.2017

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Vorwort

Die ÜNB haben aufgrund ihrer Systemverantwortung generell hohe Anforderungen an die Vertraulichkeit, die Verfügbarkeit und die Integrität ihrer Infrastrukturen sowie Informationen einzuhalten, welche sich auf alle angebundenen Infrastrukturen und Dienstleister übertragen. Die in diesem Dokument festgelegten Anforderungen für abschaltbare Lasten (AbLa) stellen Mindestanforderungen an die Sicherheit und Verfügbarkeit dar und berücksichtigen die gesetzlichen Vorgaben und Anforderungen des Bundesamtes für Sicherheit- und Informationstechnik.

2 Präambel

2.1 Zielsetzung

Das vorliegende Dokument beschreibt einen durch die deutschen ÜNB festgelegten Mindeststandard für die Anforderung an die IT der Anbieter zur Erbringung von Abschaltleistung aus abschaltbaren Lasten. Ziel ist, das Gesamtsystem im täglichen Betrieb angemessen gegen Sicherheitsbedrohungen zu schützen und eine hohe Verfügbarkeit der Abschaltleistung aufgrund der Bedeutung für die Systemsicherheit zu gewährleisten.

Im vorliegenden Dokument werden die technischen und organisatorischen Maßnahmen zur Erfüllung des festgelegten Mindeststandards definiert. Die konkrete Ausgestaltung der Schnittstelle erfolgt nach den Vorgaben des Anschluss-ÜNB. Die Einhaltung dieser Mindeststandards, z.B. durch Umsetzung der in den nachfolgenden Abbildungen dargestellten Technologien, entbindet den Anbieter nicht von seiner vertraglichen Verpflichtung zur vollständigen Vorhaltung und Erbringung von Abschaltleistung. Es liegt im Ermessen des Anbieters durch entsprechende Techniken bei der IT für Kommunikationstechnik und im Leitsystem die Verfügbarkeit zu steigern, um die Forderungen an die Verfügbarkeit der Abschaltleistung entsprechend dem Rahmenvertrag zu erfüllen.

Sofern sich durch gesetzliche Neuregelungen oder durch behördliche, regulatorische Vorgaben die Rahmenbedingungen für die IT ändern, oder wenn betriebliche oder sicherheitstechnische Erkenntnisse eine Änderung der vorliegenden „Mindestanforderungen an die Informationstechnik des Anbieters für die Erbringung von Abschaltleistung“ erfordern, sind die ÜNB einseitig zur Anpassung der „Mindestanforderungen an die Informationstechnik des Anbieters für die Erbringung von Abschaltleistung“ berechtigt. Entsprechend sind die Anbieter von Abschaltleistung verpflichtet, die neuen Anforderungen umzusetzen.
Die ÜNB behalten sich das Recht vor, die Einhaltung der technischen und organisatorischen Maßnahmen bei den Anbietern vor Ort zu auditieren oder durch Dritte auditieren zu lassen.

2.2 Geltungsbereich

Die vorliegenden Anforderungen sind Bestandteil der Präqualifikation für Anbieter die Abschaltleistung aus abschaltbaren Lasten vermarkten möchten. Diese Anforderungen sind auch im laufenden Betrieb einzuhalten.
Die für AbLa-Anbieter erforderliche Anbindung an den Lamas Server der dt. ÜNB sowie die Kommunikation mit der Ausschreibungsplattform regelleistung.net der dt. ÜNB wird von diesem Dokument nicht geregelt.

3 Sicherheitsanforderungen

Die deutschen ÜNB haben die Aufgabe, Abschaltleistung zu beschaffen. Aufgrund der Verpflichtung zur Sicherung eines sicheren, leistungsfähigen und zuverlässigen Betriebes von Energieversorgungsnetzen gemäß dem Energiewirtschaftsgesetz haben die ÜNBs hohe Anforderungen an die Sicherheit definiert. Diese sind bei der Vorhaltung und Erbringung von Abschaltleistung anzuwenden, um die Sicherheit des Gesamtsystems auf einem angemessenen Niveau zu gewährleisten. Die folgenden wesentlichen Schutzwerte sind hierbei zu beachten[1]:

- **Verfügbarkeit**
  Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Benutzern stets wie gewünscht zur Verfügung stehen.
- **Vertraulichkeit**
  Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.
- **Integrität**
  Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Der Begriff Integrität drückt aus, dass die Daten vollständig und unverändert sind.
- **Verbindlichkeit**
  Unter Verbindlichkeit werden die IT-Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.
- **Nachweisbarkeit**
  Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen der Nichtabstreitbarkeit der Herkunft (es soll einem Absender einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten) und der Nichtabstreitbarkeit des Erhalts (es soll einem Empfänger einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten).
- **Authentizität**
  Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

[1] Vgl. Definitionen des Bundesamtes für Sicherheit in der Informationstechnologie

3.1 Mindestanforderungen an die Informationstechnik für die Erbringung von Abschaltleistung

3.1.1 Überblick

Die folgende Abbildung 1 gibt einen exemplarischen und ganzheitlichen Überblick über die Anbindung der Anbieter an die ÜNB.

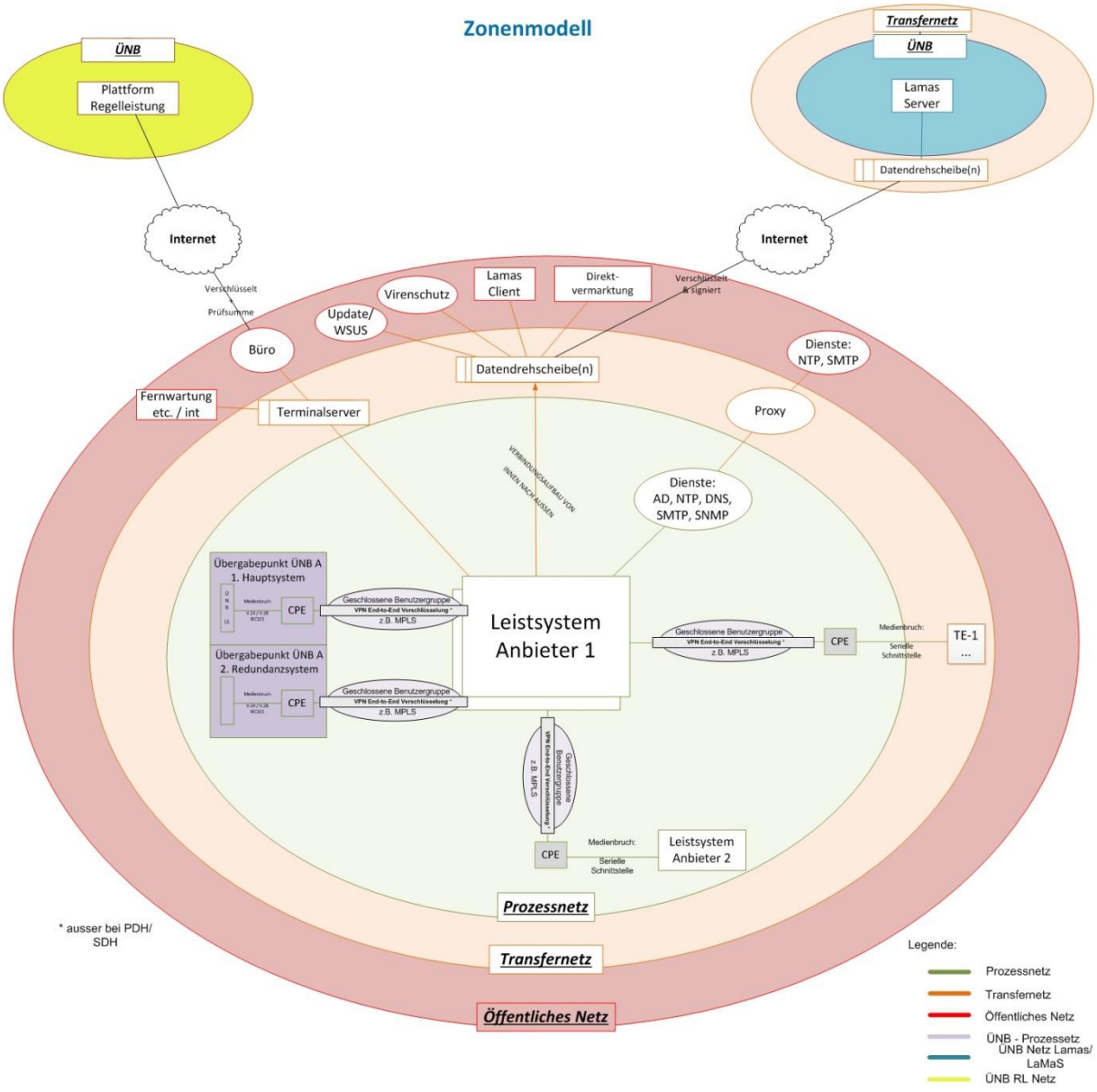

Abbildung 1: Exemplarischer und ganzheitlicher Überblick der Anbindung von einem AbLa-Anbieter an einen ÜNB

Hinweis: Abbildung 1 dient ausschließlich zur Veranschaulichung der IT-Anforderungen für Anbieter von Abschaltleistung. Die fachgerechte Konzeption und Umsetzung der IT-Anforderungen wird durch den Anbieter von Abschaltleistung verantwortet.

Die dargestellten Netzwerke unterscheiden sich durch die unterschiedlichen Schutzbedarfe:

- **Prozessnetz:**
  - Das Netzwerk um die Leitsysteme des Anbieters wird als Prozessnetz bezeichnet und stellt das Netzwerk mit dem höchsten Schutzbedarf im Bereich der Erbringung von Abschaltleistung dar.
- **Öffentliches Netz:**
  - Alle Netzwerke außerhalb des Prozessnetzwerks werden als öffentliche Netzwerke betrachtet und gelten als potentiell kompromittierbar. Eine sichere Verbindung zwischen einem Prozessnetzwerk und einem öffentlichen Netzwerk kann unter den in diesem Kapitel beschriebenen Voraussetzungen mittels Einsatz eines Transfernetzes als zulässig erachtet werden.
- **Transfernetz**:
  - Das Transfernetz dient der indirekten Verbindungsmöglichkeit zwischen dem Prozessnetz und unsicheren Netzwerken.
  - Der Datentransfer muss grundsätzlich aus dem Prozessnetz heraus gesteuert und über sog. Datendrehscheiben bzw. –schleusen erfolgen. Daten-Dateien (z.B. Vergabeergebnisse, Dispositionsdaten, Lamas-Abrufdaten aber auch Softwarepatches, Virenpattern etc.) können aus dem öffentlichen Netzwerk auf der Datendrehscheibe abgelegt und in einem zweiten Schritt in das Prozessnetz übertragen werden.
  - Jeglicher Datentransfer muss über angemessene Virenschutzmechanismen zusätzlich abgesichert werden.

3.1.2 Grundsätzliche Anforderungen

3.1.2.1 Anbieter Leitsystem

A01 | AbLa: X | Es wird empfohlen, das zentrale Leitsystem des Anbieters gedoppelt auszuführen. Diese Empfehlung gilt insbesondere bei Betrieb mehrerer abschaltbarer Lasten durch einen Anbieter innerhalb einer Regelzone. Eine Aufteilung in zwei Standorte hinsichtlich der Infrastruktur (Kommunikation und Stromversorgung) ist anzustreben. Der Anbieter hat eine angemessene Sicherheit seiner Leitsysteme zu gewährleisten.

A02 | AbLa: X | Der Betriebsstandort der eingesetzten Rechenzentren muss den Anforderungen des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (SÜG), der Verordnung zur Feststellung der Behörden des Bundes mit Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wie die der Nachrichtendienste des Bundes und zur Feststellung der öffentlichen Stellen des Bundes und der nichtöffentlichen Stellen mit lebens- oder verteidigungswichtigen

Einrichtungen (Sicherheitsüberprüfungsfeststellungsverordnung - SÜFV) und dem IT-Sicherheitsgesetz für Kritische Infrastrukturen (KRITIS) genügen.

A03 AbLa X Eine automatische Umschaltung zwischen redundanten zentralen Systemen des Anbieters hat innerhalb von einem festgelegten Zeitraum zu erfolgen.

Produkt	Maximale Umschaltzeit
Abschaltbare Lasten	15 Minuten

A04 AbLa X Die Verzögerung auf der kompletten Übertragungsstrecke E2E (von der Messwerterfassung der Abschaltbaren Last über das Anbieter-Leitsystem bis zum Eingang beim ÜNB) darf max. 10 Sekunden betragen. Generell wird ein Zeitstempel (links oder rechts gestempelt) benötigt.

3.1.2.2 ÜNB Leitsystem/Anbindung

Die folgende Abbildung 2 gibt einen exemplarischen Überblick, wie das Anbieter-Leitsystem an einen ÜNB angeschlossen werden kann.

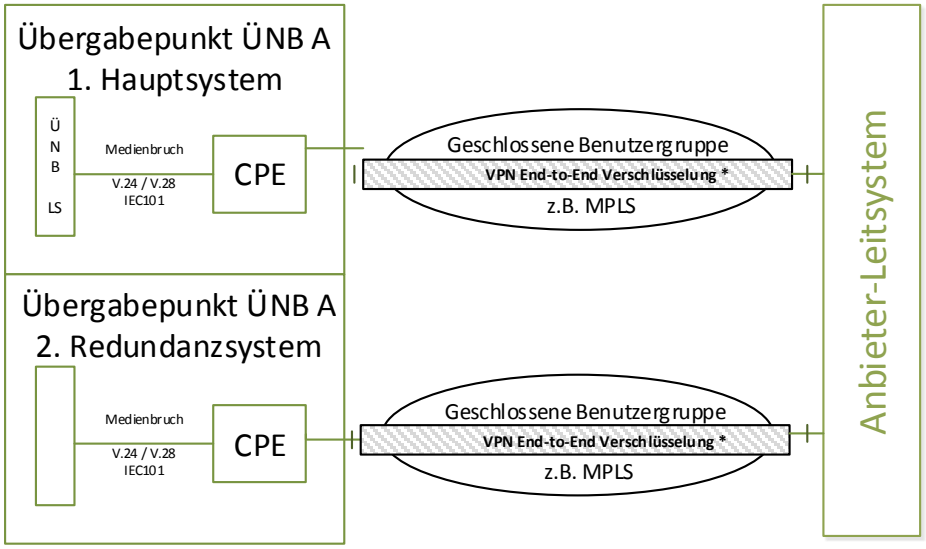

Abbildung 2: Exemplarischer Überblick der Anbindung von einem Anbieter-Leitsystem an einen ÜNB

Es gelten für die Anbindung des Leitsystems des Anbieters an den entsprechenden ÜNB die folgenden Anforderungen:

A05 AbLa X Die informationstechnische Verbindung ist in Form einer Punkt-zu-Punkt-Festnetzverbindung zu realisieren.

A06 AbLa X Bei der AbLa ist der Betrieb des Leitsystems mit einer örtlichen Redundanz anzustreben (siehe Glossar und Anlage „Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren“).

A07 AbLa X Die leittechnische Anbindung zur Erbringung von Abschaltleistung hat in Form einer dezidierten Punkt-zu-Punkt-Verbindung zwischen der Leitwarte des ÜNB und Leitsystemen des Anbieters zu erfolgen. Dies kann durch klassische Festnetzverbindungen oder in neuen Technologien realisiert werden. Zwischen den Leitsystemen sind Lösungen auf Basis des Mediums Internet ausgeschlossen. (Siehe auch Kapitel 3.1.2.3)

A08 AbLa X Es sind serielle Schnittstellen (V.24/V.28) mit Protokoll IEC 60870-5-101 (ÜNB spezifisch) zu verwenden. In Abstimmung mit dem ÜNB kann als Schnittstellenformat auch X.21 statt V.24 verwendet werden.

A09 AbLa X Die redundante Anbindung muss auf Anforderung des ÜNB zu unterschiedlichen Standorten realisiert werden (örtliche Redundanz).

A10 AbLa X Bezüglich der Nutzung von Internet-Technologien sind die grundsätzlichen Anforderungen in Kap. 3.1.2.3 zu berücksichtigen.

A11 AbLa X Die Übertragungsstrecken und Schnittstellen zu den beiden Übergabepunkten des ÜNB müssen vollständig redundant zueinander ausgelegt werden.

- knoten- und kantendisjunkt
- keine doppelt genutzten Geräte
- keine doppelt genutzten Kabelstrecken

A12 AbLa X Für die einzelne Verbindung zwischen den Leitsystemen der ÜNB und des Anbieters muss mindestens eine Verfügbarkeit von 98,5 % angestrebt werden. (Rechnerische Gesamtverfügbarkeit beider Verbindungen beträgt 99,9775 %.) Der Anbieter benennt die Verfügbarkeit je Übertragungsweg.

3.1.2.3 Geschlossene Benutzergruppe

B01 AbLa X In den Access-Netzen sind nur geschlossene Benutzergruppen zulässig. Die Kommunikation zwischen der abschaltbaren Last und Leitsystemen soll durch den Einsatz von geschlossenen Benutzergruppen stringent von anderen Netzwerken (z.B. Internet, Netzwerke anderer Kunden oder Dienstleister) abgeschirmt werden. Die geschlossene Benutzergruppe sollte ausschließlich private Adressen nutzen die von anderen Netzwerken nicht erreichbar sind. Die abschaltbare Lasten sollten untereinander nicht kommunizieren können sondern ausschließlich über den zentralen Gateway zum Leitsystem des Anbieters.

B02 AbLa X Die geschlossene Benutzergruppe dient ausschließlich zur Erbringung von Abschaltleistung. In Absprache mit dem Anschluss-ÜNB können auch weitere Daten, die im Zusammenhang mit der Erbringung von Systemdienstleistungen stehen, zugelassen werden. Alle anderen IT-Dienste sind zu deaktivieren. In einer geschlossenen Benutzergruppe dürfen sich nur die für die Vorhaltung und Erbringung von Abschaltleistung erforderlichen Teilnehmer befinden, wie z.B. Leitsystem des Anbieters oder präqualifizierte abschaltbare Lasten des Anbieters.
Innerhalb der geschlossenen Benutzergruppe dürfen insbesondere folgende Systeme nicht betrieben werden:

- Nachgelagerte IT-Systeme des TE-Betreibers
- Office-IT-Systeme des Anbieters oder Herstellers
- IT-Systeme anderer Anbieter (betrifft SaaS-Anbieter)

B03 AbLa X Die Nutzung von Internet-Technologien (z.B. IP, DSL, UMTS) ist nur bei Verwendung einer ausschließlich für diesen Zweck verwendeten und vom Telekommunikationsdienstleister bereitgestellten geschlossenen Benutzergruppe zulässig. Eine geschlossene Benutzergruppe des Telekommunikationsdienstleisters soll gewährleisten, dass der Netzwerkverkehr des Anbieters nicht mit "fremden" Netzwerken in Berührung kommt. Der Verkehr soll somit gegenüber anderen Netzwerken des Telekommunikationsdienstleisters, z.B. von anderen Kundennetzwerken oder gegenüber dem Internet abgesichert werden.

B04 AbLa X Innerhalb der geschlossenen Benutzergruppe muss durch den Anbieter eine eigene Ende zu Ende Verschlüsselung aufgebaut werden (nicht durch den Telekommunikationsdienstleister) und die Kommunikation zwischen den abschaltbaren Lasten und Leitsystemen zusätzlich gegenüber dem Netzwerk der geschlossenen Benutzergruppe absichern.

B05 AbLa X Die zwischen den Zugangsroutern übertragenen Daten müssen über einen verschlüsselten IPsec-VPN-Tunnel mit AES256 oder gleichwertigen Technologien geführt werden. Eine Empfehlung für eine sichere Verschlüsselung ist in der Anlage 2: Sicherheitsbetrachtung_VPN-Anbindung_RL beschrieben.

B06 AbLa X Konfigurationstechnisch bedingt dürfen von einem Anschluss, welcher sich in einer geschlossenen Benutzergruppe befindet, ausschließlich andere Anschlüsse innerhalb dieser Benutzergruppe erreicht werden. Eine direkte Verbindung zum Internet bzw. eine Erreichbarkeit von öffentlichen IP-Adressen im Internet oder anderer Benutzergruppen ist hierdurch ausgeschlossen. Diese Vorgabe umfasst auch Zugänge für externe Dienstleister und andere Standorte. Kommunikation via VPN oder über Site-to-Site Verbindungen, die nicht der geschlossenen Benutzergruppe angehören, ist nicht zulässig.

B07 AbLa X Die Konfiguration des Zugangsrouters hat so zu erfolgen, dass jeglicher Netzwerkverkehr in den VPN-Tunnel geroutet wird. Eine Kommunikation am Tunnel vorbei (außer zum Tunnel Aufbau) ist nicht zulässig (auch nicht zur Administration oder Monitoring).

B08 AbLa X Eine automatisierte, zyklische Überwachung der Router-Konfiguration mit integrierter Alarmierung (SMS, E-Mail) ist sicherzustellen. Durch eine tägliche bzw. mindestens wöchentliche Prüfung soll eine unerlaubte Manipulation der Router ausgeschlossen werden.

B09 AbLa X Für die Beantragung eines Anschlusses und einer geschlossenen Benutzergruppe beim Telekommunikationsdienstleister ist der Anbieter von Abschaltleistung verantwortlich. Der Vertrag hierfür ist zwischen Anbieter von Abschaltleistung und Telekommunikationsdienstleister zu schließen. Verträge bei denen sich der Internetprovider das Recht einräumt, die Verbindung kurzzeitig regelmäßig zu unterbrechen, z.B. nach 24 Stunden, sind auszuschließen.

B10 AbLa X Der Anbieter von Abschaltleistung ist verpflichtet nur solche Internetprovider auszuwählen, die den Anbieter von Abschaltleistung über geplante Wartungsarbeiten rechtzeitig vorab informieren. Unabhängig davon muss der Anbieter von Abschaltleistung für diesen Fall Vorkehrungen treffen, um seinen Verpflichtungen zur Vorhaltung und Erbringung von Abschaltleistung nachzukommen (z.B. durch redundante Verbindungen oder Aussetzen der Vermarktung).

B11 | AbLa X | Alle Übertragungsstrecken sind zu verschlüsseln. Von dieser Vorgabe nicht betroffen sind Punkt-zu-Punkt Verbindungen, die seriell ausgeführt wurden. Diese bedürfen keiner Verschlüsselung.

3.1.2.4 Anbindung der abschaltbaren Last, Medienbruch

Die folgende Abbildung 3 gibt einen exemplarischen Überblick über die Anbindung verschiedener abschaltbarer Lasten an das doppelt ausgeführte Leitsystem des Anbieters von Abschaltleistung.

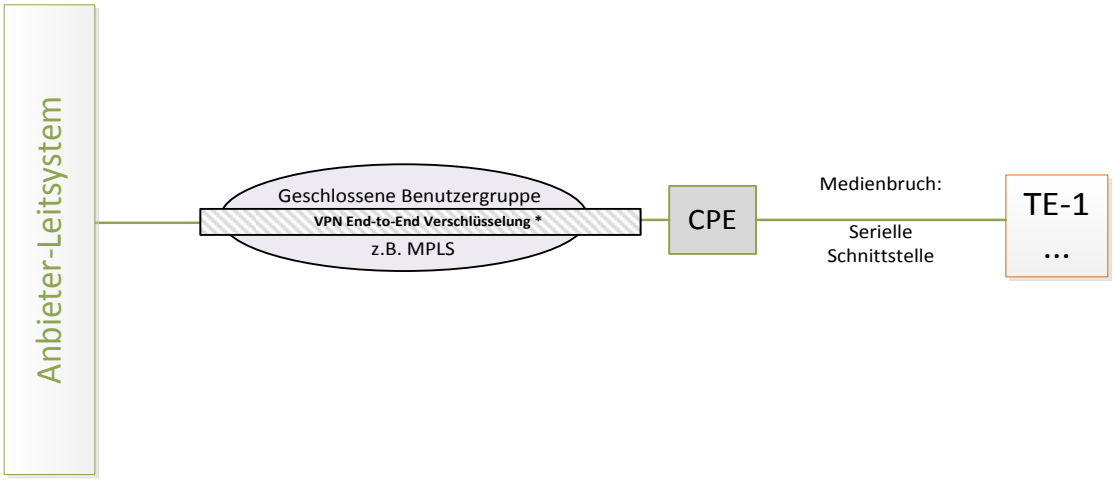

Abbildung 3: Exemplarischer Überblick der Anbindung von abschaltbaren Lasten an das Anbieter-Leitsystem

Es gelten für die Anbindung der abschaltbaren Lasten an das doppelt ausgeführte Leitsystem der Anbieter von Abschaltleistung die folgenden Anforderungen:

C01 | AbLa X | Jede abschaltbare Last muss mit einer Verfügbarkeit der Einzelverbindung von mindestens 95 % an das Leitsystem des Anbieters angebunden werden. (Nachweise können über Verträge, Systemseitig oder Statistiken erbracht werden).

C02 | AbLa X | Abschaltbare Lasten mit einer Leistung ≥ 30 MW sind zusätzlich redundant an das Anbieter-Leitsystem anzubinden.

C03 | AbLa X | Abschaltbare Lasten, die 50 MW oder mehr bereitstellen, sind weiterhin mit der bisherigen, redundanten Punkt-zu-Punkt-Festnetzverbindung (SDH/PDH) oder gleichwertigen Technologien anzubinden (siehe Definition Anlage 2, Kapitel 5 zur Anforderung für geschlossene Benutzergruppen zur Erbringung von Regelleistung).

C04 AbLa X Die abschaltbaren Lasten sind über eine serielle Schnittstelle anzubinden. Ein Medienbruch zum IP-Protokoll ist zwingend erforderlich. Alternativ ist auch eine direkte Steuerung von abschaltbaren Lasten über binäre oder analoge Ausgänge (z.B. Schalt-Aktoren) sowie eine direkte Erfassung von Messwerten mittels Binäreingängen oder AD-Wandler zulässig.

3.1.2.5 Weitere Anforderungen

D01 AbLa X Datentransfers aus und in andere Netzwerke mit abweichendem Schutzbedarf werden grundsätzlich mit Datendrehscheiben übertragen. Durch Datendrehscheiben wird gewährleistet, dass Daten zwischen dem Netz der abschaltbaren Lasten und den übrigen Netzen mit geringerem Schutzbedarf übertragen werden können, ohne dass es zu einer direkten Verbindung zwischen diesen Netzen kommt.

- Ausschließlich unidirektionale Kommunikation vom Leitsystem aus wird erlaubt, d.h. Daten sollen nur aus dem Netz des Leitsystems herausgeschrieben oder abgeholt werden können.
- Ausschließliche Nutzung von SFTP oder vergleichbaren, verschlüsselten Protokollen.
- Zweistufiger Virenschutz auf der Datendrehscheibe.

D02 AbLa X Störungen an Teilen des Gesamtsystems ohne Komplettausfall, d.h. ohne Beeinträchtigung der Vorhaltung und Erbringung, muss der Anbieter innerhalb von 24 Stunden nach Auftreten der Störung beseitigen. Sollte die Störung nicht an einem Werktag eintreten, so wird eine Fehlerbeseitigung am nächsten Werktag als ausreichend erachtet.

D03 AbLa X Der Anbieter von Abschaltleistung hat eine kontinuierliche und lückenlose Überwachung der Verfügbarkeit der Übertragungsstrecken einschließlich aller CPE zu gewährleisten.

D04 AbLa X Es ist ein angemessener Zutritts-, Zugangs- und Zugriffschutz zu Räumlichkeiten, Systemen und Netzwerken, die zur Erbringung der Abschaltleistung erforderlich sind, sicher zu stellen. (z.B. Zutritts- und Schlüsselkonzepte, Berechtigungsmanagement und physikalische Sicherheitsmaßnahmen in Verbindung mit einem angemessenen Anweisungswesen und Kontrollen). Elektrische Betriebsräume müssen abgeschlossen sein. Die Geräte des Anbieters von Abschaltleistung müssen zusätzlich in einem alarmgesicherten, verschlossenen Sicherheitsschrank untergebracht sein.

D05 AbLa X Der Anbieter von Abschaltleistung hat ein ganzheitliches Patch- und Changemanagement zu betreiben, dies im Rahmen der Präqualifikation nachzuweisen und die relevanten Prozesse zu dokumentieren. Updates werden unabhängig von der Art des zu aktualisierenden Systems (Betriebssystem, Anwendung, Anti Virus Signaturen, etc.) über das Prinzip der Datendrehscheibe übertragen (siehe D01). Dabei werden die Daten immer von den Servern abgeholt, die sich in der sichereren Zone befinden. Auf jedem der Systeme werden die Daten dabei überprüft (z.B. auf Schadsoftware, Standardkonformität und Plausibilität).

D06 AbLa X Alle Maßnahmen (technisches Konzept, Wegeführung, Entstörzeiten, Wartungsverträge etc.) zur Erreichung der geforderten Verfügbarkeit sind den ÜNB auf Anfrage darzustellen.

D07 AbLa X Im Falle von kompromittierten Technologien besteht seitens der Anbieter eine Meldepflicht gegenüber den ÜNB. Erlangt der ÜNB Kenntnis über eine kompromittierbare Technologie, so muss der Anbieter auf Anforderung die kompromittierbare Technologie nachbessern. Alternative Technologien müssen in einem solchen Fall innerhalb einer in Rücksprache mit den ÜNB abgestimmten Übergangsfrist umgesetzt werden.

3.1.2.6 Externe IT-Dienstleister

D08 AbLa X Anbieter von Abschaltleistung, die Leistungen von externen IT-Dienstleistern beziehen, die wiederum ihre Dienstleistungen mehreren Anbietern von Abschaltleistung und Regelleistung anbieten (z.B. Software as a Service Anbieter), bedürfen besonderer Regelungen:

- Der Bezug von Leistungen von o.g. IT-Dienstleistern muss ausdrücklich im Rahmen der Präqualifikation bekannt gegeben und durch die ÜNB freigegeben werden.
- Anbieter von Abschaltleistung die solche Leistungen beziehen, werden grundsätzlich behandelt wie Anbieter mit höchstem erforderlichen Schutzbedarf (wie Abschaltleistung ≥ 50MW).
- IT-Dienstleister, die für verschiedene Anbieter von Abschaltleistung Dienstleistungen erbringen und deren assoziierte Anbieter müssen gewährleisten, dass durch den Betrieb von gemeinsam genutzten Komponenten keine Risiken auf andere Anbieter von Abschaltleistung und Regelleistung ausstrahlen können. Z.B. darf pro geschlossene Benutzergruppe nur ein Anbieter angebunden werden.

- Der Anbieter von Abschaltleistung ist Hauptansprechpartner für den ÜNB und trägt die Gesamtverantwortung für die Erfüllung der IT Anforderungen.

3.2 Informationspflichten und Nachweise

Der Anbieter von Abschaltleistung hat die Security seines Gesamtsystems E2E (bidirektionaler Datenaustausch zwischen der abschaltbaren Last zum ÜNB über das Anbieter-Leitsystem) entsprechend Kapitel 3.3 nachzuweisen. Folgende Anforderungen sind zu gewährleisten:

- Technische Vertragsinhalte zur IT-Sicherheit und Verfügbarkeit hat der Anbieter von Abschaltleistung gegenüber dem ÜNB oder einem beauftragten Dritten auf Anfrage nachzuweisen (dieses kann beispielsweise in Form einer Einsichtnahme der entsprechenden Textpassagen bei vorhandenen Verträgen erfolgen).
- Vorhandene Risiko- oder Grundschutzanalyse hat der Anbieter von Abschaltleistung den ÜNB auf Anfrage nachzuweisen.
- Die Konzeption und Umsetzung von IT-Sicherheitsmaßnahmen hat der Anbieter von Abschaltleistung den ÜNB auf Anfrage nachzuweisen (ggf. auch vor Ort). Sicherheitstechnisch relevante Änderungen und Sicherheitsvorfälle im Gesamtsystem muss der Anbieter von Abschaltleistung dem ÜNB unverzüglich mitteilen.
    - Sicherheitstechnisch relevante Änderungen könnten sein: Änderungen an der Konfiguration des VPN-Tunnels, Modellwechsel der Router-Hardware, konzeptionelle Änderungen, etc.
    - Sicherheitsvorfälle sind u.a.: Bekanntwerden von Schwachstellen in der Routerkonfiguration oder Router-Firmware, unberechtigte Zugriffe Dritter, Angriffe auf den Zugangsrouter oder dahinterliegender Systeme, etc.
- Wenn die Datenbereitstellung zum ÜNB nicht ordnungsgemäß gewährleistet werden kann, muss der Anbieter von Abschaltleistung den ÜNB hierrüber unverzüglich informieren.
- Die Anbieter von Abschaltleistung haben die folgenden Informationen zur Prüfung der Zuverlässigkeit zu erfassen und insbesondere im Fehlerfall oder auf Anfrage an den ÜNB zu berichten:
    - Häufigkeit und Dauer der Störungen
    - Ursachen der Störungen
    - Umschaltzeit auf Redundanz-Verbindung
    - Zeit bis zur Behebung der Störungen
    - Getroffene Maßnahmen zur Störungseingrenzung und Behebung
    - Maßnahmen zur zukünftigen Vermeidung des Fehlers
- Änderungen der IT Anforderungen auf der Internetplattform Regelleistung werden seitens der ÜNB gegenüber den Anbietern entsprechend kommuniziert.

- Im Bedarfsfall müssen die Konzepte seitens der Anbieter von Abschaltleistung in Abstimmung mit den ÜNB entsprechend angepasst werden.
- Änderungen an den IT-Konzepten müssen dem Anschluss-ÜNB vor Beginn einer Umsetzung zur Prüfung vorgelegt werden.
- Um eine regelmäßige Anpassung der IT-Anforderungen zu unterstützen wird der Anbieter aufgefordert, jeweils zum 31.01. für das Vorjahr, einen Jahresbericht zum Betrieb der AbLa-IT Systeme dem jeweiligen Anschluss-ÜNB vorzulegen (Siehe Anlage „RL-IT Anbieter Jahresbericht).

3.3 Selbstauskunft und Nachweise

Der Anbieter bestätigt im Rahmen einer Selbstauskunft (siehe unten) und Nachweise (siehe Kap. 3.2), dass die vorliegenden Mindestanforderungen an die IT-Kommunikationstechnik des Anbieters für die Erbringung von Abschaltleistung eingehalten werden. Die Selbstauskunft ist durch den Geschäftsführer bzw. eine autorisierte Vertretung des Anbieters von Abschaltleistung zu unterzeichnen.

Im Rahmen der Präqualifikation müssen folgende Dokumente seitens des Anbieters von Abschaltleistung zur Prüfung der IT Anforderungen vorgelegt werden:

- Vorlage eines aussagekräftigen IT-Konzepts
- AbLa-IT Checkliste mit Zuordnung der entsprechenden Kapitel des IT-Konzepts einschließlich der Beschreibung der Verschlüsselungstechnik- (siehe Anlage AbLa-IT-Checkliste.xlsx)

Anlagen (siehe Plattform Regelleistung.net):

1. Checkliste AbLa-IT-Anforderungen (20170123_RL-IT_Checkliste.xlsx)
2. Anforderung für geschlossene Benutzergruppen (Sicherheitsbetrachtung_VPN-Anbindung_RL.pdf)
3. Bericht über die Informationstechnik des Anbieters und Vorfälle bei der Erbringung von Regelleistung (20160420_RL-IT_Jahresbericht.xlsx)
4. Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren (Siehe Webseite des Bundesamt für Sicherheit und Informationstechnik)

Abkürzungsverzeichnis und Glossar

Begriff/Abkürzung/Satzteil	Klärung
AbLa	Abschaltbare Last
ADSL	Asymmetric Digital Subscriber Line
CPE	Customer Premises Equipment sind Geräte des Anbieters von Regelleistung als Netzabschluss- und Übergabeschnittstelle
DSL	Digital Subscriber Line
E2E (End to End)	Übertragungsweg von der Messwerterfassung der Technischen Einheit über das Anbieter-Leitsystem bis zum Eingang beim ÜNB) Übertragungsweg, welcher zwischen den Übergabe-Schnittstellen der CPE in Richtung der ÜNB einerseits, und in Richtung der TE andererseits, konfiguriert wird
Geschlossene Benutzergruppe im Access Netz	Von einem Telekommunikationsdienstleister bereitgestellte Anschlüsse, welche von diesem in einem geschlossenen Verbund betrieben werden. Dieses können Anschlüsse in unterschiedlichen Übertragungsnetzen wie DSL/UMTS/GSM/etc. sein. Eine Kommunikation mit Anschlüssen außerhalb dieser geschlossenen Benutzergruppe, z.B. in Richtung Internet, muss ausgeschlossen sein. Zur Einrichtung dieser geschlossenen Benutzergruppen muss meist ein Vertrag mit dem jeweiligen Telekommunikationsdienstleister geschlossen werden.
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
HSL	Hauptschaltleitung
HSPA	High Speed Packet Access
IP	Internet protocol
ISDN	Integrated Services Digital Network
LFR	Leistungs-Frequenz-Regler: Regelsystem zur Einhaltung der zwischen den Übertragungsnetzbetreibern (ÜNB) vereinbarten elektrischen Größen.
LTE	Long Term Evolution
LWL	Lichtwellenleiter
MPLS	Multiprotocol Label Switching (Paketvermittelndes Übertragungsverfahren)

PDH	Plesiochrone Digitale Hierarchie

Redundanz, allgemeine	• Redundanz definiert sich wie folgt:
	  ○ knoten- und kantendisjunkt
	  ○ keine doppelt genutzten Geräte
	  ○ keine doppelt genutzten Kabelstrecken

Redundanz, örtliche	• Mindestens zwei Standorte mit jeweils vom anderen Standort unabhängigen:
	  ○ Energieversorgungen
	  ○ Kommunikationsverbindungen
	• Die Störung eines Standortes darf den anderen Standort nicht in Mitleidenschaft ziehen
	• Siehe auch Hinweise zur Entfernung von Rechenzentren in Anlage BSI_RZ_Abstand.pdf

SaaS-Anbieter	Software as a Service Anbieter
SDH	Synchrone Digitale Hierarchie (Leitungsvermittelndes Übertragungsverfahren)
SDSL	Symmetric Digital Subscriber Line
TE	Technische Einheit
UMTS	Universal Mobile Telecommunication System
ÜNB	Übertragungsnetzbetreiber
VPN	Verbindung zwischen zwei "privaten" Netzwerksegmenten, welche über ein von dritten betriebenes Netzwerk geführt wird. Alle in diesem Dokument erwähnten VPNs setzen die Verschlüsselung des VPN mit dem IPsec-Protokoll und der Verwendung von AES256/SHA1 voraus.
Gesamtsystem	Alle zur Leistungserbringung/Vertragserfüllung notwendigen Komponenten
Changemanagement	Prozess zur Autorisierung und Dokumentation von Änderungen an der IT-Infrastruktur und Applikationen, um ungewollte Auswirkungen auf den laufenden Betrieb so gering wie möglich zu halten.
Patchmanagement	Bereich des Systemmanagements zur Beschaffung, Testen und Installation von Patches.

Selbstauskunft zu den „Mindestanforderungen an die Informationstechnik des Anbieters für die Erbringung von Abschaltleistung“

_____ (Name des AbLa-Anbieters) als Anbieter für Abschaltleistung aus abschaltbaren Lasten erklärt hiermit, dass er die von den deutschen Übertragungsnetzbetreibern (ÜNB) erstellten „Mindestanforderungen an die Informationstechnik für die Erbringung von Abschaltleistung“ vom 19.01.2017 in der jeweils geltenden Fassung während der Laufzeit des AbLa-Rahmenvertrages erfüllt.

Name und Anschrift des AbLa-Anbieters:

Ort und Datum: ……..

Unterschrift (Geschäftsführer oder autorisierte Vertretung): ……..