Federatie van de elektriciteits- en gasnetbeheerders in België
Fédération des gestionnaires de réseaux électricité et gaz en Belgique

C8/07

Explanatory note

aFRR – business processes

1 Introduction

This explanatory note C8/07 explains the aFRR project context and has to be considered as a supporting document to the Synergrid C8/06 (General technical requirements measurement system and gateway for an aFRR service delivery point connected to the distribution grid) for better understanding.

2 Glossary

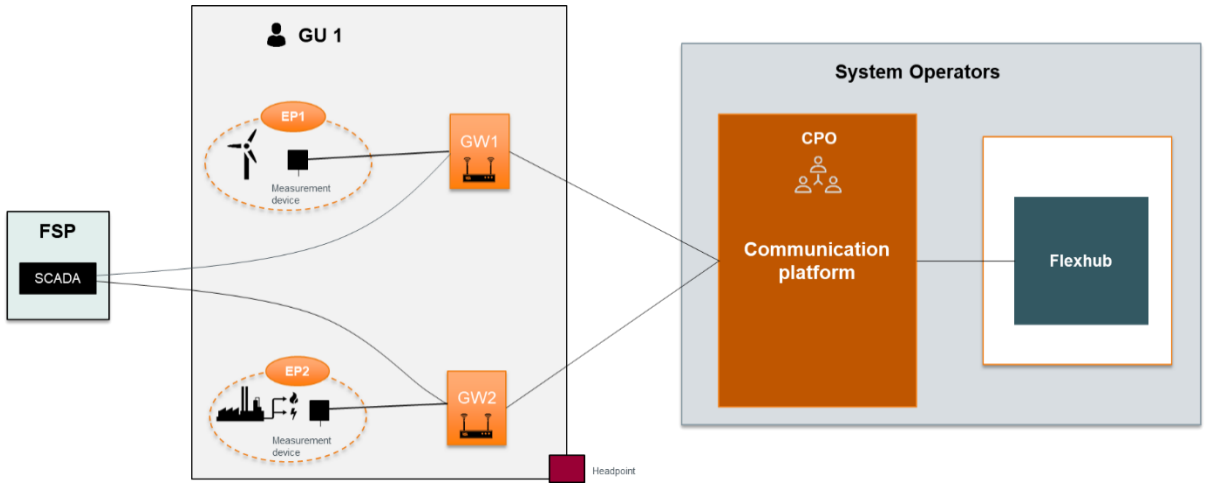
The definitions below are non-binding but are given to correctly interpret the context of this document's content and C8/06. In case of inconsistent definitions or contradictions between this document and the T&C (terms and conditions) BSP aFRR, the latter prevails.

Concept	Definition
Access Point	As defined in Art. 2 §1 (29) of the Federal Grid Code for an access to the transmission grid of ELIA. For an access to the ELIA Grid other than transmission grid, or to a Public Distribution Grid, or to a CDS: a point, defined by physical location and voltage level, at which access to the ELIA Grid other than transmission grid, or to a Public Distribution Grid, or to a CDS is granted, with a goal to inject or take off power, from an electricity generation unit, a consumption facility, a non-synchronous storage facility, connected to this grid.
Communication Platform (CP)	The Communication Platform is a platform enabling a secure exchange of real-time data between the assets of Grid Users and applications of Application Service Providers.
(Service) Delivery Point (SDP)	A point on an electricity grid or within the electrical facilities of a Grid User, where a Balancing Service or strategic reserve service is delivered – this point is associated with one metering and/or measures, according to dispositions of the BSP Contract aFRR, that enable(s) ELIA to control and assess the delivery of the aFRR Service.
Endpoint (EP)	A digital data access point registered on the CP that allows the exchange of data between the SDP and an Application over the CP via a Gateway.
Flexhub (FH)	The Flexhub is an application that stores and structures flexibility related data. It is connected to the Communication Platform for the exchange of data and the activation of services.
Flexibility Service Provider (FSP)	The Flexibility Service Provider (FSP) offers flexibility services and valorises the aFRR service on the GUs Service Delivery Points. In the context of aFRR, the flexibility offered is for system balancing so the FSP is considered a Balance Service Provider (BSP).
Gateway (GW)	A private communication gateway connecting the physical asset and its metering device to the CP in a digital way. This gateway must be installed locally for the exchange of aFRR data.
Headpoint (HP)	Means an Access Point (always identified by a single EAN number representing offtake). Each Headpoint is registered by the System Operator in the Access Register.

Measurement device (MD)	The measurement device is the device that measures the electrical asset(s). Either it pushes the data or the data is pulled by a gateway.
Grid User (GU)	As defined in Art. 2 §1 (57) of the Federal Grid Code for a Grid User connected to the ELIA Grid or to Public Distribution Grid; or as defined in Art. 2 §1 (58) of the Federal Grid Code for a Grid User connected to a CDS. In the context of this technical guide, Grid Users are companies that are connected to the transmission or medium-voltage distribution grids and are contracted by FSPs to participate in the delivery of aFRR via DP_DG units.
Communication Platform Operator (CPO)	The Communication Platform Operator operates, maintains and manages the Communication Platform. The CPO is representing and mandated by the System Operators.

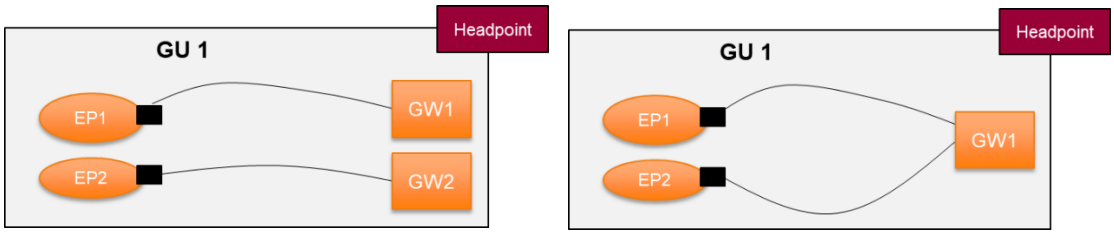
3 Overview of actors and concepts

The figure below gives an overview of the actors that are involved and concepts that are used in the real-time data exchange of the aFRR settlement messages. Note that the contracting and the onboarding process precede this situation. The onboarding processes are described in the next section. The contracting process is described in the T&C BSP aFRR.



4 Data sources

The data sources consist of three elements:



- **Measurement device**: Pmeas is measured and sent in real time by the measurement device via the private local gateway towards the Communication Platform. The data can either be pushed

by the measurement device via the local gateway or pulled by the gateway from the measurement device. The FSP system enriches the message with the required aFRR parameters. The measurement device general technical requirements are described in document C8/06 (which can be found on Synergrid website). The measurement devices must not be registered on the Communication Platform.

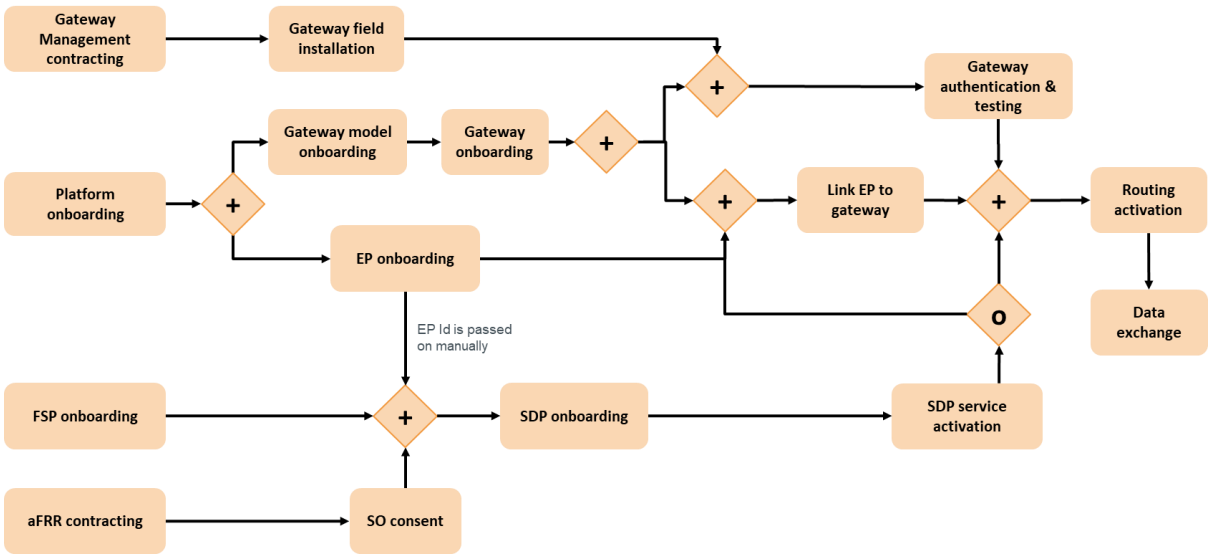
- **Gateways**: Private gateways are operated and maintained by the GU or an FSP mandated by the GU. The gateways have to be installed **locally** within the premise of the grid user and must have direct connection with the Communication Platform. A gateway can be connected to multiple endpoints behind the same headpoint (access point) but **cannot** be connected to endpoints of different headpoints. The gateways must be connected to the Communication Platform and comply with the general technical requirements set out in document C8/06 (which can be found on Synergrid website). They are administratively registered on the Communication Platform via the management portal.

- **Endpoints**: The endpoint is considered the digital data access point and by transfering data towards the Communication Platform it enables services on this point. Endpoints must be registered under a headpoint on the Communication Platform, and can only be done in case a correct mandate is obtained. In the context of aFRR, an endpoint can be seen as a digital version of the Delivery Point, which is not providing energy but used for data exchange.

5 High level business processes

In the figure below you can find the high-level business processes representing the necessary preliminary activities that must be fulfilled in order to establish the digital metering data chain required for the real-time data exchange of aFRR settlement data.

DISCLAMER: Note that these processes are work in progress and can still be subject to change.



5.1 Data source related processes

5.1.1 *Contracting and registration*

- ***Gateway management contracting:***

In case the grid user does not manage his own gateways and endpoints, these activities can be delegated to an FSP. This delegation contract will be the subject to the subsequently use of a Gateway Management (GWM) designation document. In the text below the term **CP user** will be used, which will either be the GU or the FSP if mandated by the GU.

- ***Account onboarding***

The CP user onboards his account and users in order to manage its data sources on the Communication Platform.

5.1.2 *Physical processes*

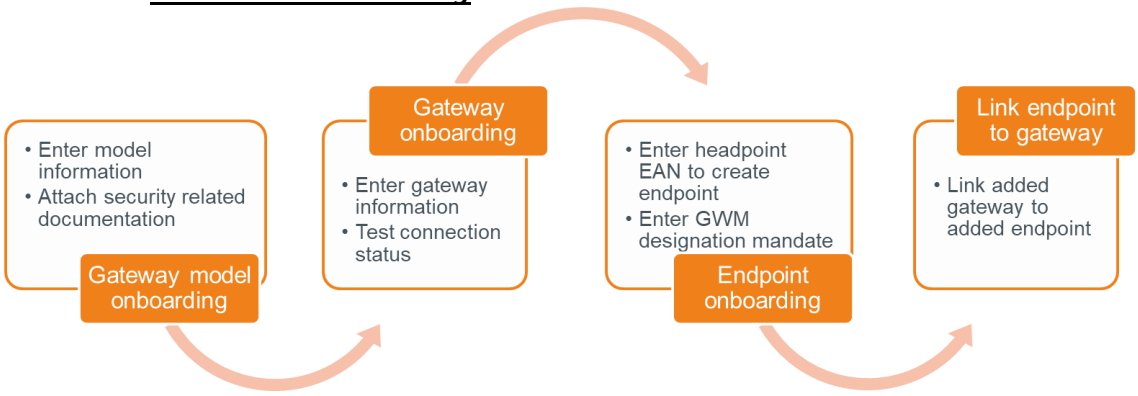
- ***Gateway field installation***

The CP user physically installs the gateway on the premise of the grid user, connects it to the measurement device, and assures the gateway is configured correctly.

- ***Gateway authentication and testing***

The CP user installs the digital certificate on the gateway and connects to the platform to test the installed gateway via the heartbeat (see document C8/06).

5.1.3 *Data source onboarding*



- ***Gateway model onboarding***

The CP user must first register a gateway model and upload the required security documentation related to the model.

The following security documentation is required:

Documentation	Description
Secure product development lifecycle	Documentation of the secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify provided energy delivery system hardware, software, and firmware. If applicable, it

	must be documented how the most critical application security weaknesses (including OWASP Top 10 or SANS Top 25 Most Dangerous Software Errors) are addressed in the Supplier's SDLC.
Secure network configuration management	Provide documentation that the network configuration management interface is secured.
Security standards	Listing of security standards to which the implementation adheres.
Patches and updates	Documentation that the installed GW (including third-party hardware, software, firmware, and services) has appropriate updates and patches installed prior to activation of the communication to the Communication Platform or within (a pre-negotiated period) after installation. Patches and updates need to be done continuously during the GW lifecycle.
Publicly disclosed vulnerabilities	Upon request of the Communication Platform operator, and prior to activation of the communication to the Communication Platform, a summary documentation must be provided of publicly disclosed vulnerabilities in the procured product and the status of the party's disposition of those publicly disclosed vulnerabilities.
Hardware - software testing	A Quality Assurance program and validation that the software and firmware of the procured product have undergone Quality Control testing to identify and correct potential cybersecurity weaknesses and vulnerabilities. This testing shall include fuzz testing, static testing, dynamic testing, and penetration testing. Positive and appropriate negative tests must be used to verify that the procured product operates in accordance with requirements and without extra functionality, as well as monitor for unexpected or undesirable behaviour during these tests. This testing may be done by an independent entity or the CP user's company. Summary documentation of the results of the testing must be provided including unresolved vulnerabilities and recommended mitigation measures.
Cybersecurity program	The Communication Platform Operator shall reserve the right to request documentation of CP user's implemented cybersecurity program, including recent assessment results or conduct periodic (at a negotiated frequency and scope) on-site security assessments at the GW installed facilities. These on-site security assessments may be conducted by an independent third party, at the discretion of the CPO.

- ***Gateway onboarding***

The CP user can subsequently register gateways of successfully uploaded models on the platform.

- ***Endpoint onboarding***

In parallel, the CP user can onboard endpoints. Therefore, he enters a headpoint EAN number and uploads the GWM designation document, in case the CP user is an FSP mandated by the GU, for the gateway management activities. He subsequently creates an endpoint, which will automatically be linked to this headpoint on the platform.

- ***Link endpoint to gateway***

When an active endpoint and gateway are correctly registered on the platform, CP user links the gateway to the endpoint on which it is (or will be) installed.

5.2 Other processes

To give additional project context the following processes are introduced. The final processes will be included in the aFRR terms and conditions.

- ***aFRR contracting***

The grid user contracts the Flexibility Service Provider to valorise its flexibility to the Flexibility Requesting Party (FRP). This contract will be the subject of the subsequently used Grid User declaration.

- ***FSP onboarding***

The FSP will contract either the Flexibility Requesting Party and System Operator with a preliminary agreement or final contract. The FRP or SO will request the Flexhub Operator to register or update the FSP account in the Flexhub.

- ***SO consent***

The DSOs assess with a Network Flexibility Study whether the delivery point can participate in aFRR and the SO reviews the GU declaration. After reviewing the SDP request, the SDP is registered in the Flexhub.

- ***SDP onboarding***

The SDP is subsequently onboarded in the Flexhub and linked to the corresponding Flexibility Service Provider. The FSP is able to already register the corresponding Endpoint ID, but this is not mandatory.

- ***SDP activation***

Once the SDP is onboarded and the Endpoint Id is completed (by the SO in the Flexhub), the SO will send a service activation message via the Flexhub to the Communication Platform to open up the routing.

- ***Routing activation***

When an endpoint, on which the aFRR service is activated from the Flexhub **and** which is linked to an active registered gateway installed on the premise of the grid user, the routing will be enabled.

- ***Data exchange***

Once messages enter with this endpoint and gateway combination, the Communication Platform will route the data to the Flexhub from where it will be collected by aFRR settlement systems.