



Mindestanforderungen an die Informationstechnik des Reservenankbieters zur Erbringung von Regelreserve

Stand: 01.05.2023

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	<ul style="list-style-type: none"> 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
2.2	04.11.2020	<ul style="list-style-type: none"> Anpassung C04 und Abbildung 3 (Option zentraler Medienbruch) Erweiterung C06 für Bündelung von Erzeugungsanlagen an einem Netzanschlusspunkt Erweiterung Kapitel 3.3 (Informationspflicht bei Änderungen der IT-Konzeption)
2.3	01.03.2022	<ul style="list-style-type: none"> Anpassung C06 für Bündelung von Erzeugungsanlagen (maximale Leistung) Erweiterung Kapitel 3.3 gemäß BSI-KritisV 2.0 (Informationspflicht bei Änderungen der IT-Konzeption)
2.4	01.05.2023	<ul style="list-style-type: none"> Anpassung A02 bzgl. Vorgaben zum Betrieb der Systeme innerhalb der EU Anpassung B05 zur Verschlüsselung mit IPsec-VPN oder OpenVPN, jeweils mit AES256, oder Wireguard-VPN Anpassung C05 zu den Besicherungsbedingungen

Inhalt

Abbildungsverzeichnis.....	4
1 Vorwort	4
2 Präambel	6
2.1 Zielsetzung	6
2.2 Geltungsbereich	7
3 Sicherheitsanforderungen	8
3.1 Mindestanforderungen an die Informationstechnik des Reservenansbieters für die Erbringung von Regelreserve	10
3.1.1 Überblick	10
3.1.2 Grundsätzliche Anforderungen	11
3.1.2.1 Reservenansbieter Leitsystem	12
3.1.2.2 ÜNB Leitsystem/Anbindung	13
3.1.2.3 Geschlossene Benutzergruppe	15
3.1.2.4 Anbindung Technische Einheit (TE), Medienbruch.....	19
3.1.2.5 Weitere Anforderungen	23
3.1.2.6 Externe IT-Dienstleister	25
3.2 Informationspflichten und Nachweise.....	25
3.3 Selbstauskunft und Nachweise	27
4 Abkürzungsverzeichnis und Glossar	29

Abbildungsverzeichnis

Abbildung 1: Exemplarischer und ganzheitlicher Überblick der Anbindung von einem Reservenansichters an einen ÜNB	10
Abbildung 2: Exemplarischer Überblick der Anbindung von einem Reservenansichters-Leitsystem an einen ÜNB	13
Abbildung 3: Exemplarischer Überblick der Anbindung von TE an das Reservenansichters-Leitsystem	19
Abbildung 4: Exemplarischer Überblick einer Bündelung von Kleinanlagen	20

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 angebotenen 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 Reservenansbieter 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 Reservenansbieters 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 Reservenansbieter nicht von seiner vertraglichen Verpflichtung zur vollständigen Vorhaltung und Erbringung von Regelreserve. Es liegt im Ermessen des Reservenansbieters, 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 Reservenansbieters für die Erbringung von Regelreserve“ erfordern, sind die ÜNB einseitig zur Anpassung der „Mindestanforderungen an die Informationstechnik des Reservenansbieters für die Erbringung von Regelreserve“ berechtigt. Entsprechend sind die Reservenansbieter verpflichtet, die neuen Anforderungen umzusetzen.

Die ÜNB behalten sich das Recht vor, die Einhaltung der technischen und organisatorischen Maßnahmen bei den Reservenansbietern 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 beachten¹:

- **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 Reservenansbieters für die Erbringung von Regelreserve

3.1.1 Überblick

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

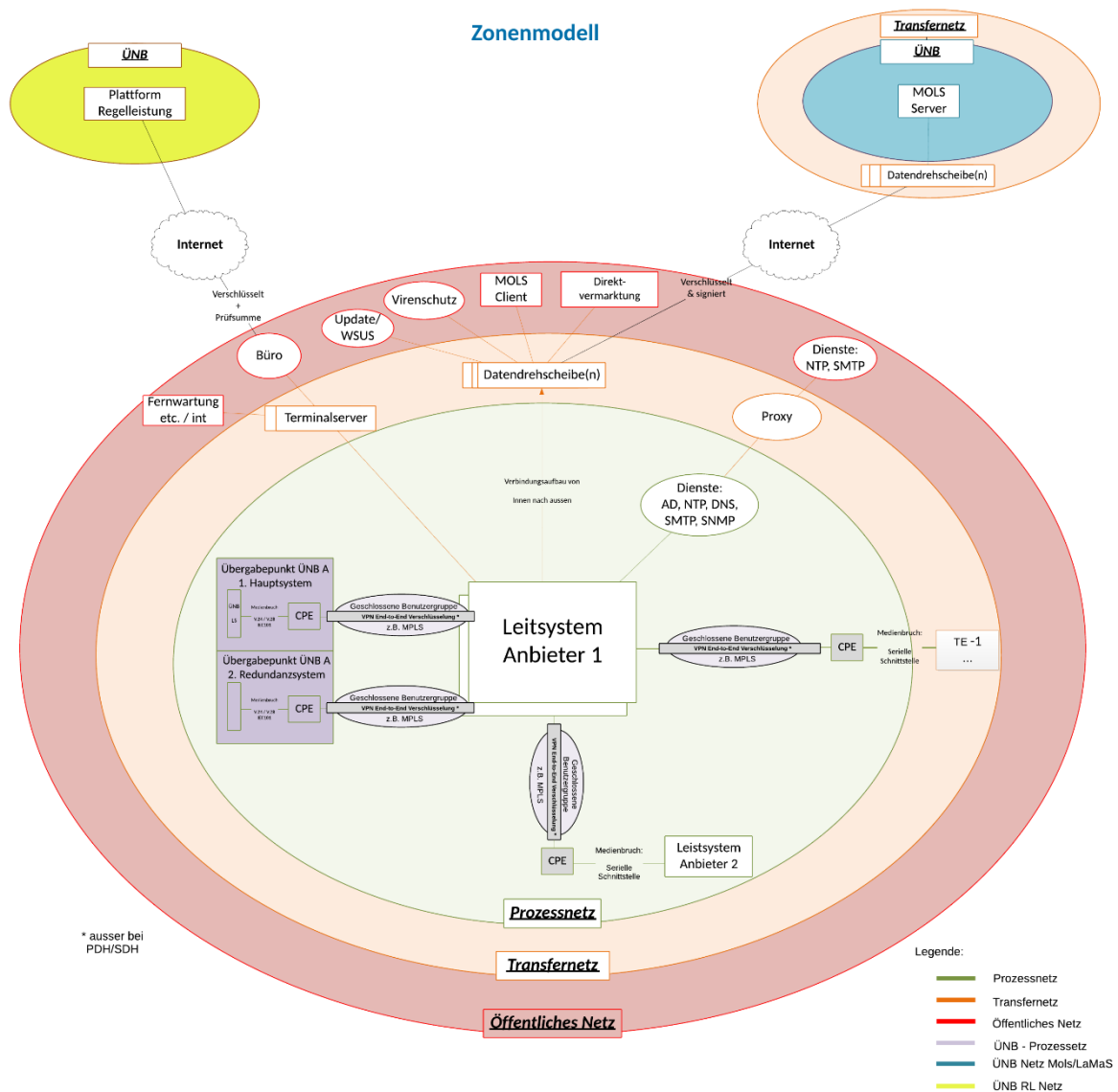


Abbildung 1: Exemplarischer und ganzheitlicher Überblick der Anbindung von einem Reservenanbieter an einen ÜNB

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 Reservenansbieters 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 Reservenankbieters angebotenen 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 Reservenankbieter Leitsystem

A01 **FCR** **aFRR** **mFRR** Das zentrale Leitsystem des Reservenankbieters ist gedoppelt auszuführen. Eine Aufteilung in zwei redundante Standorte hinsichtlich der Infrastruktur (Kommunikation und Stromversorgung) ist anzustreben. Der Reservenankbieter hat eine angemessene Sicherheit seiner Leitsysteme für Regelreserve zu gewährleisten. Diese Anforderung gilt grundsätzlich für aFRR, FCR und auch für mFRR bei einer vermarktaren Leistung ab 50 MW.

A02 **FCR** **aFRR** **mFRR** Der Betriebsstandort der eingesetzten Rechenzentren einschließlich der eingesetzten Mitarbeiter muss den gesetzlichen Anforderungen zum Datenschutz der EU unterliegen und den anerkannten Regeln der Technik genügen.

A03 **FCR** **aFRR** **mFRR** Eine automatische Umschaltung zwischen den redundanten zentralen Leitsystemen des Reservenankbieters 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** Die Verzögerung auf der kompletten Übertragungsstrecke E2E (von der Messwerterfassung der Technischen Einheit über das Reservenankbieter-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.

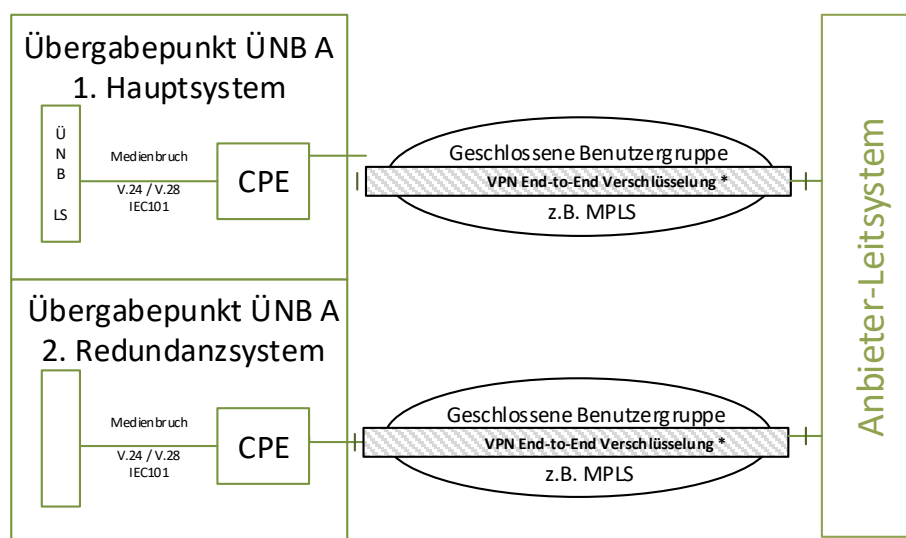


Abbildung 2: Exemplarischer Überblick der Anbindung von einem Reservenanbieter-Leitsystem an einen ÜNB

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

- A05 **FCR** **aFRR** **mFRR** Reservenanbieter, deren vermarktete aFRR innerhalb einer LFR-Zone 50 MW oder mehr beträgt, müssen die Verbindung zwischen dem ÜNB und dem Leitsystem des Reservenansbieters weiterhin mit der bisherigen Punkt-zu-Punkt-Festnetzverbindung (SDH/PDH) oder gleichwertigen Technologien realisieren (siehe Definition Anlage 3, Kapitel 5 zur Anforderung für geschlossene Benutzergruppen zur Erbringung von Regelreserve). Diese
- ≥ 50
MW

Anforderung gilt auch für Reservenanbieter, die in der Zukunft eine Vermarktung von 50 MW oder mehr aFRR anstreben.

- | | | | | | | | | | | | |
|-----------|--|-----------|------|------|-----------|-----------|-----------|--|----|----|---|
| A06 | <table border="0"> <tr> <td style="background-color: #e0b0ff; padding: 2px;">FCR</td> <td style="background-color: #e0b0ff; padding: 2px;">aFRR</td> <td style="background-color: #e0b0ff; padding: 2px;">mFRR</td> </tr> <tr> <td style="padding: 2px;">≥ 90</td> <td style="padding: 2px;">≥ 50</td> <td></td> </tr> <tr> <td style="padding: 2px;">MW</td> <td style="padding: 2px;">MW</td> <td></td> </tr> </table> | FCR | aFRR | mFRR | ≥ 90 | ≥ 50 | | MW | MW | | <p>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 vermarktete 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 Batteriemangement) erforderlich ist, ist das Leitsystem ab einer vermarkteten Leistung ≥ 90 MW örtlich redundant auszuführen.</p> |
| FCR | aFRR | mFRR | | | | | | | | | |
| ≥ 90 | ≥ 50 | | | | | | | | | | |
| MW | MW | | | | | | | | | | |
| A07 | <table border="0"> <tr> <td style="background-color: #e0b0ff; padding: 2px;">FCR</td> <td style="background-color: #e0b0ff; padding: 2px;">aFRR</td> <td style="background-color: #e0b0ff; padding: 2px;">mFRR</td> </tr> <tr> <td style="padding: 2px;">X</td> <td style="padding: 2px;">X</td> <td style="padding: 2px;">≥ 50</td> </tr> <tr> <td></td> <td></td> <td style="padding: 2px;">MW</td> </tr> </table> | FCR | aFRR | mFRR | X | X | ≥ 50 | | | MW | <p>Die leittechnische Anbindung zur Erbringung von Regelreserve hat in Form einer dedizierten Punkt-zu-Punkt-Verbindung zwischen der Leitwarte des ÜNB und dem Leitsystem des Reservenbieters 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 vermarkteter Regelreserve auch für mFRR (siehe auch Kapitel 3.1.2.3).</p> |
| FCR | aFRR | mFRR | | | | | | | | | |
| X | X | ≥ 50 | | | | | | | | | |
| | | MW | | | | | | | | | |
| A08 | <table border="0"> <tr> <td style="background-color: #e0b0ff; padding: 2px;">FCR</td> <td style="background-color: #e0b0ff; padding: 2px;">aFRR</td> <td style="background-color: #e0b0ff; padding: 2px;">mFRR</td> </tr> <tr> <td style="padding: 2px;">X</td> <td style="padding: 2px;">X</td> <td style="padding: 2px;">X</td> </tr> </table> | FCR | aFRR | mFRR | X | X | X | <p>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.</p> | | | |
| FCR | aFRR | mFRR | | | | | | | | | |
| X | X | X | | | | | | | | | |

- A09 **FCR** **aFRR** **mFRR** 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)).
X X X
- A10 **FCR** **aFRR** **mFRR** 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.
X X X
- A11 **FCR** **aFRR** **mFRR** Die Übertragungstrecken und Schnittstellen zu den beiden Übergabepunkten des ÜNB müssen vollständig redundant zueinander ausgelegt werden:
X
- knoten- und kantendisjunkt,
 - keine doppelt genutzten Geräte und
 - keine doppelt genutzten Kabelstrecken.
- A12 **FCR** **aFRR** **mFRR** Die einzelne Verbindung zwischen den Leitsystemen des ÜNB und des Reservenansbieters 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.
X X X

3.1.2.3 Geschlossene Benutzergruppe

- B01 **FCR** **aFRR** **mFRR** 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
X X X

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 Reservenbieters.

B02	FCR	aFRR	mFRR	<p>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 Reservenbieters oder präqualifizierte TE des Reservenbieters.</p> <p>Innerhalb der geschlossenen Benutzergruppe dürfen insbesondere folgende Systeme nicht betrieben werden:</p> <ul style="list-style-type: none"> • Nachgelagerte IT-Systeme des TE-Betreibers, • Office-IT-Systeme des Reservenbieters oder Herstellers und • IT-Systeme anderer Reservenbieter (betrifft SaaS-Anbieter).
	X	X	X	

B03	FCR	aFRR	mFRR	<p>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 Reservenbieters nicht mit "fremden" Netzwerken in Berührung kommt. Der Verkehr soll somit gegenüber anderen Netzwerken</p>
	X	X	X	

des Telekommunikationsdienstleisters, z.B. von anderen Kundennetzwerken oder gegenüber dem Internet, abgesichert werden.

- B04 **FCR** **aFRR** **mFRR**
X X X Innerhalb der geschlossenen Benutzergruppe muss durch den Reservenanbieter eine eigene Ende-zu-Ende-Verschlüsselung aufgebaut werden (nicht durch den Telekommunikationsdienstleister), um die Kommunikation zwischen den TE und Leitsystemen zusätzlich gegenüber dem Netzwerk der geschlossenen Benutzergruppe abzusichern.
- B05 **FCR** **aFRR** **mFRR**
X X X Die zwischen den Zugangsroutern übertragenen Daten müssen über einen verschlüsselten Tunnel mit einem IPsec-VPN oder OpenVPN, jeweils mit mindestens AES256, oder Wireguard-VPN geführt werden. Eine Empfehlung für eine sichere Verschlüsselung ist in der Anlage 3 (Anforderung für geschlossene Benutzergruppen zur Erbringung von Regelreserve) beschrieben.
- B06 **FCR** **aFRR** **mFRR**
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 **FCR** **aFRR** **mFRR**
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 | <table border="0"> <tr> <td style="background-color: #800080; color: white; padding: 2px;">FCR</td> <td style="background-color: #4169E1; color: white; padding: 2px;">aFRR</td> <td style="background-color: #4169E1; color: white; padding: 2px;">mFRR</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table> | FCR | aFRR | mFRR | X | X | X | <p>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.</p> |
| FCR | aFRR | mFRR | | | | | | |
| X | X | X | | | | | | |
| B09 | <table border="0"> <tr> <td style="background-color: #800080; color: white; padding: 2px;">FCR</td> <td style="background-color: #4169E1; color: white; padding: 2px;">aFRR</td> <td style="background-color: #4169E1; color: white; padding: 2px;">mFRR</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table> | FCR | aFRR | mFRR | X | X | X | <p>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.</p> |
| FCR | aFRR | mFRR | | | | | | |
| X | X | X | | | | | | |
| B10 | <table border="0"> <tr> <td style="background-color: #800080; color: white; padding: 2px;">FCR</td> <td style="background-color: #4169E1; color: white; padding: 2px;">aFRR</td> <td style="background-color: #4169E1; color: white; padding: 2px;">mFRR</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table> | FCR | aFRR | mFRR | X | X | X | <p>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).</p> |
| FCR | aFRR | mFRR | | | | | | |
| X | X | X | | | | | | |
| B11 | <table border="0"> <tr> <td style="background-color: #800080; color: white; padding: 2px;">FCR</td> <td style="background-color: #4169E1; color: white; padding: 2px;">aFRR</td> <td style="background-color: #4169E1; color: white; padding: 2px;">mFRR</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table> | FCR | aFRR | mFRR | X | X | X | <p>Alle Übertragungsstrecken sind zu verschlüsseln. Von dieser Vorgabe nicht betroffen sind Punkt-zu-Punkt Verbindungen, die seriell ausgeführt sind. Diese bedürfen keiner Verschlüsselung.</p> |
| FCR | aFRR | mFRR | | | | | | |
| X | X | X | | | | | | |

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 Reservenansbieters.

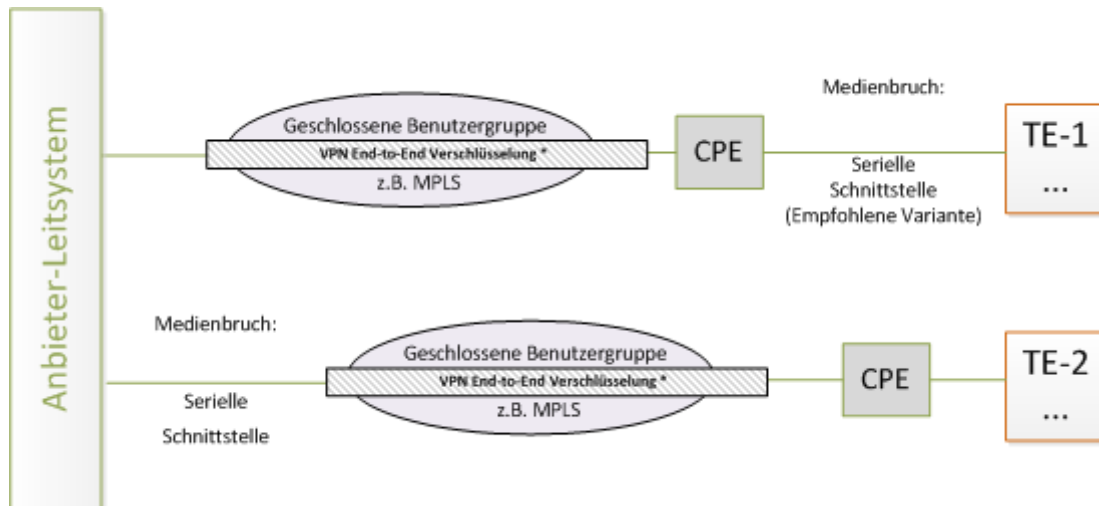


Abbildung 3: Exemplarischer Überblick der Anbindung von TE an das Reservenanbieter-Leitsystem

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

C01

FCR	aFRR	mFRR
X	X	X

 Jede TE muss mit einer Verfügbarkeit der Einzelverbindung von mindestens 95 % an das Leitsystem des Reservenansbieters 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

FCR	aFRR	mFRR
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 3, Kapitel 5 zur Anforderung für geschlossene Benutzergruppen zur Erbringung von Regelreserve).
- ≥ 50
MW
- C04 **FCR** **aFRR** **mFRR** Eine TE ist über eine serielle Schnittstelle anzubinden. Ein Medienbruch zum Internetprotokoll (IP) ist zwingend erforderlich. Der Medienbruch kann lokal bei der TE (empfohlene Variante) oder zentral beim Leitsystem erfolgen. 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
- X X X
- Die Bündelung von Kleinstanlagen über öffentliches Internet mit verschlüsseltem VPN ist erlaubt.
 - Bei der Bündelung von Kleinstanlagen kann auf die geschlossenen Benutzergruppen verzichtet werden.
 - Werden Kleinstanlagen über das Internet gebündelt, ist z.B. durch einen Penetrationstest vom Anbieter nachzuweisen, dass die Bündelung sicher entsprechend dem Stand der Technik betrieben wird.
 - Zwischen gebündelten Kleinstanlagen und dem Poolbetreiber muss eine serielle Schnittstelle als Medienbruch gemäß den IT-Anforderungen implementiert werden.
 - Die installierte Leistung einer Kleinstanlage darf maximal 100 kW betragen.
 - Die vermarktete Leistung einer Bündelung von Kleinstanlagen darf maximal 10 MW betragen.

- Die Anbindung einer Kleinstanlage ist nur an einen Pool erlaubt (keine Mehrfachvermarktung).
- Die Besicherung einer Bündelung von Kleinstanlagen durch eine andere Bündelung von Kleinstanlagen ist nicht erlaubt, sofern die Voraussetzung für die gesicherte Vorhaltung und Erbringung von Regelreserve eine intakte kommunikationstechnische Anbindung ist.
- Innerhalb einer Bündelung von Kleinstanlagen dürfen Kleinstanlagen zur Ausfallabsicherung benutzt werden. Diese Ausfallabsicherung kann aber nicht den Ausfall des gesamten Bündels kompensieren.
- Innerhalb einer Bündelung von Kleinstanlagen ist eine Aggregation von Kleinstanlagen erlaubt, die dann in der Bündelung von Kleinstanlagen zugeführt werden, solange die maximal vermarktete Leistung der Bündelung von Kleinstanlagen nicht überschritten wird. Jede Aggregation darf nur an eine Bündelung von Kleinstanlagen über Internet mit VPN angeschlossen werden. Diese Aggregation gilt nur für die Kommunikationswege, nicht aber für die Datenpunkte.
- Die Anforderungen aus D02 (Entstörung innerhalb von 24h) gelten nicht für einzelne Kleinstanlagen, aber für die gesamte Bündelung von Kleinstanlagen.

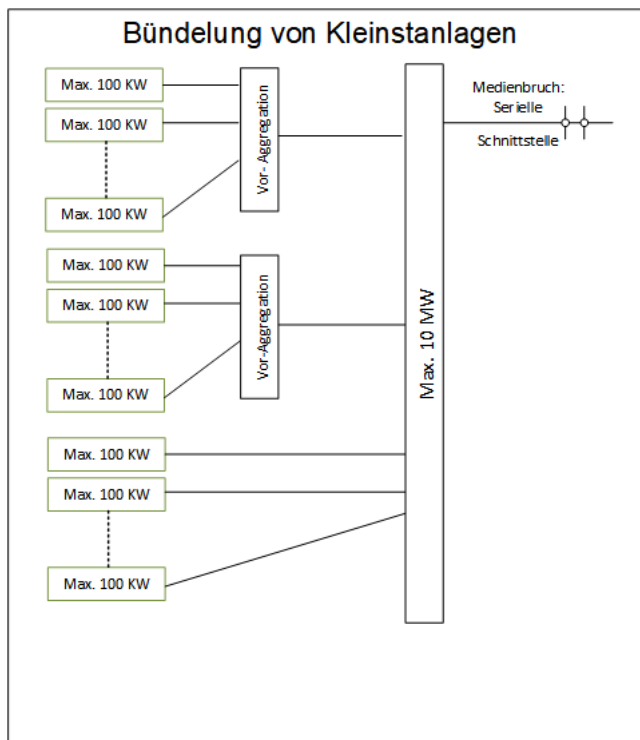


Abbildung 4: Exemplarischer Überblick einer Bündelung von Kleinanlagen

C06 **FCR** **aFRR** **mFRR** Bündelung von Anlagen (Erzeuger und/oder Verbraucher) an einem gemeinsamen Netzanschlusspunkt
X X X

- TE, die über einen gemeinsamen Netzanschlusspunkt angeschlossen sind, können als eine TE im Sinne dieses IT-Konzeptes verstanden werden. Für diese Bündelung ist dann nur eine Kommunikationsverbindung zum Anbieterleitsystem erforderlich.
- Die Redundanzanforderungen aus C02 und C03 müssen entsprechend berücksichtigt werden.
- Diese gebündelten Anlagen werden bei der Besicherung wie eine TE behandelt.
- Innerhalb der Bündelung von Anlagen müssen eigene Netzwerke ohne öffentliches Internet verwendet werden.
- Die Nutzung der seriellen Schnittstelle gemäß C04 ist weiterhin erforderlich.

3.1.2.5 Weitere Anforderungen

D01	<table border="0"> <tr> <td style="background-color: #e0b0ff;">FCR</td> <td style="background-color: #e0b0ff;">aFRR</td> <td style="background-color: #e0b0ff;">mFRR</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table>	FCR	aFRR	mFRR	X	X	X	<p>Datentransfers aus und in andere Netzwerke mit abweichendem Schutzbedarf werden grundsätzlich mit Datendreh scheiben vorgenommen. Durch Datendreh scheiben 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.</p> <ul style="list-style-type: none"> • 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 Datendreh scheibe.
FCR	aFRR	mFRR						
X	X	X						
D02	<table border="0"> <tr> <td style="background-color: #e0b0ff;">FCR</td> <td style="background-color: #e0b0ff;">aFRR</td> <td style="background-color: #e0b0ff;">mFRR</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table>	FCR	aFRR	mFRR	X	X	X	<p>Störungen an Teilen des Gesamtsystems ohne Komplettausfall, d.h. ohne Beeinträchtigung der Vorhaltung und Erbringung, muss der Reservenansbieter 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.</p>
FCR	aFRR	mFRR						
X	X	X						
D03	<table border="0"> <tr> <td style="background-color: #e0b0ff;">FCR</td> <td style="background-color: #e0b0ff;">aFRR</td> <td style="background-color: #e0b0ff;">mFRR</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table>	FCR	aFRR	mFRR	X	X	X	<p>Der Reservenansbieter hat eine kontinuierliche und lückenlose Überwachung der Verfügbarkeit der Übertragungsstrecken einschließlich aller CPE zu gewährleisten.</p>
FCR	aFRR	mFRR						
X	X	X						
D04	<table border="0"> <tr> <td style="background-color: #e0b0ff;">FCR</td> <td style="background-color: #e0b0ff;">aFRR</td> <td style="background-color: #e0b0ff;">mFRR</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table>	FCR	aFRR	mFRR	X	X	X	<p>Es ist ein angemessener Zutritts-, Zugangs- und Zugriffschutz zu Räumlichkeiten, Systemen und Netzwerken, die zur Erbringung der Regelreserve erforderlich sind, sicherzustellen. (z.B. Zutritts-</p>
FCR	aFRR	mFRR						
X	X	X						

und Schlüsselkonzepte, Berechtigungsmanagement und physikalische Sicherheitsmaßnahmen in Verbindung mit einem angemessenen Anweisungswesen und Kontrollen). Elektrische Betriebsräume müssen abgeschlossen sein. Die Geräte des Reservenansbieters müssen zusätzlich in einem alarmgesicherten, verschlossenen Sicherheitsschrank untergebracht sein. Diese Anforderung gilt nicht für Kleinanlagen gemäß C05.

- | | | | | | | | | |
|-----|--|------|------|------|---|---|---|---|
| D05 | <table border="0"> <tr> <td style="background-color: #e0b0ff; padding: 2px;">FCR</td> <td style="background-color: #e0b0ff; padding: 2px;">aFRR</td> <td style="background-color: #e0b0ff; padding: 2px;">mFRR</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table> | FCR | aFRR | mFRR | X | X | X | <p>Der Reservenansbieter hat ein ganzheitliches Patch- und Change-Management 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).</p> |
| FCR | aFRR | mFRR | | | | | | |
| X | X | X | | | | | | |
| D06 | <table border="0"> <tr> <td style="background-color: #e0b0ff; padding: 2px;">FCR</td> <td style="background-color: #e0b0ff; padding: 2px;">aFRR</td> <td style="background-color: #e0b0ff; padding: 2px;">mFRR</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table> | FCR | aFRR | mFRR | X | X | X | <p>Alle Maßnahmen (technisches Konzept, Wegeführung, Entstörzeiten, Wartungsverträge etc.) zur Erreichung der geforderten Verfügbarkeit sind den ÜNB auf Anfrage darzustellen.</p> |
| FCR | aFRR | mFRR | | | | | | |
| X | X | X | | | | | | |
| D07 | <table border="0"> <tr> <td style="background-color: #e0b0ff; padding: 2px;">FCR</td> <td style="background-color: #e0b0ff; padding: 2px;">aFRR</td> <td style="background-color: #e0b0ff; padding: 2px;">mFRR</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table> | FCR | aFRR | mFRR | X | X | X | <p>Im Falle von kompromittierten Technologien besteht seitens der Reservenansbieter eine Meldepflicht gegenüber den ÜNB. Erlangt der ÜNB Kenntnis über eine kompromittierbare Technologie, so muss der Reservenansbieter auf Anforderung die kompromittierbare Technologie nachbessern. Alternative Technologien müssen in einem solchen Fall innerhalb einer in Rücksprache mit den ÜNB abgestimmten Übergangsfrist umgesetzt werden.</p> |
| FCR | aFRR | mFRR | | | | | | |
| X | X | X | | | | | | |

3.1.2.6 Externe IT-Dienstleister

D08 **FCR** **aFRR** **mFRR** Reservenanbieter, die Leistungen von externen IT-Dienstleistern beziehen, die wiederum ihre Dienstleistungen mehreren Reservenansbiestern anbieten (z.B. SaaS-Anbieter), bedürfen besonderer Regelungen:

X X X

- 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 \geq 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 Zugangsrouten 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 Reservenansbiestern 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 4 Reservenankbieter Bericht über die Informationstechnik des Reservenankbieters und Vorfälle bei der Erbringung von Regelreserve).

3.3 Selbstauskunft und Nachweise

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

Im Rahmen der Präqualifikation müssen folgende Dokumente seitens des Reservenankbieters 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 sowie einer Aufstellung der involvierten Telekommunikationsdienstleister bzw. *Software as a Service* Anbietern (siehe Anlage 1 Checkliste für die Mindestanforderungen an die Informationstechnik des Reservenankbieters für die Erbringung von Regelreserve)
- Klassifizierung der Informationssicherheit der durch den Anbieter abgegebenen Dokumente

Änderungen an den IT-Konzepten (auch ohne Auswirkung auf die präqualifizierte Leistung) müssen vor der Nutzung bei den ÜNB zur Freigabe eingereicht werden.

Reservenankbieter, 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 104 MW (36 MW bei Präqualifikation zur Erbringung von Primärregelleistung) in Deutschland bündeln, unterliegen ab 14.09.2021 einer Zertifizierungspflicht nach BSI-KritisV 2.0. 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 Reservenankbieter bis auf Weiteres ab. Die vorangehend beschriebenen Anforderungen sind gesetzlich vorgeschriebene Mindestanforderungen, die eine Zertifizierungspflicht ab einer installierten Nennleistung von 104 / 36 MW (elektrisch) vorsehen.

Die in diesem Dokument formulierten Mindestanforderungen werden ergänzt durch die folgenden Anlagen: (siehe Plattform [regelleistung.net](https://www.regelleistung.net)):

- Checkliste für die Mindestanforderungen an die Informationstechnik des Reservenankbieters für die Erbringung von Regelreserve
- Anforderung für geschlossene Benutzergruppen zur Erbringung von Regelreserve
- Bericht über die Informationstechnik des Reservenankbieters und Vorfälle bei der Erbringung von Regelreserve Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren²

² Siehe Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren:
<https://www.regelleistung.net/de-de/Infos-f%C3%BCr-Anbieter/Wie-werde-ich-Regelenergieanbieter-Pr%C3%A4qualifikation>

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 Reservenansbieters 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 Reservenansbieter-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 Zugangnetz, 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 <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • knoten- und kantendisjunkt • keine doppelt genutzten Geräte • keine doppelt genutzten Kabelstrecken
RE	Reserveeinheit
RG	Reservegruppe
SaaS-Reservenansichters	Software-as-a-Service-Reservenansichters
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 Reservenbieters für die Erbringung von Regelreserve“**

_____ (Name des Reservenbieters) als Reservenbieter für Regelreserve erklärt hiermit, dass er die von den deutschen Übertragungsnetzbetreibern (ÜNB) erstellten „Mindestanforderungen an die Informationstechnik des Reservenbieters für die Erbringung von Regelreserve“ vom 01.05.2023 in der jeweils geltenden Fassung während der Laufzeit des Rahmenvertrages erfüllt.

Name und Anschrift des Reservenbieters:

Ort und Datum:

Unterschrift (Geschäftsführer oder autorisierte Vertretung):