Minimum requirements for the information technology of the reserve provider for the provision of control reserve and providers of interruptible loads

Version of: 01.08.2024

Version history

Version	Date	Remark
1.0	22/04/2016	First valid version (consolidated version for all RL products)
1.1	19/01/2017	Introduction of the alternative connection to SDH/PDH
1.2	05/09/2017	Specification of the certification obligation in accordance with BSI-KritisV (Critical Infrastructure Ordinance)
2.0	26/10/2018	Revision as part of the renewal of the PQ conditions
2.1	20/12/2019	• Adaptation of A02 and B02 as well as chapter 4.6 (notes on spatial distance between redundant data centres). Extension by conception of reserve unit/reserve group (TU) for bundling of micro-installations in C05 • Classification of the information security of the document by the providers in chapter 3.3
2.2	04/11/2020	• Adaptation C04 and figure 3 (option central media break) • Extension C06 for bundling of generation plants at one grid connection point • Extension of chapter 3.3 (Duty to inform in case of changes in IT conception)
2.3	01/03/2022	• Adaptation C06 for bundling of generation plants (maximum capacity) • Extension of chapter 3.3 according to BSI-KritisV 2.0 (duty to inform in case of changes to the IT conception)
2.4	01/05/2023	• Adjustment of A02 with regard to specifications for operation of the systems within the EU • Adjustment of B05 regarding encryption with IPsec VPN or OpenVPN, with AES256 or Wireguard VPN, respectively • Adjustment of CO5 regarding collateralization conditions
2.5	01.08.2024	• Integration of the requirements for interruptible loads (FSV SEAL) • Adaptions in A01, A04, A05, A06, A07, A09, A12, B02, C04

Table of Contents

List of figures

1 Introduction

As the TSOs are responsible for the system, they have to meet generally high requirements as to the confidentiality, the availability and the integrity of their infrastructure as well as of their data. These also apply to all connected infrastructure and service providers. The requirements specified in this document are minimum requirements for security and availability and take account of the legal provisions and requirements of the Federal Office for Information Security.

2 Preamble

2.1 Objectives

This document describes a minimum standard for the requirement of the reserve provider's IT to provide control reserve and providers with interruptible power from interruptible loads (hereinafter referred to as providers) as defined by the German transmission system operators. The aim is to adequately protect the day-to-day operation of the entire system from security threats and to ensure a high availability of the control reserve due to the importance for system security.

This document defines the technical and organisational measures for fulfilling the defined minimum standard. The specific layout of the interface for connecting the provider to the TSO's systems is based on the provisions of the TSO connecting to the reserve. Compliance with this minimum standard, e.g. by implementing the technologies presented in the following figures, does not release the provider from their contractual obligation to the complete provision of control reserve or interruptible loads. At its discretion, the provider can increase the availability of the communication technology and control system by using appropriate IT to fulfil the requirements for one hundred percent availability for the provision of control reserve or interruptible loads in accordance with the relevant framework contracts.

If new statutory regulations or official, regulatory provisions result in a change in the framework conditions for IT, or if operational or security insights require a change to the existing "Minimum requirements for the information technology of the reserve provider for the provision of control reserve or providers of interruptible loads", the TSOs are entitled to unilaterally adapt the "Minimum requirements for the information technology of the reserve provider for the provision of control reserve or providers of interruptible loads". The providers are obliged to implement the new requirements accordingly.

The TSOs reserve the right to audit compliance with the technical and organisational measures by the providers on site or may commission third parties to perform the audit.

2.2 Scope

These requirements are an integral part of the pre-qualification for reserve providers that market control reserve as well as providers that are looking to market interruptible power from interruptible loads (also referred to in German as ‘AbLa’). These requirements also must be complied with during operation.

The connection to the Merit Order List Server (MOLS) of the German TSOs, required for the mFRR, as well as the communication with the German TSOs’ tender platform regelleistung.net are not regulated by this document.

The connection to the Lamas Server of the German TSOs, required for AbLa providers, as well as the communication with the German TSOs’ tender platform regelleistung.net are not regulated by this document.

3 Safety requirements

The German TSOs are tasked with acquiring and using control reserve to specifically counteract power fluctuations in the grid.

The TSOs have defined strict safety requirements based on the obligation to ensure the secure, efficient and reliable operation of energy supply grids in accordance with the Energy Industry Act. These must be applied when providing control reserve to ensure an appropriate level of security of the overall system. The following fundamental values and generic concepts of information security to be protected must be observed[1]:

- **Availability**
  Services, functions of an IT system, IT applications or IT networks or even information are available if these are always available to users as requested.
- **Confidentiality**
  Confidentiality is the protection of information against unauthorised disclosure. Confidential data and information may only be accessible to authorised parties in a permissible manner.
- **Integrity**
  Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. The term integrity expresses that the data are complete and unchanged.
- **Reliability**
  Reliability refers to the IT security objectives of authenticity and non-repudiation. When transferring information, this means that the information source has proven its identity and the receipt of the message cannot be denied.
- **Authenticity**
  The term authenticity refers to the property that ensures that a communication partner is actually who they claim to be. Authentic information is information of which the creation by the stated source has been ensured. The term is not only used when checking the identity of persons, but also for IT components or applications.

[1] Cf. Definitions of the Federal Office for Information Security

- **Non-repudiation**

  The aim is to ensure that the dispatch and receipt of data and information cannot be denied. A distinction is made between the non-repudiation of the origin (it should be impossible for the sender of a message to subsequently dispute the dispatch of a certain message) and the non-repudiation of the receipt (it should be impossible for a recipient of a message to subsequently dispute the receipt of a sent message).

3.1 Minimum requirements for the information technology of the reserve provider for the provision of control reserve or providers of interruptible loads

3.1.1 Overview

The following Figure 1 provides an example overview of the connection of the provider to connecting TSOs.

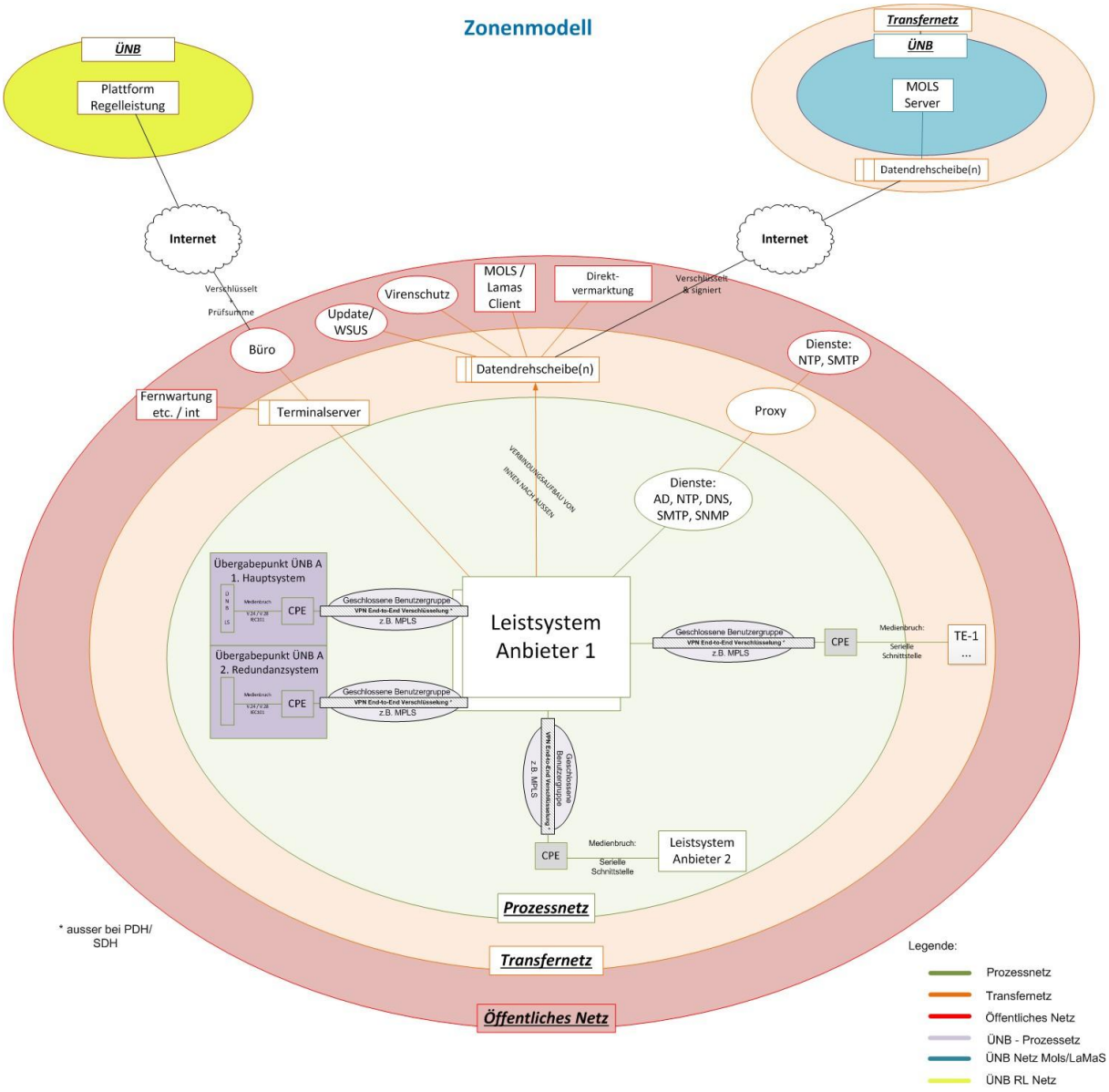

Figure 1: Exemplary and overall overview of the connection of a provider to a TSO

Note: Figure 1 merely intends to illustrate the IT requirements for providers. The professional conception and implementation of the IT requirements is the responsibility of the provider.

The networks presented differ based on the different protection requirements:

- Process network:
  - The network relating to the provider's control systems is called the process network and is the network with the highest protection requirement in the area of the provision of control reserve.
- Public network:
  - All networks outside the process network are referred to as public networks and can potentially be compromised. A secure connection between a process network and a public network can be considered permissible under the requirements described in this chapter with the use of a transfer network.
- Transfer network:
  - The transfer network is an indirect connection possibility between the process network and non-secure networks.
  - The data transfer must essentially be controlled from the process network and take place via data hubs and locks. Files (e.g. award of contract results, scheduling data, MOLS call data as well as software patches, virus patterns, etc.) can be stored on the data hub from the public network and transferred to the process network in a second step.
  - Any data transfer must be additionally secured using adequate virus protection mechanisms.

3.1.2 Basic requirements

The following applies for all requirements described in this document:

- The provider is responsible for the implementation of the requirements. The TSOs reserve the right to verify compliance with the requirements.
- If a provider operates more than one pool for the provision of the same type of control energy and the pools are not operated completely separately from one another (e.g. separate control systems, etc.), the powers of the pools are combined with regard to the minimum IT requirements so that relevant thresholds apply for the entire power provided in the pools for the relevant type of control energy. The number of and which

load-frequency controller (LFR) zones across which the relevant pools may be divided are irrelevant.

- The geographic distribution of the pools connected to the provider's central control system must be described in the IT concept.
- Other power limits not specifically defined by the TSOs (such as the thresholds pursuant to BSI-KritisV) are not affected by this regulation.

3.1.2.1 Reserve provider control system

	FCR	aFRR	mFRR	AbLa
A01	X	X	≥ -50 MW	X *

The provider's central control system must be duplicated. A division into two redundant locations with regard to the infrastructure (communication and power supply) is targeted. The provider must ensure adequate security of its control systems for control reserve. This requirement essentially applies for aFRR, FCR as well as mFRR and AbLA for a marketable power from 50 MW.
* For AbLa, it is recommended for the provider's central control system to be duplicated.

	FCR	aFRR	mFRR	AbLa
A02	X	X	X	X

The operating location of the data centres or control systems used including staff must satisfy the EU's legal requirements regarding data protection and comply with state of the art techniques.

	FCR	aFRR	mFRR	AbLa
A03	X	X	≥ 50 MW	X

An automatic switch between the provider's redundant central control systems must take place within a defined period.

Product	Maximum switch-over time
aFRR	20 seconds
FCR	15 minutes
mFRR (≥ 50 MW per LFR zone)	15 minutes
Interruptible loads	15 minutes

	FCR	aFRR	mFRR	AbLa
A04	X	X	X	X

The delay on the complete transmission route E2E (from the data logging by the technical unit through to the provider control system and the receipt by the TSO) must take no longer than 5 seconds (and no longer than 30 seconds for AbLa).

The requirement applies for aFRR. Similar times must be targeted for FCR and mFRR. The provider specifies the maximum delay time. For AbLa, no more than 30 seconds are allowed.

3.1.2.2 TSO control system/connection

The following Figure 2 provides an example overview of how a provider control system can be connected to a TSO.

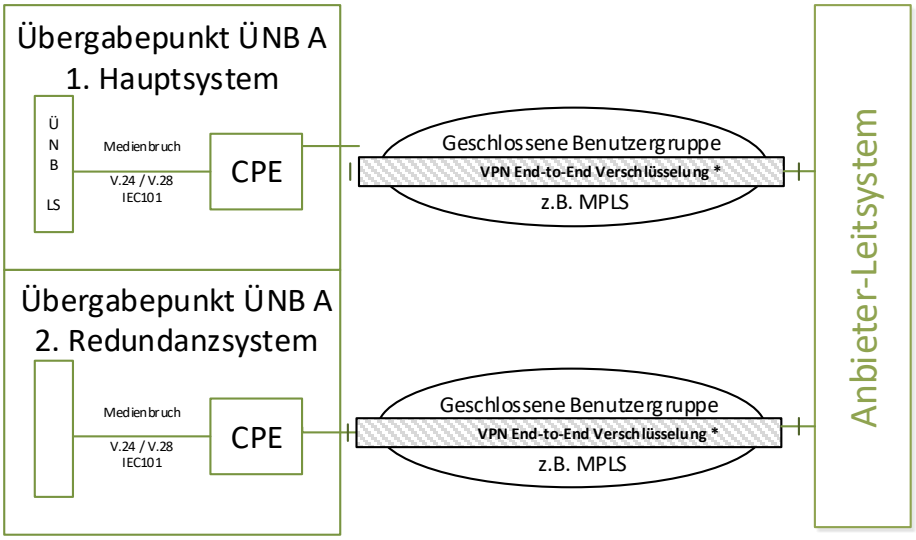

Figure 2: Example overview of the connection of a provider control system to a TSO

The following requirements apply for connecting the provider's control system to the relevant TSO:

	FCR	aFRR	mFRR	AbLa
A05	≥ 50 MW			

Providers must continue to realise the connection between the TSO and the provider's control system with the current point-to-point fixed-line connection (SDH/PDH) or equivalent technologies (see the definition in Annex 3, chapter 5 on the

requirement for closed user groups for providing control reserve).

A06 | FCR ≥ 90 MW | aFRR ≥ 50 MW | mFRR | AbLa

Providers must operate the control system with a local redundancy (see the glossary and annex “Notes concerning the spatial separation between redundant data centres”). Providers who are targeting a marketable power of 50 MW or more per LFR zone should note that the implementation of this requirement is a prerequisite for marketing higher power (≥ 50 MW). The requirement applies for aFRR. A local redundancy should be targeted for FCR and mFRR. If the central control system is required for the compliant provision of the FCR (e.g. for battery management), the control system must have a locally redundant design from a marketable power ≥ 90 MW.

A07 | FCR X | aFRR X | mFRR ≥ 50 MW | AbLa ≥ 50 MW

The connection of the control technology to provide control reserve must take place in the form of a dedicated point-to-point connection between the TSO’s control centre and the provider’s control system. This can be realised by classic fixed-line connections or new technologies. Solutions based on the Internet as the medium are excluded between control systems.

A08 | FCR X | aFRR X | mFRR X | AbLa X

Serial interfaces (V.24/V.28) with IEC protocol 60870-5-101 (TSO-specific) must be used. In consultation with the TSO, X.21 instead of V.24 can be used as the interface format.

A09 | FCR X | aFRR X | mFRR X | AbLa X

The redundant connection of the control systems to the TSO must be realised at the different locations of the TSO.

A10 | FCR X | aFRR X | mFRR X | AbLa X

With regard to the use of Internet technologies (not to be confused with the use of the public Internet excluded under A07), the basic requirements in chapter 3.1.2.3 must be observed.

A11 | FCR | aFRR | mFRR | AbLa
X

The transmission routes and interfaces to the TSO's two transfer points must have a completely redundant design in relation to one another:

- node and edge disconnected,
- no double use of devices and
- no double use of cable routes.

A12 | FCR | aFRR | mFRR | AbLa
X | X | X | X

The individual connection between the TSO's and provider's control systems must at least have an availability of 98.5% (arithmetic total availability of both connections is 99.9775%). The provider nominates the availability per transmission path.

3.1.2.3 Closed user group

B01 | FCR | aFRR | mFRR | AbLa
X | X | X | X

Only closed user groups are permitted in the access networks for the participant connection. The communication between the TUs and control systems must be strictly shielded from other networks (e.g. Internet, networks of other customers or service providers) by using closed user groups. The closed user group should only use private addresses, which cannot be accessed by other networks. The TUs should not be able to communicate with one another, but rather exclusively via the central gateway to the provider's control system.

B02 | FCR | aFRR | mFRR | AbLa
X | X | X | X

The closed user group is exclusively used to provide control reserve. Additional data, which is related to the provision of system services, may be permitted in consultation with the TSO connecting to the reserves (e.g. for the following services: SNMP for monitoring the connected devices, central time synchronization, configuration updates). The provider can use the closed user group for direct marketing. All other IT services must be disabled. Only the participants required

for the provision of the control reserve, such as the provider's control system or the provider's pre-qualified TU, may be included in a closed user group.
In particular, the following systems must not be operated within the closed user group:

- downstream IT systems of the TU operator,
- Office IT systems of the provider or manufacturer and
- IT systems of other providers (relates to SaaS providers).

B03 | FCR | aFRR | mFRR | AbLa
X | X | X | X

The use of Internet technologies (e.g. IP, xDSL, UMTS, LTE) is only permitted when using a closed user group established exclusively for this purpose and provided by the telecommunications provider.
A closed user group established by the telecommunications provider must ensure that the provider's network traffic does not come into contact with "external" networks. The traffic should therefore be secured from the telecommunications provider's other networks, e.g. from other customer networks or the Internet.

B04 | FCR | aFRR | mFRR | AbLa
X | X | X | X

Within the closed user group, the provider (not the telecommunications provider) must establish a separate end-to-end encryption to additionally secure the communication between the TUs and control systems with the closed user group's network.

B05 | FCR | aFRR | mFRR | AbLa
X | X | X | X

The data transferred between the access routers must be transmitted via an encrypted tunnel with an IPsec VPN or OpenVPN, with AES256 or Wireguard VPN, respectively. A recommendation for a secure encryption is described in Annex 3 (Requirement for closed user groups for the provision of control reserve).

	FCR	aFRR	mFRR	AbLa	
B06	X	X	X	X	From a configuration perspective, only other connections within this user group may be reached by a connection within a closed user group. A direct connection to the Internet or the availability of public IP addresses on the Internet or other user groups is therefore excluded. This requirement also includes access points for external service providers and other locations. Communication via VPN or site-to-site connections, which do not belong to the closed user group, is prohibited.
B07	X	X	X	X	The access router must be configured such that all network traffic is routed to the VPN tunnel. Communication outside the tunnel (except to establish the tunnel) is prohibited (including for administration and monitoring).
B08	X	X	X	X	Automated, cyclical monitoring of the router configuration with an integrated alert function (SMS, email) must be ensured. A daily or at least weekly check should prevent any prohibited manipulation of the router.
B09	X	X	X	X	The provider is responsible for applying for a connection and a closed user group with the telecommunications provider. The associated contract must be concluded between the reserve provider and the telecommunications provider. Contracts where the telecommunications provider grants itself the right to temporarily interrupt the connection on a regular basis, e.g. after 24 hours, must be excluded.
B10	X	X	X	X	The provider is obliged to only select telecommunications providers that promptly inform the provider of planned maintenance work in advance. Irrespective of this, the reserve provider must take precautions for this case in order to meet

its obligations to provide control reserve or interruptible loads (e.g. via redundant connections or suspension of marketing).

	FCR	aFRR	mFRR	AbLa
B11	X	X	X	X

All transmission routes must be encrypted. This requirement does not affect point-to-point connections with a serial design. These do not require any encryption.

3.1.2.4 TU connection, media break

The following Figure 3 provides an example overview of the connection of various TUs to the provider's control system.

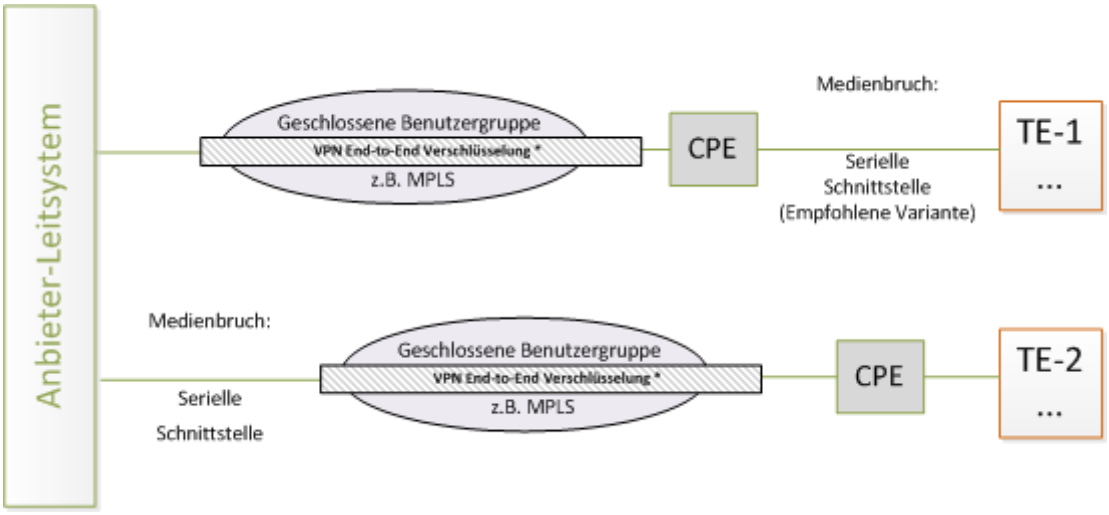

Figure 3: Example overview of the connection of TUs to the provider control system

The following requirements apply for connecting the TU to the provider's control system:

	FCR	aFRR	mFRR	AbLa
C01	X	X	X	X

Every TU must be connected to the provider's control system with an availability of the individual connection of at least 95%. (Evidence can be provided by contracts, by the system or via statistics). If the provider operates locally separated control systems based on requirement A06, the TU is

connected to each of the two control systems (potentially also redundant per control system as per C02 / C03).

C02 | FCR | aFRR ≥ 30 MW | mFRR | AbLa

TUs shall also be redundantly connected to the provider control system. This requirement must be targeted for TUs that provide mFRR or FCR.

C03 | FCR | aFRR ≥ 50 MW | mFRR | AbLa

TUs that provide 50 MW aFRR must continue to be connected with the existing, redundant point-to-point fixed-line connection (SDH/PDH) or equivalent technologies (see the definition in Annex 3, chapter 5 on the requirement for closed user groups for providing control reserve).

C04 | FCR | aFRR | mFRR | AbLa
X | X | X | X

The TU must be connected via a media break. The media break concerns the interruption of the Internet protocol (IP) and is mandatory. The media break can, for instance, be established via a serial interface. The media break can be implemented locally at the TU (recommended variant) or centrally at the control system. Alternatively, the direct control of TUs via binary or analogue outputs (e.g. switch actuators) as well as the direct recording of measured values using binary inputs or AD converters is also permitted.

C05 | FCR | aFRR | mFRR | AbLa
X | X | X | X

Concept for bundling of small TUs

- Bundling of small TUs via public Internet with encrypted VPN is allowed.
- For bundling of small TUs, closed user groups are not obligatory.
- If small TUs are bundled via the Internet, the provider must demonstrate, e.g. by means of a penetration test, that the bundling is operated securely in accordance with the state of the art.

- A serial interface must be implemented as a media break between bundled small TUs and the pool operator in accordance with IT requirements.
- The installed capacity of a small TU may not exceed 100 kW.
- The marketed capacity of a bundle of small TUs may not exceed 10 MW.
- The connection of a micro-installation (small TU) is only permitted to a pool (no multiple sales possible).
- Within a bundling of small TUs, no small TUs for outage backup can be used. However, this outage backup cannot compensate for the outage of the entire bundle.
- Within a bundling of small TUs, an aggregation of small TUs is allowed, which are then integrated in the bundling of small TUs, as long as the maximum marketed capacity of the bundling of small TUs is not exceeded. Each aggregation can only be connected to a bundling of small TUs via internet using VPN. This aggregation only applies to the communication channels, not to the data points.
- The requirements from D02 (fault clearance within 24 hours) do not apply to individual small TUs, but to the entire bundle of small TUs.

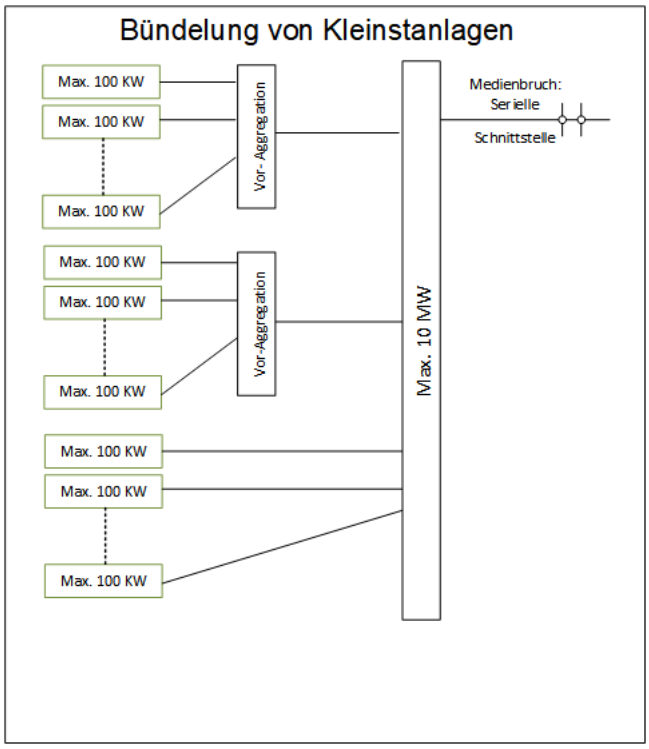

Figure 4: Example overview of a bundling of small TUs

C06

FCR	aFRR	mFRR	AbLa
X	X	X	X

Bundling of power plants (generators and/or consumers) at a common grid connection point

- TUs that are connected via a common grid connection point, can be understood as one TU in the sense of this IT concept. For this bundling, only one communication link to the provider control system is required.
- The redundancy requirements from C02 and C03 must be considered accordingly.
- These bundled power plants are treated as one TU for collateralization purposes.
- Within the bundling of power plants, own networks without public Internet must be used.
- The use of the serial interface according to C04 is still required.

3.1.2.5 Additional requirements

D01

FCR	aFRR	mFRR	AbLa
X	X	X	X

Data transfers from and to other networks with a different protection requirement essentially take place with data hubs. Data hubs ensure that data can be transferred between the network used for provision and the other networks with a lower protection requirement without establishing a direct connection between these networks.

- Only unidirectional communication from the control system is permitted, i.e. data can only be exported or retrieved from the control system's network.
- Exclusive use of SFTP or comparable, encrypted protocols.
- Multi-stage virus protection on the data hub.

D02

FCR	aFRR	mFRR	AbLa
X	X	X	X

Faults on parts of the overall system without a complete failure, i.e. without impairing the provision, must be rectified by the provider within 24 hours after the occurrence of the fault. If the fault does not occur on a working day, troubleshooting on the next working day is considered adequate.

D03

FCR	aFRR	mFRR	AbLa
X	X	X	X

The provider must ensure the continuous and seamless monitoring of the availability of the transmission paths, including all CPE.

D04

FCR	aFRR	mFRR	AbLa
X	X	X	X

Adequate access and entry protection shall be provided to premises, systems, and networks necessary to provide the control reserve. (E.g. access and key concepts, authorisation management and physical security measures in conjunction with adequate instruction and controls.). Electrical operating rooms must be locked. The provider's devices must also be

housed in a sealed safety cabinet secured by an alarm. This requirement does not apply for small TUs according to C05.

D05

FCR	aFRR	mFRR	AbLa
X	X	X	X

The provider must operate an integrated patch and change management, demonstrate this as part of the pre-qualification and document the relevant processes. Updates are transferred via the data hub principle (see D01) independent of the type of system to be updated (operating system, application, virus signatures, etc.). In this case, the data are always retrieved by the servers located in the secure zone. The data are therefore reviewed on every system (e.g. for malware, standard conformity and plausibility).

D06

FCR	aFRR	mFRR	AbLa
X	X	X	X

All measures (technical concept, routing, fault clearance times, maintenance contracts, etc.) to achieve the required availability must be presented to the TSO upon request.

D07

FCR	aFRR	mFRR	AbLa
X	X	X	X

If technologies are compromised, the provider is obliged to notify the TSO. If the TSO becomes aware of a compromised technology, the provider must repair the compromised technology upon request. In this case, alternative technologies must be implemented within a transition period arranged with the TSO.

3.1.2.6 External IT service providers

D08

FCR	aFRR	mFRR	AbLa
X	X	X	X

Providers that procure services from external IT service providers that, in turn, offer their services to several providers (e.g. SaaS providers) are subject to special regulations:

- The procurement of services from the aforementioned IT service providers must expressly be disclosed as part of the pre-qualification and approved by the TSO.

- Providers that procure these kinds of services are essentially treated as providers with the highest protection requirements (such as aFRR ≥ 50MW).
- IT service providers that provide services for various providers and their associated providers must ensure that the operation of jointly used components does not present any risks for other providers. For example, only one provider may be connected per closed user group.
- The provider is the main contact partner for the TSO and bears overall responsibility for fulfilling the IT requirements to provide control reserve.

3.2 Notification obligations and verifications

The provider must verify the security of its overall E2E system (bidirectional data exchange between the technical unit to the TSO via the provider control system) as defined in chapter 3.3. The following requirements must be ensured:

- The provider must verify the technical contractual content on IT security and availability with the TSO or a commissioned third party (for example, this can take place in the form of an inspection of the relevant text passages for existing contracts).
- The provider must demonstrate the existing risk or basic protection analyses with the TSO upon request.
- The provider must demonstrate the conceptual planning and implementation of IT security measures with the TSO upon request (also on-site if necessary). The provider must immediately notify the TSO of security-related changes and security incidents in the overall system.
    - Security-related changes may include: changes to the configuration of the VPN tunnel, change of the router hardware model, conceptual changes, etc.
    - Security incidents include: awareness of weaknesses in the router configuration or router firmware, unauthorised third-party access, attacks on the access router or downstream systems, etc.

- The provider must immediately inform the TSO if the data provision to the TSO cannot be properly ensured.
- The providers must record the following information to check the reliability and report to the TSO, particularly in case of an error or upon request:
    - Frequency and duration of the faults
    - Causes of the faults
    - Switch-over time to redundancy connection
    - Time until the rectification of the faults
    - Measures taken to limit and eliminate the fault
    - Measures to prevent the error in the future
- The TSO communicates changes to the IT requirements on the internet platform regelleistung.net to the providers accordingly.
- If necessary, the concepts must be adapted accordingly by the provider in consultation with the TSO.
- Changes to the IT concepts must be presented to the connecting TSO for review before the start of implementation.
- To support a regular adaptation of the IT requirements, the provider is asked to provide an annual report on the operation of the IT systems used to provide the control reserve or interruptible loads to the relevant connecting TSO on 31/01 each year for the previous year (see Annex 4 “Provider report on the provider’s information technology and incidents while providing control reserve or interruptible loads”).

3.3 Self-disclosure and verifications

The provider confirms, within the scope of self-disclosure (see below) and verifications (see chap. 3.2), that the existing minimum requirements for the provider’s information technology for the provision of control reserve or interruptible loads are complied with. The self-disclosure must be signed by the managing director or an authorised representative of the provider.

As part of the pre-qualification, the provider must submit the following documents to check the IT requirements for providing control reserve or interruptible loads:

- Submission of a comprehensive IT concept (without specification of any operational relevant information such as an IP address)

- IT checklist with assignment of the corresponding chapters of the IT concept including the description of the encryption technology as well as a list of the involved telecommunication service providers or Software as a Service providers (see Annex 1: Checklist for the minimum requirements for the information technology of the reserve provider or provider of interruptible loads for the provision of control reserve)
- Classification of the information security of documents submitted by the provider

Changes to the IT concepts (even without impact on the pre-qualified service) must be submitted to the TSOs for approval prior to use.

Providers, service providers for the provision of control reserve and IT system service providers that bundle units or systems for the control and bundling of generation and consumption equipment with a net nominal output of at least 104 MW (36 MW in the case of pre-qualification for the provision of primary control reserve) in Germany are subject to mandatory certification in accordance with BSI-KritisV 2.0 as from 14/09/2021. In this case, verification is required by way of a certification pursuant to the provisions of the BSI, the IT Security Act and BSI-KritisV as well as based on the IT security catalogue in accordance with Section 11 (1a) EnWG or pursuant to an IT security catalogue in accordance with Section 11 (1b) EnWG.

As was already the case in the consultation version of this document from April 2018, the TSOs do not require a mandatory certification of all providers until further notice. The requirements described above are legally prescribed minimum requirements, which provide for a certification obligation from an installed nominal capacity of 104 / 36 MW (electrical).

The minimum requirements formulated in this document are complemented by the following annexes (see the regelleistung.net platform):

- Checklist for the minimum requirements for the information technology of the reserve provider or provider of interruptible loads for the provision of control reserve
- Requirement for closed user groups for the provision of control reserve or interruptible loads
- Report on the information technology of the reserve provider or provider of interruptible loads and incidents during the provision of control reserve

- Notes concerning the spatial separation between redundant data centres[2]

[2] See Notes concerning the spatial separation between redundant data centres: https://www.regelleistung.net/de-de/Infos-f%C3%BCr-Anbieter/Wie-werde-ich-Regelenergieanbieter-Pr%C3%A4qualifikation

4 List of abbreviations and glossary

Term/abbreviation/clause	Explanation
AbLa	Interruptible loads
AD	Active directory
aFRR	Automatic frequency restoration reserve (formerly SRL)
BSI	Federal Office for Information Security
Change management	Process for authorising and documenting changes to the IT infrastructure and applications to keep unwanted impacts on ongoing operation as low as possible.
CPE	Customer premises equipment is the equipment of the reserve provider or provider of interruptible loads for control power as a grid connection and transmission interface
DNS	Domain name system
DSL	Digital subscriber line
E2E (End-to-End)	Transmission route from the technical unit to the TSO's control system via the reserve provider control system
FCR	Frequency containment reserve (formerly PRL)
Overall system	All components necessary for service provision/fulfilment of contract
Closed user group	Connections in the access network provided by a telecommunications provider, which are operated by this provider in a closed system. These may be connections to different transmission networks, such as DSL/UMTS/GSM/LTE, etc. Communication with connections outside this closed user group, e.g. to the Internet, must be excluded. A contract generally has to be concluded with the relevant telecommunications provider to set up these closed user groups.
GSM	Global system for mobile communication
IP	Internet protocol
IT	Information Technology

KRITIS	Critical infrastructure
LS	Control system
LTE	Long term evolution
mFRR	Manual frequency restoration reserve (formerly MRL)
MPLS	Multiprotocol label switching
NTP	Network Time Protocol
Patch management	Area of system management for procuring, testing and installing patches.
PDH	Plesiochrone digital hierarchy (circuit-switching transmission system)
Redundancy (control system)	In the case of local redundancy, at least two locations are independent from the other location • Energy supplies and • communication connections. A fault in one location must not affect the other location (also refer to the notes on the distance between data centres in Annex 4 Notes concerning the spatial separation between redundant data centres).
Redundancy (transmission route)	Redundancy during data transmission is defined as follows: • node and edge disconnected • no double use of devices • no double use of cable routes
RU	Reserve unit
RG	Reserve group
SaaS reserve provider	Software as a service reserve provider
SDH	Synchronous digital hierarchy (circuit-switching transmission system)
SFTP	Secure file transfer protocol
SMTP	Simple mail transfer protocol
SNMP	Simple network management protocol
SO GL	System Operation Guideline

SÜFV	*Sicherheitsüberprüfungsfeststellungsverordnung*, Security Screening Ordinance
SÜG	*Sicherheitsüberprüfungsgesetz*, Security Screening Act
TU	Technical unit(s) or interruptible load
UMTS	Universal mobile telecommunication system
TSO	Transmission System Operator
VPN	Virtual private network Connection between two “private” network segments that is established via a network operated by a third party.
WSUS	Windows server update services

Self-disclosure on the "Minimum requirements for the information technology of the reserve provider or provider of interruptible loads for the provision of control reserve"

_____ (name of the reserve provider or provider of interruptible loads) as the provider for control reserve hereby declares that it satisfies the "Minimum requirements for the information technology of the reserve provider or provider of interruptible loads for the provision of control reserve", from 01/08/2024 as amended, prepared by the German transmission system operators (TSOs) for the duration of the framework contract.

Name and address of the reserve provider or provider of interruptible loads:

Place and date: ……..

Signature (managing director or authorised representative): ……..