Fingrid Oyj

Requirements for the Reliability of Reserve Provision

30.9.2026

1 Introduction

The purpose of this document is to define reliability requirements related to the reserve provision. The document covers requirements related to e.g. cybersecurity, redundancy of central functions, and exception management. The general technical requirements and the required prequalification tests are defined in the following documents:

- *The technical requirements and the prequalification process of Fast Frequency Reserve (FFR)*
- *The technical requirements and the prequalification process of Frequency Containment Reserves (FCR)*
- *The technical requirements and the prequalification process of Automatic Frequency Restoration Reserve (aFRR)*
- *Technical requirements and prequalification process for the Manual Frequency Restoration Reserve (mFRR)*

The documents are available on Fingrid's website, see the attachments on the product specific pages.

The reserve provider is responsible for its own reserve units and systems. Compliance with the terms of this document therefore does not automatically ensure that, for example, an insurance company's contractual terms concerning physical or cybersecurity are fulfilled.

The process and system descriptions required later in this document are primarily intended for the reserve provider's own use, unless they are separately required as part of the application form. However, Fingrid may agree with the provider on a separate audit if it is considered necessary. In cases where a description is required as part of the application form, the given requirements define the minimum scope of the description. An example of such a case is subsection 3.1.1, which concerns the description of the architecture of centralised control systems.

For justified reasons, Fingrid may grant a transition period for the implementation of the requirements set out in this document or grant exceptions to individual requirements. An example of such a case is granting a transition period for implementing video surveillance in connection with the renewal of prequalification tests.

1.1 Abbreviations and definitions

Definitions:

Centralised control system: A system that transmits power commands to the providing entities under its control.

Centralised trading system: A system that transmits information about allocated reserve capacity to locally controlled units. These systems are related to FCR-N, FCR-D and FFR reserves.

Operational party: The reserve provider or an authorised representative, such as a service provider, that can modify the providing unit's bids, monitor activation, change the control status of the providing unit, and initiate fault investigation when necessary.

Providing entity: An entity that meets the requirements for providing reserve. A providing entity may consist of one or several providing units.

Providing unit: An individual controllable resource, such as a power plant, consumption site or energy storage facility.

Reserve provider: Fingrid's contractual counterparty that offers, maintains and activates reserve.

IT support: IT support refers to the party that has the necessary knowledge and competence to maintain the entire service being provided, to isolate, resolve and correct problems. IT support may be internal, external or consist of several parties. What is essential is that the party providing the service has agreed responsibilities, service levels and service hours for the service being provided, and that these are consistent and aligned, especially when several parties are involved in the service. IT support must cover all components, hardware, applications and licences essential for providing the service.

Multi-factor authentication: Authentication is verified using at least two different authentication methods. Further information is available on Traficom's website under the topic "multi-factor authentication".

Hardening: Hardening a device or information system refers to measures taken to minimize its attack surface. These include removing unused services and accounts, tightening default security settings, regularly applying security patches, and following various manufacturer recommendations and guidelines.

1.2 Implementation of requirements

For new providing entities, the requirements enter into force on the date stated at the beginning of the document. For units approved before validity date of this document, the requirements enter into force at the time of renewal of their prequalification or, at the latest, within five years of the entry into force of this document. If the operation of a providing entity is dependent on a centralised trading or control system, these systems become subject to the requirements during the unit's prequalification process (initial or renewal of prequalification) or during the market approval process.

2 General reliability requirements

This chapter covers general reliability requirements for reserve provision. The requirements apply to all reserve products and to all reserve providers, as well as to their service providers.

General requirement 1: The provider is responsible for ensuring that the reserve unit is performing according to the specified requirements when it is used to maintain reserve.

General requirement 2: The operational party of the entity must be reachable by phone whenever the reserve provider has valid and binding bids.

General requirement 3: The maintained reserve behind a single point of failure (incl. both capacity and energy markets) can be at most:

- 50 MW of FFR reserve
- +/-70 MW of FCR-N or FCR-D reserve
- +/-70 MW of aFRR reserve

- A total of +/-100 MW of FCR-N and FCR-D reserve
- A total of +/-200 MW of FCR-N, FCR-D, FFR, aFRR and mFRR reserve
- In addition, the following restriction applies to entities that are part of the Olkiluoto 3 system protection scheme:
  - A total of 70 MW of FFR reserve and Olkiluoto 3 system protection scheme capacity.
  - A total of +/-200 MW of FCR-N, FCR-D, FFR, aFRR and mFRR reserve and Olkiluoto 3 system protection scheme capacity.

If the provision of reserve has been implemented so that there is no single point of failures that could prevent maintaining of the reserve in its entirety, there is no upper limit for the maintained reserve. This can be achieved, for example, through system redundancy. Matters to be considered here:

- Examples of single point of failures include: electrical fault, control system failure, equipment failure or telecommunications outage.
- The reserve provider is responsible for the fault tolerance of the service provider.
- Redundancy must not be based solely on duplicating functions within the same hardware.
- The sufficiency of redundancy is verified by reviewing the implementation separately with Fingrid and having it approved by Fingrid.

Guidance for interpreting the redundancy requirement:

- In the case of mFRR, the redundancy requirement is considered fulfilled between Fingrid and the reserve provider if Fingrid can activate bids by calling the reserve provider's control room. A phone call is also considered a sufficient redundancy measure between the reserve provider's control room and the reserve unit if activations normally take place via another route.
- The redundancy of electrical components (such as transformers, meters and current paths) is assessed from the reserve unit up to the connection point of the licensed electricity network.
- The provider's own connecting line to the licensed grid does not need to be redundant in the case of aFRR and mFRR reserves, but redundancy is required in the case of FFR and FCR reserves.

General requirement 4: The reserve provider is responsible for planning the trading and maintenance of reserve so that it is technically possible. When maintaining reserves, it must be ensured that power and energy capacity reserved for other reserve products or other purposes is not offered to the market twice.

2.1 Physical and cybersecurity

2.1.1 Cybersecurity

The requirements outlined in this section aim to establish a set of controls in which security do not rely on a single component, but on a layered approach where the failure of one component would not yet enable a complete compromise of the system.

Requirement 1: General practices and geographical location. Physical and cybersecurity must be at a level that is in line with good industry practices, such as following the practices of the NIS2 Directive, CRA or ISO27001 standard and the General Data Protection Regulation (GDPR). Examples of good industry practices include training personnel, continuous improvement of operations, assigning clear responsibility for security, comprehensive risk management, and obtaining approval from the company's management for the operating models used. The ISO27001 standard significantly helps in meeting compliance requirements arising from various regulations, although official certification is not a mandatory requirement for suppliers. In addition, as regulation increases and providers' services may expand, they may in the future meet the criteria of NIS2 or CRA even if they do not yet meet them. Additionally, the trading and control systems must be geographically located within the internal market area of the European Union.

Requirement 2: Strong authentication. Multi-factor authentication must be in place for all users before access to components of the control or trading system is granted. IP restrictions must allow only connections that are necessary for the operation and must be implemented whenever technically feasible. This limits unnecessary exposure to malicious traffic from the internet by restricting access to trusted IP addresses that require it and that are reviewed regularly. Strong authentication may be omitted only if other compensating restrictions have been taken into account, such as traffic not passing through the internet but through a completely separate connection, and user groups being limited to administrator and user groups through RBAC (Role Based Access Control), where user groups have only read rights or appropriately limited modification rights.

Requirement 3: Logging and monitoring. Logs must be collected from access management systems, jump hosts and system application events and stored on a separate log management server. The logs must show logins related to the system, application errors, actions performed by users and access management events, so that it can be traced which accounts have performed which actions or which data has been compromised. Logs must be retained for at least 6 months. Logs from critical and essential services must be monitored 24/7/365, and responses must be carried out in accordance with their criticality.

Requirement 4: Access rights. Access rights are limited according to individuals' work tasks, and their necessity is monitored regularly. The roles formed in this way must have a lifecycle with a clear beginning and end, and they are extended when necessary. No account should remain valid indefinitely, and the recommended review interval for accounts and roles is less than one year. Exceptions include the so-called emergency account and a read-only or restricted account intended for monitoring use. These

accounts do not have to have a predefined expiry date. The emergency account must be used only in emergency situations, for example when logging in with other accounts is not possible during system recovery or installation. The passwords for this account, and all other accounts, must be forced to be long random strings of more than 15 characters, including special characters. Use of the emergency account must trigger an alert to administrators. In addition, this account and the account used for monitoring and control-room purposes may be the only accounts that do not require strong authentication. The password for this account must be kept in a password vault and covered by backup arrangements or stored in a safe. Other shared accounts must not be allowed without approval from the provider's management.

Requirement 5: Remote access and management connections. Remote access must be limited to functions where it is necessary for the operation, and strong authentication (MFA) must be enforced. As a rule, the management connection must not be open to the internet. If it must be opened to the internet, access must be restricted by IP filtering to only the IP addresses required for the operation, and IP restrictions must be implemented whenever technically feasible. As a strong recommendation, management connections should be used only through jump host connections, which aim to break the direct connection from the user's machine to the target and thereby limit the direct use of unauthorised applications or functionalities through the remote connection. This requires that only necessary applications confirmed as secure are installed on the jump host, and that it has up-to-date endpoint protection software, continuously updated components and operating system, as well as log collection and monitoring.

Requirement 6: Updating and hardening. All system components must be updated regularly from the manufacturer's site, and their vulnerabilities must be monitored regularly. All components connected to the internet must be updated without delay if high or critical vulnerabilities have been identified in them. Records of components must be maintained, such as an SBOM (Software Bill of Materials), so that it is known which products and versions must be specifically monitored and updated. Traficom's vulnerability advisories are one example of a useful monitoring source. Note: Devices isolated from the internet, or devices well protected through IP restrictions, significantly help prevent the exploitation of critical vulnerabilities. Device configurations must be hardened in accordance with the equipment manufacturers' instructions and kept up to date.

Requirement 7: Encryption. All API or management connections between the system itself and external systems must use either TLS v1.2 or TLS v1.3 protocol, and AES256 or stronger AES encryption. In symmetric encryption, an algorithm based on SHA-2 must be used for both key exchange and the protection of IKE messages and SA lifetimes and renegotiation intervals must be: IKE-SA < 24 h and IPsec-SA < 4 h. The encryption key must be more than 15 characters long and consist of completely random characters and special characters (typically applies to VPN connections). When certificates are used, weak encryption algorithms (cipher suites) must be removed, and Traficom's recommendations for secure encryption algorithms may be used as guidance. If the above encryption requirements are too demanding for the device, a separate device must be selected to perform the encryption, such as a VPN device, or the device's most secure available encryption algorithm must be used, or the device must be replaced with a newer

one that is capable of better encryption. IP restrictions must also be set for these connections so that only connections necessary for the operation are allowed, and this must be implemented whenever technically feasible. The provided must also consider the new algorithms introduced by the PQC (Post-Quantum Cryptography) transition and have an approved plan for their implementation. Guidance on quantum-safe encryption methods is available on Traficom's website.

Requirement 8: Internet connections. Controlled devices, or other critical devices, must not have direct connections to the internet by default. Only separately defined outbound connections that are necessary for system operation are permitted; in other words, they must be whitelisted and otherwise blocked by default. Whitelisting means only trusted destinations, such as the device manufacturer's update sites and other connections and protocols necessary for the operation. This aims to prevent unauthorised connections from the device to malicious destinations.

Requirement 9: Endpoint protection. Management and remote connections as well as jump hosts must have up-to-date endpoint security protection that logs and alerts on anomalies at all times of day. These alerts must be monitored and responded to according to the criticality of the anomaly. Endpoint protection must be in place on all essential components through which the system can be accessed. If it cannot be installed, alerts and logging must be arranged in another way so that deviations from normal operation can be detected.

Requirement 10: IR (Incident Response) process. An incident response process must exist, be documented and be approved by the provider's management. It must be kept up to date as systems change and in accordance with good practices. Customers potentially affected by incidents must always be informed of critical or serious incidents. The same obligation also applies towards National Competent Authority, as defined under NIS2 or the CRA.

2.1.2 Physical security

This subsection addresses physical security requirements for control and trading systems as well as for individual providing units. Providing units whose product-specific approved reserve capacity is less than 10 MW are outside the scope of the requirements outlined in this section. For these units, however, the requirements presented in this section are recommendations. The same limitation and recommendation also apply to centralised control and trading systems.

For smaller sites, ready-made integrated solutions may be used, including alarms, camera surveillance and a remote connection to the control room. For high-risk or extensive premises, a separate guarding contract and preparation of a plan in cooperation with a security planner are always recommended to ensure a high-quality outcome.

If the requirements presented in this subsection cannot be implemented appropriately for the protected site, the provider may, for a justified reason, apply for an approval of an alternative solution from Fingrid. The exception must be justified from risk management perspective and documented.

If the site is located in an industrial area or a comparable environment, existing solutions intended for perimeter management and area surveillance, such as fencing, access control and camera surveillance, may be used as part of the site's protection. These solutions may be managed by the owner of the area or by another operator. Natural obstacles, such as water areas or rock cuttings, may be considered in perimeter protection planning if it can be justified that separate fencing is not necessary. Requirements related to the site's outer perimeter protection, internal area protection and asset protection must be fully implemented.

Requirement 1: Intruder alarm system. An intruder alarm system must be installed at the sites and must meet the following requirements:

- The system must monitor the doors of critical areas and the building perimeter. Doors must be equipped with detectors that identify when door is opened or left open.
- The alarm system must be connected to a security control centre operating 24/7. Alarms must generate an immediate notification to the security control centre, where response takes place in accordance with separately agreed alarm instructions.
- A security control centre means an operating unit where alarms generated by the intruder alarm system are continuously monitored and responded to in accordance with a predefined alarm procedure.
- The measures to be taken after a possible break-in must be agreed and documented precisely with the guarding company. The operation of the systems must be retested, and the protected site must be inspected by an expert for possible sabotage or external devices connected to the protected site.

Requirement 2: Window protection. Ground-floor rooms with windows must be equipped with intrusion detection devices that detect attempted intrusions and acts of vandalism through the windows. The detectors must be connected to the intrusion alarm system.

Requirement 3: Camera surveillance. Sites must have a functional camera surveillance system. Minimum requirements for the system:

- All entrances must be covered by camera surveillance.
- Recordings must be retained for at least 30 days.
- The system must provide a real-time remote connection to the control room.

Requirement 4: Ensuring the functionality of systems. The operation of intruder alarm and camera surveillance systems must be inspected regularly:

- Comprehensive testing of the systems, including detectors, connections and alarm transmission, must be carried out at least once a year.
- Fault situations and deficiencies must be corrected without delay.

In addition to the requirements above, it is recommended that the sites burglary protection is implemented in accordance with Finanssialan rakenteellinen murtosuojausohje II or III.

2.2 Detection of disturbances and response capability

Requirement 1: Information about a communication interruption must be sent to the unit's maintenance organisation/operator, and the interruption must be responded to.

Requirement 2: Monitoring must cover at least the following areas:

- The status of reserve unit's and the implementation of reserve control
- Connections between the control system, the reserve unit and the metering devices
- Alarms related to cybersecurity and physical security, and responses according to the criticality of the alarms and logs.

Requirement 3: A description of the response to possible disturbances and the related response and repair times. The description must consider that there may be several types of fault events, such as a communication interruption, power outage, device freeze or complete device failure.

Requirement 4: The response and repair time must be reasonable in relation to the harm caused by the disturbance.

Requirement 5: A description of fault tolerance testing. Testing is described in the processes and is carried out at regular intervals, for example according to an annual schedule or in connection with updates.

3 Requirements for systems of reserve provider and reserve unit

The reliability requirements presented in this section relate to the properties of centralised control or trading systems and to their operation during abnormal conditions.

3.1 Requirements for centralised control systems

This section addresses more detailed reliability requirements related to centralised control systems. A centralised control system transmits power commands to the providing units within its scope. These power commands are calculated in the control system based on trading data, frequency measurement (FFR and FCR), and activation signals (aFRR and mFRR).

3.1.1 High-level description of the system architecture

Requirement 1: The description must show the significant components of the system and the data flows between them.

Requirement 2: The description must show the placement of the different parts of the system (own server, AWS, Azure, etc.).

Requirement 3: The description must show the interfaces to the centralised control system as well as their users and remote connections (operator, customer, etc.).

Requirement 4: The factors affecting the delay between frequency measurement and activation of the unit must be clearly visible in the description.

3.1.2 Control system redundancy:

Requirement 1: At least three frequency meters are required within the same bidding zone if the combined product-specific approved reserve capacity of the reserve units under the control system exceeds 10 MW. The requirement applies to systems used to maintain FCR or FFR.

- In addition, the frequency meters must be geographically distributed and independent of a single electrical fault.
- If the connection between the meter and the control system is implemented wirelessly, the connection must be redundant. Redundancy may be implemented by using several telecommunications operators per meter or by distributing the meters across the networks of several telecommunications operators.
- If frequency measurement is procured from a service provider, the service provider must meet the same requirement if the combined approved product-specific reserve capacity of the providers using its frequency measurement exceeds 10 MW.

Requirement 2: If data transmission takes place using mobile network data connections, such as 4G/5G networks, the provider must use a separate APN connection available from operators, which separates the connections from the public internet and creates a dedicated mobile connection for the provider that is more secure than public internet connections. Another alternative to an APN is a separate security device that performs NAT (Network Address Translation) and where incoming connections are restricted by IP filtering to allow only connections necessary for the operation. These must be implemented whenever technically feasible.

In addition to the requirements above, it is recommended to make the connection between the reserve unit and the control system redundant.

3.1.3 Segmentation:

Requirement 1: Frequency measurement may only control units located in the same bidding zone.

Requirement 2: A separate centralised control system is required for each bidding zone.

3.1.4 Control system IT support

Requirement 1: IT support must be available whenever the reserve provider has valid binding bids.

Requirement 2: A governance model description approved by the provider’s management, as well as a preparedness and recovery plan, must exist for critical and important services.

3.2 Requirements for centralised trading systems (FCR and FFR reserves):

This section addresses more detailed reliability requirements related to centralised trading systems. A centralised trading system transmits information about allocated reserve capacity to locally controlled units. The system does not transmit power commands; instead, the activated power according to the trades is calculated locally at the providing units based on their frequency measurement and the trading data transmitted by the system.

3.2.1 Sending trading data to the reserve unit

Requirement 1: The data must be sent no later than 3 hours before the delivery period. It is recommended that trading data for the entire following day is sent at once.

Requirement 2: Alternatively, trading data may be sent later if its receival is manually verified from the unit's control room.

If the provider is unable to meet requirement 1 or 2, it may apply to Fingrid for approval of an alternative solution. For example, requirement 2 may be considered fulfilled by the following solution: the providing unit sends an notification of capacity acceptance to the unit's control room. A missing notification message, or information about failed receival of information, triggers an alarm in the control room and is responded to.

3.2.2 Trading system IT support

Requirement 1: IT support must be available whenever the reserve provider has valid binding bids.

Requirement 2: A governance model description approved by the provider's management, as well as a preparedness and recovery plan, must exist for critical and important services.

3.2.3 Operation of providing units at a time of communication interruption

Requirement 1: There are two alternative approaches for the operation of a providing unit during a communication interruption, listed in recommended order:

1. The unit continues using the trading data already received, for example until the end of the day, and then changes the maintained reserve capacity to 0 MW.
2. The unit continues reserve provision by using the trading data in force at the time of the communication interruption until instructed otherwise.

If the provider is unable to implement either of the alternatives provided, it may apply to Fingrid for approval of an alternative solution. The implementation must also consider any more detailed guidance in the grid code requirements concerning operation during communication interruptions.