Mindestanforderungen an die Informationstechnik des Reservenanbieters zur Erbringung von Regelreserve

Stand: 20.12.2019

Versionsverlauf

Version	Datum	Bemerkung
1.0	22.04.2016	Erste gültige Version (konsolidierte Fassung für alle RL-Produkte)
1.1	19.01.2017	Einführung der alternativen Anbindung zu SDH/PDH
1.2	05.09.2017	Präzisierung zur Zertifizierungspflicht nach BSI-KritisV
2.0	26.10.2018	Überarbeitung im Rahmen der Neuerstellung der PQ-Bedingungen
2.1	20.12.2019	Anpassung zu A02 und B02 sowie Kapitel 4.6 (Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren) Erweiterung um Konzeption von Reserveeinheit/Reservegruppe (TE) zur Bündelung von Kleinstanlagen in C05 Klassifizierung der Informationssicherheit des Dokumentes durch die Anbieter in Kapitel 3.3

Inhalt

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 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 Reservenanbieter zur Erbringung von Regelreserve. Ziel ist, das Gesamtsystem im täglichen Betrieb angemessen gegen Sicherheitsbedrohungen zu schützen und eine hohe Verfügbarkeit der Regelreserve 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 zur Anbindung des Reservenanbieters an die Systeme des ÜNB erfolgt nach den Vorgaben des Reserven anschließenden ÜNB. Die Einhaltung dieser Mindeststandards, z.B. durch Umsetzung der in den nachfolgenden Abbildungen dargestellten Technologien, entbindet den Reservenanbieter nicht von seiner vertraglichen Verpflichtung zur vollständigen Vorhaltung und Erbringung von Regelreserve. Es liegt im Ermessen des Reservenanbieters, durch geeigneten IT-Einsatz die Verfügbarkeit der Kommunikationstechnik und des Leitsystems zu steigern, um die Forderungen nach einer hundertprozentigen Verfügbarkeit der Erbringung von Regelreserve entsprechend den jeweiligen Rahmenverträgen 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 Reservenanbieters für die Erbringung von Regelreserve“ erfordern, sind die ÜNB einseitig zur Anpassung der „Mindestanforderungen an die Informationstechnik des Reservenanbieters für die Erbringung von Regelreserve“ berechtigt. Entsprechend sind die Reservenanbieter verpflichtet, die neuen Anforderungen umzusetzen.

Die ÜNB behalten sich das Recht vor, die Einhaltung der technischen und organisatorischen Maßnahmen bei den Reservenanbietern vor Ort zu auditieren oder durch Dritte auditieren zu lassen.

2.2 Geltungsbereich

Die vorliegenden Anforderungen sind Bestandteil der Präqualifikation für Reservenanbieter, die Regelreserve vermarkten möchten. Diese Anforderungen sind auch im laufenden Betrieb einzuhalten.

Die für mFRR erforderliche Anbindung an den Merit Order List Server (MOLS) der dt. ÜNB sowie die Kommunikation mit der Ausschreibungsplattform regelleistung.net der dt. ÜNB werden von diesem Dokument nicht geregelt.

3 Sicherheitsanforderungen

Die deutschen ÜNB haben die Aufgabe, Regelreserve zu beschaffen und einzusetzen, um Leistungsschwankungen im Netz gezielt entgegen zu wirken.

Aufgrund der Verpflichtung zum sicheren, leistungsfähigen und zuverlässigen Betrieb von Energieversorgungsnetzen gemäß dem Energiewirtschaftsgesetz haben die ÜNBs hohe Anforderungen an die Sicherheit definiert. Diese sind bei der Vorhaltung und Erbringung von Regelreserve anzuwenden, um die Sicherheit des Gesamtsystems auf einem angemessenen Niveau zu gewährleisten. Die folgenden zu schützenden, wesentlichen Grundwerte und generischen Oberbegriffe der Informationssicherheit 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.
- **Authentizität**
  Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass

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

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.

- **Nichtabstreitbarkeit**

  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).

3.1 Mindestanforderungen an die Informationstechnik des Reservenanbieters für die Erbringung von Regelreserve

3.1.1 Überblick

Die folgende Abbildung 1 gibt einen exemplarischen und ganzheitlichen Überblick über die Anbindung des Reservenanbieters an den Reserven anschließenden ÜNB.

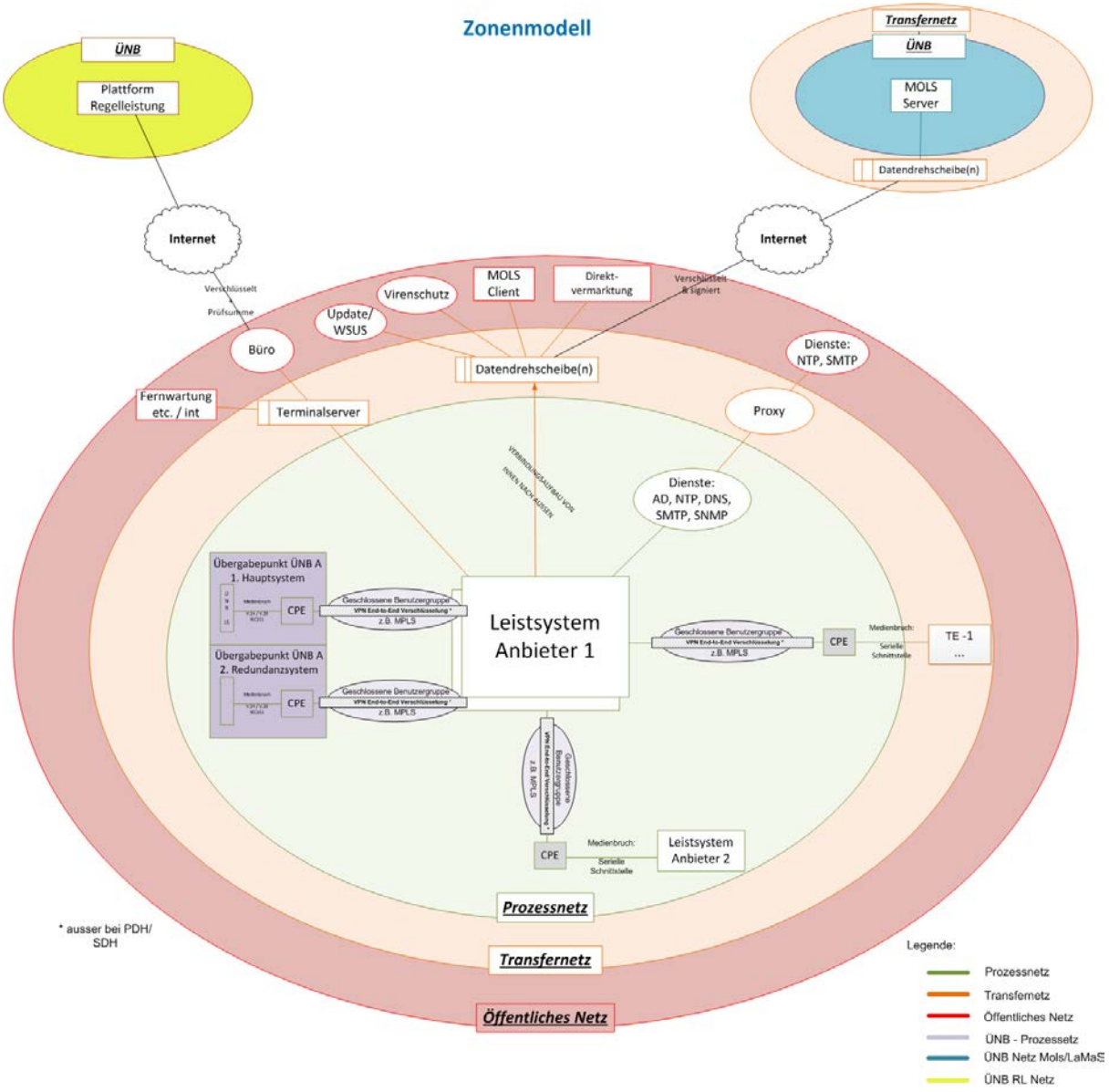

Abbildung 1: Exemplarischer und ganzheitlicher Überblick der Anbindung von einem Reservenanbieter an einen ÜNB

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

Die dargestellten Netzwerke unterscheiden sich durch die unterschiedlichen Schutzbedarfe:

- Prozessnetz:
  - Das Netzwerk um die Leitsysteme des Reservenanbieters wird als Prozessnetz bezeichnet und stellt das Netzwerk mit dem höchsten Schutzbedarf im Bereich der Erbringung von Regelreserve 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. Dateien (z.B. Vergabeergebnisse, Dispositionsdaten, MOLS-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

Für alle in dem vorliegenden Dokument beschriebenen Anforderungen gilt Folgendes: Falls ein Reservenanbieter mehr als einen Pool für die Vorhaltung und Erbringung derselben Regelenergieart betreibt und die Pools nicht vollkommen separat voneinander betrieben werden (bspw. jeweils separate Leitsysteme etc), so werden hinsichtlich der IT-Mindestanforderungen die Leistungen der Pools zusammengefasst, so dass entsprechende

Schwellenwerte auf die gesamte für die betreffende Regelenergieart in den Pools vorgehaltene Leistung angewendet werden. Hierbei ist unerheblich, über wie viele und welche LFR-Zonen die entsprechenden Pools ggf. verteilt sind. Die geographische Verteilung der an das zentrale Leitsystem des Reservenanbieters angebundenen Pools ist im IT-Konzept zu beschreiben. Andere, nicht von den ÜNB selbst festgelegte Leistungsgrenzen (wie bspw. die Schwellenwerte gemäß BSI-KritisV) sind von dieser Regelung nicht berührt.

3.1.2.1 Reservenanbieter Leitsystem

A01 | FCR | aFRR | mFRR
X | X | ≥ 50 MW

Das zentrale Leitsystem des Reservenanbieters ist gedoppelt auszuführen. Eine Aufteilung in zwei redundante Standorte hinsichtlich der Infrastruktur (Kommunikation und Stromversorgung) ist anzustreben. Der Reservenanbieter hat eine angemessene Sicherheit seiner Leitsysteme für Regelreserve zu gewährleisten. Diese Anforderung gilt grundsätzlich für aFRR, FCR und auch für mFRR bei einer vermarktbaren Leistung ab 50 MW.

A02 | FCR | aFRR | mFRR
X | X | X

Der Betriebsstandort der eingesetzten Rechenzentren einschließlich der eingesetzten Mitarbeiter muss den gesetzlichen Anforderungen und den anerkannten Regeln der Technik genügen.

A03 | FCR | aFRR | mFRR
X | X | ≥ 50 MW

Eine automatische Umschaltung zwischen den redundanten zentralen Leitsystemen des Reservenanbieters hat innerhalb eines festgelegten Zeitraums zu erfolgen.

Produkt	Maximale Umschaltzeit
aFRR	20 Sekunden
FCR	15 Minuten
mFRR (≥ 50MW pro LFR-Zone)	15 Minuten

A04 | FCR | aFRR | mFRR
X | X | X

Die Verzögerung auf der kompletten Übertragungsstrecke E2E (von der Messwerterfassung der Technischen Einheit über das Reservenanbieter-Leitsystem bis zum Eingang beim ÜNB) darf

max. 5 Sekunden betragen. Generell wird ein Zeitstempel (links oder rechts gestempelt) benötigt.
Die Anforderung gilt bei aFRR. Bei FCR und mFRR sind vergleichbare Zeiten anzustreben. Der Reservenanbieter benennt die maximale Verzögerungszeit.

3.1.2.2 ÜNB Leitsystem/Anbindung

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

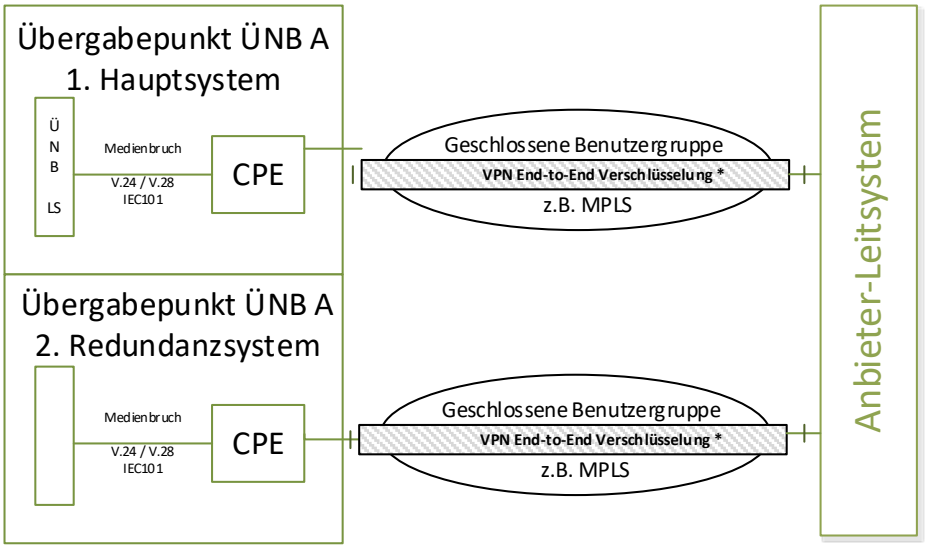

Abbildung 2: Exemplarischer Überblick der Anbindung von einem Reservenanbieter-Leitsystem an einen ÜNB

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

A05	FCR aFRR mFRR ≥ 50 MW	Reservenanbieter, deren vermarktete aFRR innerhalb einer LFR-Zone 50 MW oder mehr beträgt, müssen die Verbindung zwischen dem ÜNB und dem Leitsystem des Reservenanbieters weiterhin mit der bisherigen Punkt-zu-Punkt-Festnetzverbindung (SDH/PDH) oder gleichwertigen Technologien realisieren (siehe Definition Anlage 2, Kapitel 5 zur Anforderung für geschlossene Benutzergruppen zur Erbringung von Regelreserve). Diese

				Anforderung gilt auch für Reservenanbieter, die in der Zukunft eine Vermarktung von 50 MW oder mehr aFRR anstreben.
A06	FCR ≥ 90 MW	aFRR ≥ 50 MW	mFRR	Reservenanbieter, deren vermarktete RL 50 MW oder mehr beträgt, müssen das Leitsystem mit einer örtlichen Redundanz betreiben (siehe Glossar und Anlage „Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren“). Reservenanbieter, die eine vermarktbare Leistung von 50 MW oder mehr pro LFR-Zone anstreben, sollten berücksichtigen, dass die Umsetzung dieser Anforderung eine Voraussetzung für die Vermarktung der erhöhten Leistung (≥ 50 MW) ist. Die Anforderung gilt bei aFRR. Bei FCR und mFRR wäre eine örtliche Redundanz anzustreben. Sofern das zentrale Leitsystem für eine vertragsgemäße Erbringung der FCR (z.B. für das Batteriemanagement) erforderlich ist, ist das Leitsystem ab einer vermarktbaren Leistung ≥ 90 MW örtlich redundant auszuführen.
A07	FCR X	aFRR X	mFRR ≥ 50 MW	Die leittechnische Anbindung zur Erbringung von Regelreserve hat in Form einer dezidierten Punkt-zu-Punkt-Verbindung zwischen der Leitwarte des ÜNB und dem Leitsystem des Reservenanbieters zu erfolgen. Dies kann durch klassische Festnetzverbindungen oder in neuen Technologien realisiert werden. Zwischen den Leitsystemen sind Lösungen auf Basis des Mediums Internet ausgeschlossen. Diese Anforderung gilt ab 50 MW vermarktbarer Regelreserve auch für mFRR (siehe auch Kapitel 3.1.2.3).
A08	FCR X	aFRR X	mFRR 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.

	FCR	aFRR	mFRR	
A09	X	X	X	Betreibt der Reservenanbieter Leitsysteme mit örtlicher Redundanz, so sind diese auf Anforderung des ÜNB redundant an das Leitsystem des ÜNB anzubinden (ggf. mit zusätzlicher Redundanz zu den beiden Übergabepunkten des ÜNB (s. A11)).
A10	X	X	X	Bezüglich der Nutzung von Internet-Technologien (nicht zu verwechseln mit der unter A07 ausgeschlossenen Nutzung des öffentlichen Internets) sind die grundsätzlichen Anforderungen in Kapitel 3.1.2.3 zu berücksichtigen.
A11		X		Die Übertragungsstrecken und Schnittstellen zu den beiden Übergabepunkten des ÜNB müssen vollständig redundant zueinander ausgelegt werden: • knoten- und kantendisjunkt, • keine doppelt genutzten Geräte und • keine doppelt genutzten Kabelstrecken.
A12	X	X	X	Die einzelne Verbindung zwischen den Leitsystemen des ÜNB und des Reservenanbieters muss mindestens eine Verfügbarkeit von 98,5 % aufweisen (rechnerische Gesamtverfügbarkeit beider Verbindungen beträgt 99,9775 %). Die Anforderung gilt bei aFRR. Bei der FCR und mFRR sind vergleichbare Verfügbarkeiten anzustreben. Der Reservenanbieter benennt die Verfügbarkeit je Übertragungsweg.

3.1.2.3 Geschlossene Benutzergruppe

	FCR	aFRR	mFRR	
B01	X	X	X	In den Zugangsnetzen zum Teilnehmeranschluss sind nur geschlossene Benutzergruppen zulässig. Die Kommunikation zwischen den TE 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 TE sollten untereinander nicht kommunizieren können, sondern ausschließlich über das zentrale Gateway zum Leitsystem des Reservenanbieters.

	FCR	aFRR	mFRR
B02	X	X	X

Die geschlossene Benutzergruppe dient ausschließlich zur Erbringung von Regelreserve. In Absprache mit dem Reserven anschließenden ÜNB können auch weitere Daten, die im Zusammenhang mit der Erbringung von Systemdienstleistungen stehen, zugelassen werden (z.B. für folgende Dienste: SNMP zur Überwachung der angeschlossenen Geräte, zentrale Zeitsynchronisation, Konfigurationsupdates). Alle anderen IT-Dienste sind zu deaktivieren. In einer geschlossenen Benutzergruppe dürfen sich nur die für die Vorhaltung und Erbringung von Regelreserve erforderlichen Teilnehmer befinden, wie z.B. Leitsystem des Reservenanbieters oder präqualifizierte TE des Reservenanbieters.
Innerhalb der geschlossenen Benutzergruppe dürfen insbesondere folgende Systeme nicht betrieben werden:

- Nachgelagerte IT-Systeme des TE-Betreibers,
- Office-IT-Systeme des Reservenanbieters oder Herstellers und
- IT-Systeme anderer Reservenanbieter (betrifft SaaS-Anbieter).

	FCR	aFRR	mFRR
B03	X	X	X

Die Nutzung von Internet-Technologien (z.B. IP, xDSL, UMTS, LTE) 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 Reservenanbieters 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.

	FCR	aFRR	mFRR	
B04	X	X	X	Innerhalb der geschlossenen Benutzergruppe muss durch den Reservenanbieter eine eigene Ende-zu-Ende-Verschlüsselung aufgebaut werden (nicht durch den Telekommunikations-dienstleister), um die Kommunikation zwischen den TE und Leitsystemen zusätzlich gegenüber dem Netzwerk der geschlossenen Benutzergruppe abzusichern.
B05	X	X	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 (Anforderung für geschlossene Benutzergruppen zur Erbringung von Regelreserve) beschrieben.
B06	X	X	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	X	X	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 Tunnelaufbau) ist nicht zulässig (auch nicht für Administration oder Monitoring).

B08 | FCR | aFRR | mFRR
X | X | 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 | FCR | aFRR | mFRR
X | X | X

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

B10 | FCR | aFRR | mFRR
X | X | X

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

B11 | FCR | aFRR | mFRR
X | X | X

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

3.1.2.4 Anbindung Technische Einheit (TE), Medienbruch

Die folgende Abbildung 3 gibt einen exemplarischen Überblick über die Anbindung verschiedener TE an das Leitsystem des Reservenanbieters.

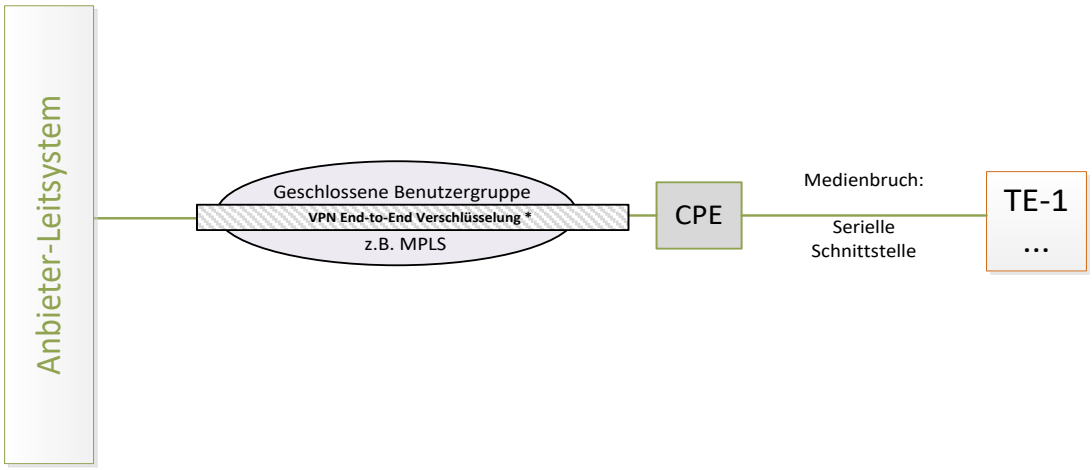

Abbildung 3: Exemplarischer Überblick der Anbindung von TE an das Reservenanbieter-Leitsystem

Es gelten für die Anbindung der TE an das Leitsystem des Reservenanbieters die folgenden Anforderungen:

	FCR	aFRR	mFRR	
C01	X	X	X	Jede TE muss mit einer Verfügbarkeit der Einzelverbindung von mindestens 95 % an das Leitsystem des Reservenanbieters angebunden werden. (Nachweise können über Verträge, systemseitig oder mittels Statistiken erbracht werden). Betreibt der Reservenanbieter aufgrund der Anforderung A06 örtlich getrennte Leitsysteme, so erfolgt die Anbindung der TE an jedes der beiden Leitsysteme (ggf. je Leitsystem zusätzlich redundant gemäß C02 / C03).
C02	X	X	X	TE mit einer Leistung ≥ 30 MW aFRR sind zusätzlich redundant an das Reservenanbieter-Leitsystem anzubinden. Diese Anforderung ist bei TE, die mFRR oder FCR zur Verfügung stellen, anzustreben.

C03	FCR	aFRR	mFRR	TE, die 50 MW aFRR 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 Regelreserve).
		≥ 50 MW		
C04	FCR	aFRR	mFRR	Die TE ist über eine serielle Schnittstelle anzubinden. Ein Medienbruch zum Internetprotokoll (IP) ist zwingend erforderlich. Alternativ ist auch eine direkte Steuerung von TE über binäre oder analoge Ausgänge (z.B. Schalt-Aktoren) sowie eine direkte Erfassung von Messwerten mittels Binäreingängen oder AD-Wandler zulässig.
	X	X	X	
C05	FCR	aFRR	mFRR	Konzeption zur Bündelung von Kleinstanlagen • Die Bündelung von Kleinstanlagen über öffentliches Internet mit verschlüsseltem VPN ist erlaubt • Bei der Bündelung von Kleinstanlagen kann auf die geschlossenen Benutzergruppen verzichtet werden • Zwischen gebündelten Kleinstanlagen und dem Poolbetreiber muss eine serielle Schnittstelle als Medienbruch gemäß den IT-Anforderungen implementiert werden • Maximale Größe von Kleinstanlagen: 25 KW • Maximale Größe einer Bündelung von Kleinstanlagen: 2 MW • Die Anbindung einer Kleinstanlage ist nur an einen Pool erlaubt (keine Mehrfachvermarktung) • Die Besicherung von gebündelten Kleinstanlagen durch andere gebündelte Kleinstanlagen ist nicht erlaubt, sofern die Voraussetzung für die gesicherte Vorhaltung
	X	X	X	

und Erbringung von Regelreserve eine intakte kommunikationstechnische Anbindung ist.

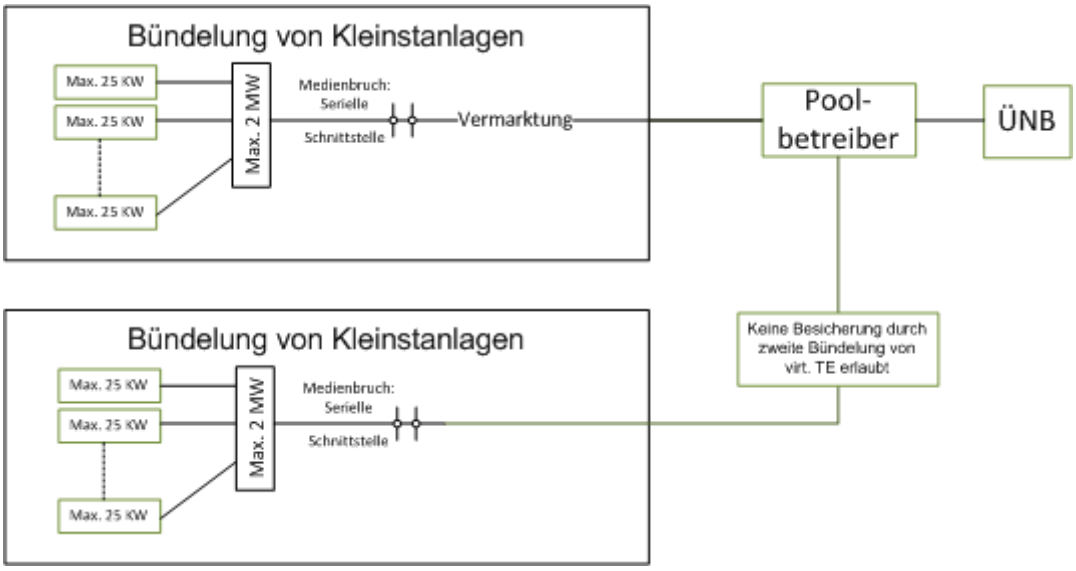

Abbildung 4: Exemplarischer Überblick einer Bündelung von Kleinstanlagen

3.1.2.5 Weitere Anforderungen

	FCR	aFRR	mFRR
D01	X	X	X

Datentransfers aus und in andere Netzwerke mit abweichendem Schutzbedarf werden grundsätzlich mit Datendrehscheiben vorgenommen. Durch Datendrehscheiben wird gewährleistet, dass Daten zwischen dem für die Erbringung der Regelreserve genutzten Netz 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.

- Mehrstufiger Virenschutz auf der Datendrehscheibe.

	FCR	aFRR	mFRR	
D02	X	X	X	Störungen an Teilen des Gesamtsystems ohne Komplettausfall, d.h. ohne Beeinträchtigung der Vorhaltung und Erbringung, muss der Reservenanbieter 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	X	X	X	Der Reservenanbieter hat eine kontinuierliche und lückenlose Überwachung der Verfügbarkeit der Übertragungsstrecken einschließlich aller CPE zu gewährleisten.
D04	X	X	X	Es ist ein angemessener Zutritts-, Zugangs- und Zugriffschutz zu Räumlichkeiten, Systemen und Netzwerken, die zur Erbringung der Regelreserve erforderlich sind, sicherzustellen. (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 Reservenanbieters müssen zusätzlich in einem alarmgesicherten, verschlossenen Sicherheitsschrank untergebracht sein. Diese Anforderung gilt nicht für Kleinstanlagen gemäß C05.
D05	X	X	X	Der Reservenanbieter 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, Virensignaturen, 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).

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

	FCR	aFRR	mFRR	
D07	X	X	X	Im Falle von kompromittierten Technologien besteht seitens der Reservenanbieter eine Meldepflicht gegenüber den ÜNB. Erlangt der ÜNB Kenntnis über eine kompromittierbare Technologie, so muss der Reservenanbieter 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

	FCR	aFRR	mFRR	
D08	X	X	X	Reservenanbieter, die Leistungen von externen IT-Dienstleistern beziehen, die wiederum ihre Dienstleistungen mehreren Reservenanbietern anbieten (z.B. SaaS-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. • Reservenanbieter, die solche Leistungen beziehen, werden grundsätzlich behandelt wie Reservenanbieter mit höchstem erforderlichen Schutzbedarf (wie aFRR ≥ 50MW). • IT-Dienstleister, die für verschiedene Reservenanbieter Dienstleistungen erbringen und deren assoziierte Reservenanbieter müssen gewährleisten, dass durch den Betrieb von gemeinsam genutzten Komponenten keine Risiken auf andere Reservenanbieter ausstrahlen können. So. darf z.B.

pro geschlossene Benutzergruppe nur ein Reservenanbieter angebunden werden.

- Der Reservenanbieter ist Hauptansprechpartner für den ÜNB und trägt die Gesamtverantwortung für die Erfüllung der IT Anforderungen zur Erbringung von Regelreserve.

3.2 Informationspflichten und Nachweise

Der Reservenanbieter hat die Sicherheit seines Gesamtsystems E2E (bidirektionaler Datenaustausch zwischen der Technischen Einheit zum ÜNB über das Reservenanbieter-Leitsystem) entsprechend Kapitel 3.3 nachzuweisen. Folgende Anforderungen sind zu gewährleisten:

- Technische Vertragsinhalte zur IT-Sicherheit und Verfügbarkeit hat der Reservenanbieter 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 Grundschutzanalysen hat der Reservenanbieter den ÜNB auf Anfrage nachzuweisen.
- Die Konzeption und Umsetzung von IT-Sicherheitsmaßnahmen hat der Reservenanbieter den ÜNB auf Anfrage nachzuweisen (ggf. auch vor Ort). Sicherheitstechnisch relevante Änderungen und Sicherheitsvorfälle im Gesamtsystem muss der Reservenanbieter 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 dahinterliegende Systeme, etc.
- Wenn die Datenbereitstellung zum ÜNB nicht ordnungsgemäß gewährleistet werden kann, muss der Reservenanbieter den ÜNB hierüber unverzüglich informieren.
- Die Reservenanbieter 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.net werden seitens der ÜNB gegenüber den Reservenanbietern entsprechend kommuniziert.
- Im Bedarfsfall müssen die Konzepte seitens der Reservenanbieter 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 Reservenanbieter aufgefordert, jeweils zum 31.01. für das Vorjahr einen Jahresbericht zum Betrieb der für die Erbringung der Regelreserve verwendeten IT- Systeme dem jeweiligen Reserven anschließenden ÜNB vorzulegen (siehe Anlage 3Reservenanbieter Bericht über die Informationstechnik des Reservenanbieters und Vorfälle bei der Erbringung von Regelreserve).

3.3 Selbstauskunft und Nachweise

Der Reservenanbieter bestätigt im Rahmen einer Selbstauskunft (siehe unten) und durch Nachweise (siehe Kap. 3.2), dass die vorliegenden Mindestanforderungen an die Informationstechnik des Reservenanbieters für die Erbringung von Regelreserve eingehalten werden. Die Selbstauskunft ist durch den Geschäftsführer bzw. eine autorisierte Vertretung des Reservenanbieters zu unterzeichnen.

Im Rahmen der Präqualifikation müssen folgende Dokumente seitens des Reservenanbieters zur Prüfung der IT-Anforderungen zur Erbringung von Regelreserve vorgelegt werden:

- Vorlage eines aussagekräftigen IT-Konzepts (ohne Angabe von betriebsrelevanten Informationen wie z.B. IP-Adressen)
- IT-Checkliste mit Zuordnung der entsprechenden Kapitel des IT-Konzepts einschließlich der Beschreibung der Verschlüsselungstechnik- (siehe Anlage 1 Checkliste für die

Mindestanforderungen an die Informationstechnik des Reservenanbieters für die Erbringung von Regelreserve)

- Klassifizierung der Informationssicherheit der durch den Anbieter abgegebenen Dokumente

Reservenanbieter, Dienstleister zur Erbringung von Regelreserve und IT-Systemdienstleister, die Anlagen oder Systeme zur Steuerung und Bündelung von Erzeugungs- und Verbrauchseinrichtung mit einer Netto-Nennleistung von mindestens 420 MW in Deutschland bündeln, unterliegen ab 31.01.2018 einer Zertifizierungspflicht nach BSI-KritisV. In diesem Fall ist der Nachweis über eine Zertifizierung gemäß den Vorgaben des BSI, des IT-Sicherheitsgesetzes und BSI-KritisV sowie in Anlehnung an den IT-Sicherheitskatalog nach §11 Absatz 1a EnWG bzw. gem. eines IT-Sicherheitskatalogs nach § 11 Abs. 1b EnWG erforderlich.

Wie bereits in der Konsultationsfassung des vorliegenden Dokuments vom April 2018 sehen die ÜNB von einer verpflichtenden Zertifizierung aller Reservenanbieter bis auf Weiteres ab. Die vorangehend beschriebenen Anforderungen sind gesetzlich vorgeschriebene Mindestanforderungen, die eine Zertifizierungspflicht ab einer installierten Nennleistung von 420 MW (elektrisch) vorsehen. Die ÜNB behalten sich allerdings vor, zu einem späteren Zeitpunkt und mit einer angemessenen Umsetzungszeit weitere Vorgaben hinsichtlich der ISMS-Zertifizierung zu machen.

Anlagen (siehe Plattform regelleistung.net):

4.3 Checkliste für die Mindestanforderungen an die Informationstechnik des Reservenanbieters für die Erbringung von Regelreserve

4.4 Anforderung für geschlossene Benutzergruppen zur Erbringung von Regelreserve

4.5 Bericht über die Informationstechnik des Reservenanbieters und Vorfälle bei der Erbringung von Regelreserve

4.6 Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren[2]

[2] Siehe Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren: https://www.regelleistung.net/ext/static/srl/it (Stand: 20.12.2019)

4 Abkürzungsverzeichnis und Glossar

Begriff/Abkürzung/Satzteil	Klärung
AD	Active Directory
aFRR	automatic Frequency Restoration Reserve (ehemals SRL)
BSI	Bundesamt für Sicherheit in der Informationstechnik
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.
CPE	Customer Premises Equipment sind Geräte des Reservenanbieters von Regelleistung als Netzabschluss- und Übergabeschnittstelle
DNS	Domain Name System
DSL	Digital Subscriber Line
E2E (End–to–End)	Übertragungsweg von der Technischen Einheit über das Reservenanbieter-Leitsystem bis zum Leitsystem des ÜNB
FCR	Frequency Containment Reserve (ehemals PRL)
Gesamtsystem	alle zur Leistungserbringung/Vertragserfüllung notwendigen Komponenten
Geschlossene Benutzergruppe	Von einem Telekommunikationsdienstleister bereitgestellte Anschlüsse im Zugangsnetz, welche von diesem in einem geschlossenen Verbund betrieben werden. Dieses können Anschlüsse in unterschiedlichen Übertragungsnetzen wie DSL/UMTS/GSM/LTE 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.
GSM	Global System for Mobile communication
IP	Internet protocol

IT	Informationstechnologie
KRITIS	Kritische Infrastruktur
LS	Leitsystem
LTE	Long Term Evolution
mFRR	manual Frequency Restoration Reserve (ehemals MRL)
MPLS	Multiprotocol Label Switching (paketvermittelndes Übertragungsverfahren)
NTP	Network Time Protocol
Patchmanagement	Bereich des Systemmanagements zur Beschaffung, Testen und Installation von Patches.
PDH	Plesiochrone Digitale Hierarchie (leitungsvermittelndes Übertragungsverfahren)
Redundanz (Leitsystem)	Bei örtlicher Redundanz mindestens zwei Standorte mit jeweils vom anderen Standort unabhängigen • Energieversorgungen und • Kommunikationsverbindungen. Die Störung eines Standortes darf den anderen Standort nicht in Mitleidenschaft ziehen (siehe auch Hinweise zur Entfernung von Rechenzentren in Anlage 4 Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren).
Redundanz (Übertragungsstrecke)	Redundanz bei der Datenübertragung definiert sich wie folgt: • knoten- und kantendisjunkt • keine doppelt genutzten Geräte • keine doppelt genutzten Kabelstrecken
RE	Reserveeinheit
RG	Reservegruppe
SaaS-Reservenanbieter	Software-as-a-Service-Reservenanbieter
SDH	Synchrone Digitale Hierarchie (leitungsvermittelndes Übertragungsverfahren)
SFTP	Secure File Transfer Protocol

SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SO GL	System Operation Guideline
SÜFV	Sicherheitsüberprüfungsfeststellungsverordnung
SÜG	Sicherheitsüberprüfungsgesetz
TE	Technische Einheit(en)
UMTS	Universal Mobile Telecommunication System
ÜNB	Übertragungsnetzbetreiber
VPN	Virtual Private Network Verbindung zwischen zwei „privaten“ Netzwerksegmenten, welche über ein von Dritten betriebenes Netzwerk geführt wird.
WSUS	Windows Server Update Services

Selbstauskunft zu den „Mindestanforderungen an die Informationstechnik des Reservenanbieters für die Erbringung von Regelreserve“

_____ (Name des Reservenanbieters) als Reservenanbieter für Regelreserve erklärt hiermit, dass er die von den deutschen Übertragungsnetzbetreibern (ÜNB) erstellten „Mindestanforderungen an die Informationstechnik des Reservenanbieters für die Erbringung von Regelreserve“ vom 20.12.2019 in der jeweils geltenden Fassung während der Laufzeit des Rahmenvertrages erfüllt.

Name und Anschrift des Reservenanbieters:

Ort und Datum: ……..

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