HOW TO FACILITATE THE INTEGRATION OF A HUGE NUMBER OF HETEROGENEOUS SMARTGRID DEVICES ?

Maxime GILLAUX
EDF – France
maxime.gillaux@edf.fr

Florent LEMENAGER
EDF – France
florent.lemenager@edf.fr

Thierry COSTE
EDF - France
thierry.coste@edf.fr

ABSTRACT

In the new paradigm of energy and digital transition, the system automation designed for smart grid applications must be adapted to cater for new functional and reliability needs.

*To avoid significant increasing operating expenditure, the devices will therefore need to be updatable, configurable, and supervisable remotely. This is a cornerstone of the solution we call "**System Management**" (SM), which refers to functionalities that are not directly linked to the operational role of the equipment but allow it to perform its operational functions in the best conditions possible.*

This paper presents the ongoing EDF's work on system management. To face the challenge of a widespread deployment and interoperability, EDF R&D is developing a first System management prototype tool. The goal is to build an interoperable and vendor independent system, homogenous with the core 61850 primary functions of the equipment.

INTRODUCTION TO SYSTEM MANAGEMENT

Energy transition will be accompanied by a digital transition for network operators which are or will be facing massive roll-outs and refurbishment of their distributed automation to implement deeper monitoring and new smart grid applications. The devices to be deployed to solve today's issues (MV voltage and reactive power regulation for example) will necessarily have to be upgradeable to face those of tomorrow (e.g. electric vehicles, low voltage automation) which will arrive long before the end of its lifetime. Furthermore, there is a necessity for the equipment to adapt to the evolving and growing cybersecurity threats.

To avoid significant costs, this requirement of adaptability will therefore introduce a need for remote System Management capability, as a huge number of equipment will have to be able to be patched, updated and reconfigured. This is a cornerstone of System Management, but it also encompasses a large range of functions including asset management, supervision…

As we see it, this issue will be of major importance for the upcoming smart grid solutions and must be standardized in coordination with the IEC 61850 standard specifying data and communication for the grid automation equipment.

EDF R&D has taken the lead of the IEC TC57 WG17 Task Force in charge of specifying a Technical Specification (IEC TR 61850-90-16: Using IEC 61850 for System Management purposes) to standardize System Management use cases for IEC 61850 IEDs.

We will describe the system management use cases we have started to specify and develop in a dedicated Proof of Concept, and look at the impacts on the system.

SYSTEM MANAGEMENT USE CASES

The Use Cases of System Management can be summarized in four categories:

1. Configuration
2. Administration
3. Supervision
4. Asset management

More detailed explanation regarding these four categories will be provided in the following sections.

Configuration

It consists in configuring operational data (grid topology, protection and PLC parameters…), and can be divided in two distinct use cases:

- Offline IED configuration update through a CID file
- Online parameter modification.

Regarding the offline configuration of IEDs through a CID configuration file, we can identify two scenarios:

- Upload of a new configuration file in the equipment
- Fallback on the previous configuration which was saved as backup in the equipment.

The conservation of the previous configuration (necessary for the second scenario is in any case necessary in case of failure in the installation process of the new configuration for the first scenario.

Concerning the upload of a new configuration, it is necessary to be able to carry out the following steps to secure the process:

- Retrieve the current configuration of the equipment, in order to identify, check or compare it with the new configuration to upload;
- Transfer a new configuration file to the IED;
- Validate the new configuration;
- Activate the updated configuration;
- Fallback on the previous configuration in case of failure.

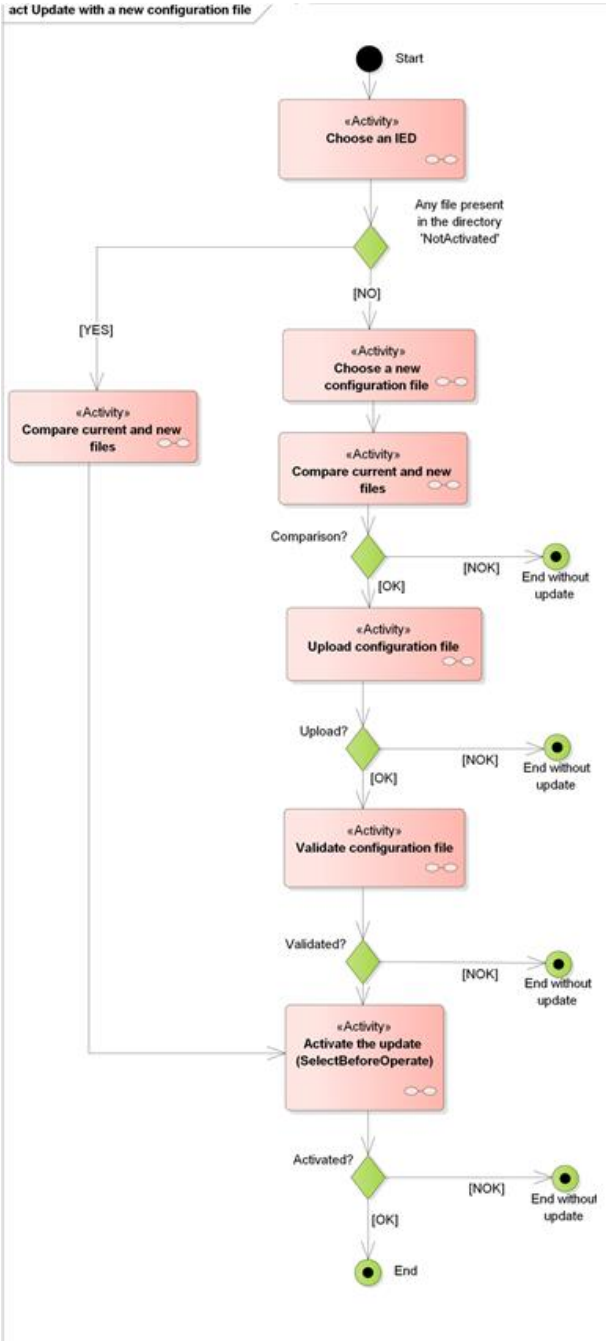

Figure 1: IED configuration update thanks to a new configuration file

In order to carry out these processes, a dedicated folder structure inside the IED (inspired by Annex D of IEC 61850-8-1 Ed.1) has been suggested to store:

- the current activated configuration file;
- a new one that has not yet been activated;
- the old one which contains the previous configuration and is still present for possible backup purpose.

An IEC-61850 client will then only be capable of uploading a new file in the folder dedicated to new and not yet activated configuration files. Furthermore, each folder can contain only a single file.

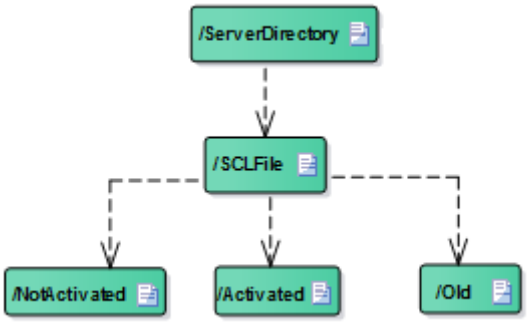

Figure 2: Proposed folder structure for configuration

The system use cases that have been drafted will require the use of the following model classes and their related services: GetServer, GenDataObjectClass, Report-Control-Block, and File transfer. Furthermore, a new ACSI service needs to be defined, based on the SCL control block described in Annex D of IEC 61850-8-1 Ed.1, to interact with the validation and activation states of the configuration files.

Administration

Administration concerns the upgrade and version management of an IED's firmware.
It relies on the ability to check the current firmware version of the device, to download a new one, and to activate it.

On a technical point of view, this use case is therefore very similar to the offline configuration one.

Supervision

This part consists in two use cases

- Supervise live the smooth running of the system to identify deficiencies and if possible suggest resiliency solutions
- Collect data concerning the operational state of the equipment in order to lead predictive analysis, launch maintenance actions and reduce failure probabilities

Specifically, it will therefore be necessary to remotely monitor a number of operating states of the device, including different alarm information.

The information for the real-time monitoring will be obtained through the mechanisms of Buffered Report Control Block and its different trigger options: data-change, quality-change, data-update, etc.

Concerning the maintenance related data, the information mainly includes the different logs stored in the equipment, or performance indicators which can provide valuable information for corrective, predictive, condition-based (etc.) maintenance, such as the number of operations of a switch

Examples of indicators to supervise include alerts relating to:

- Watchdogs of the internal functioning of the equipment, such as for example the data objects of logical node LPHD (Physical Device Information, see IEC 61850-7-4).
- Communication on local networks (connectivity, buffer), such as for example the data objects of logical node LCCH (Physical Channel Communication supervision cf. IEC 61850-7-4).

Comprehensive live supervision and maintenance related data needs to be identified and if not already standardised ad hoc logical nodes need to be defined.

Asset Management

The goal of asset management is to improve one's knowledge of its assets. It consists in collecting patrimonial data from system automation devices and transferring it to the asset management and maintenance information systems.

From an IEC-61850 point of view, the concerned information is essentially that which is stored in the Device Name Plate data class (DPL: cf. IEC 61850-7-3) like for example:

- Vendor name ("vendor" attribute)
- Hardware revision ("hwRev" attribute)
- Serial number ("serName" attribute)

This information could be easily retrieved by using the IEC-61850 services allowing to read and send dataset structures.

CYBER-SECURITY ISSUES

"Securing" is not a System Management use case per say but also needs to be mentioned. On one hand System Management functionalities (in particular configuring and managing the software) are critical and need to be secured, and on the other they are necessary to deploy cybersecurity patches and ensure the system's supervision.

COMPLETE SYSTEM PARADIGM

The previous sections of this paper have only considered the System Management issues for pure system automation objects. But the emerging smart grid devices can not only be considered as such. They are in fact a combination of three types of objects:

- System automation devices
- Telecommunication devices
- Cyber-security devices

Therefore, the previously described System Management use cases will have to be considered for these three categories of equipment.

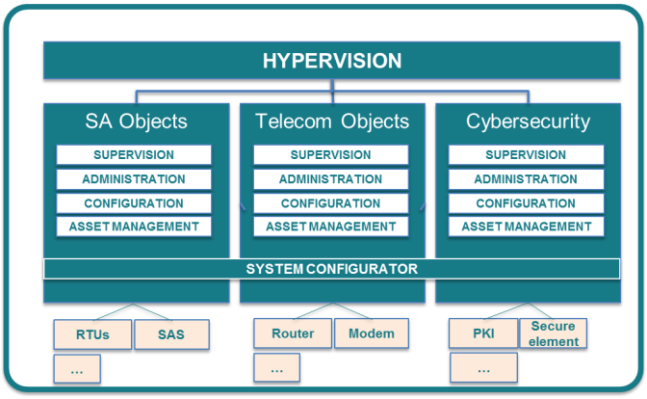

Figure 3: Logical view of Industrial Device Management System solution

As the categories denote different kinds of devices, using heterogeneous technologies, and possibly based on various standards, it is obvious that their System Management use cases will be significantly different. But their specification should be conducted jointly to ensure a full system integration.

This crucial characteristic will also strongly rely on two important adjacent notions:

- Transverse system configuration
- Hypervision

Transverse system configuration

As previously seen, System Management of various categories of equipment can possibly result in a diversity of use cases and implementations, and therefore may be hosted in separate tools. But as they are intended to be managed together in an integrated smart grid perspective, a key step toward success will be to ensure that these

different System Management tools work together and share transverse information.

It highlights the need to configure these devices jointly in a transverse system configurator. This configurator aims to centralize the description and static setting of the system, and then dispatch the adequate information to each System Management tool.

Hypervision

From the point of view of real-time operation, it can be considered that the notion of hypervision is a bit symmetrical to the one of transverse system configuration. It consists in a synthetic view aggregating information of all three categories of objects to provide an efficient monitoring of the whole system.

This concept is still in its infancy and needs to be refined and developed as soon as the essential System Management use cases have acquired a sufficient level of maturity.

CONCLUSION

From our point of view, the System Management functionalities introduced in this paper need to be managed by the network operator with an interoperable and vendor independent Information System. EDF leveraging its industrial strategy mainly on the standardization work, the use cases and workflow need to be standardized. As these are to be applied to IEC 61850 compliant system automation equipment, these functionalities need to be integrated in this standard.

This is why, we have just initiated a new task force in IEC TC57 where we intend to share our work in order to come up with a standardized System Management technical specification (IEC-61850-90-16) in preparation for a new part of the IEC 61850 standard.

EDF also intends to develop a System Management prototype which will be part of a larger industrial device management system for the DSO addressing system automation, telecom and cybersecurity devices.

REFERENCES

[1] IEC-61850 part 7-3: Basic communication structure – Common data classes
[2] IEC-61850 part 7-4: Basic communication structure – Compatible logical node classes and data object classes
[3] IEC TR-61850-90-16: Using IEC 61850 for System Management purposes