Technical University of Denmark

Deliverable 1.1 Smart grid scenario

Project: Cyber-phySicAl security for Low-VoltAGE grids (SALVAGE)

Korman, Matus; Ekstedt, Mathias; Gehrke, Oliver; Kosek, Anna Magdalena

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

SmartGrids ERA-Net

Project:

Cyber-phySicAl security for Low-VoltAGE grids (SALVAGE)

Project partners:
KTH - Royal Institute of Technology
DTU - Technical University of Denmark
PWR - Wroclaw Institute of Technology

Deliverable 1.1
Smart grid scenario

Matus Korman (KTH)
Mathias Ekstedt (KTH)
Oliver Gehrke (DTU)
Anna Magdalena Kosek (DTU)

April 2015

Revision history

Issue	Date	Changed page(s)	Cause of Change	Implemented by
0.1	2015-03-16	All	First draft	Matus Korman Mathias Ekstedt
1.0	2015-04-23	All	First release	Anna Magdalena Kosek Oliver Gehrke Matus Korman Mathias Ekstedt

1. Table of Contents

SALVAGE project

The purpose of the SALVAGE project is to develop better support for managing and designing a secure future smart grid. This approach includes cyber security technologies dedicated to power grid operation as well as support for the migration to the future smart grid solutions, including the legacy of ICT that necessarily will be part of it. The objective is further to develop cyber security technology and methodology optimized with the particular needs and context of the power industry, something that is to a large extent lacking in general cyber security best practices and technologies today. In particular the focus of the project will be on smart grid with many small distributed energy resources, in particular LV substation automation systems and LV distribution system.

2. Introduction

The purpose of work package 1 is to build a common understanding and context on which further research in the other work packages can be based. The common ground for the project is to find one or several smart grid scenarios that can be further analyzed with respect to cyber-physical security from various aspects in the other work packages. This delivery reports on the first iteration of identifying such a scenario. The results presented here are thus preliminary and will be further refined throughout the project in six month intervals and finally reported in Deliverable 1.2 at the end of the project.

At the time of writing the project proposal we envisioned the common smart grid scenario ground to be 2-5 different scenarios. Currently our plan is to use one, quite extensive, example as the project base scenario labeled PowerCap. This scenario is based on a future envisioned solution for power peak shaving in low voltage grids. It is a comprehensive example since it is one of the core functions of a smart grid, it involves a number of actors, and it uses a quite vast part of the ICT infrastructure for its implementation. In chapter 2 we describe the basic structure of the PowerCap scenario. The project will likely use a few variants of the same base scenario.

3. The PowerCap scenario

1.1 Description

The scenario (described in more detail in [Han13], [Nor13]) is set in a low-voltage (LV) distribution grid, on a grid feeder in a predominantly residential area. Connected to the feeder are mostly building loads and a small number of distributed generation units (photovoltaics in this case).

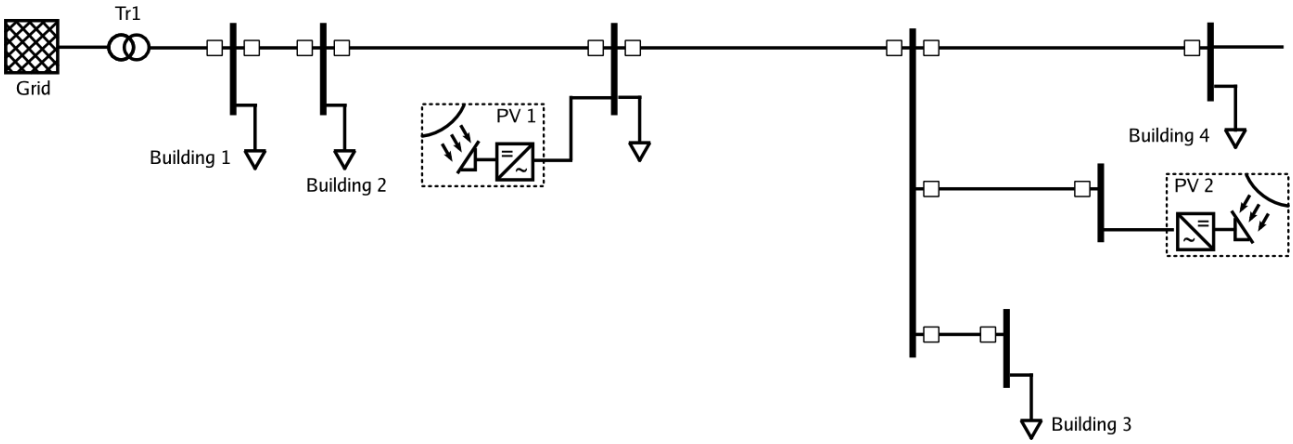

Figure 1: Power scheme of the scenario

Some of the buildings and PV units can be externally controlled in order to offer flexibility services to the grid.

The flexibility service chosen for this scenario is PowerCap. The service is used by a distribution grid operator (DSO) to ensure that certain assets in the grid, such as transformers or cables, do not get overloaded in extreme power flow situations. In order to achieve this, the DSO periodically measures the power flow through the asset in question and, if the asset is loaded higher than a preset

limit, asks the flexible assets to reduce their consumption or to increase their production by the difference amount between load and load limit.

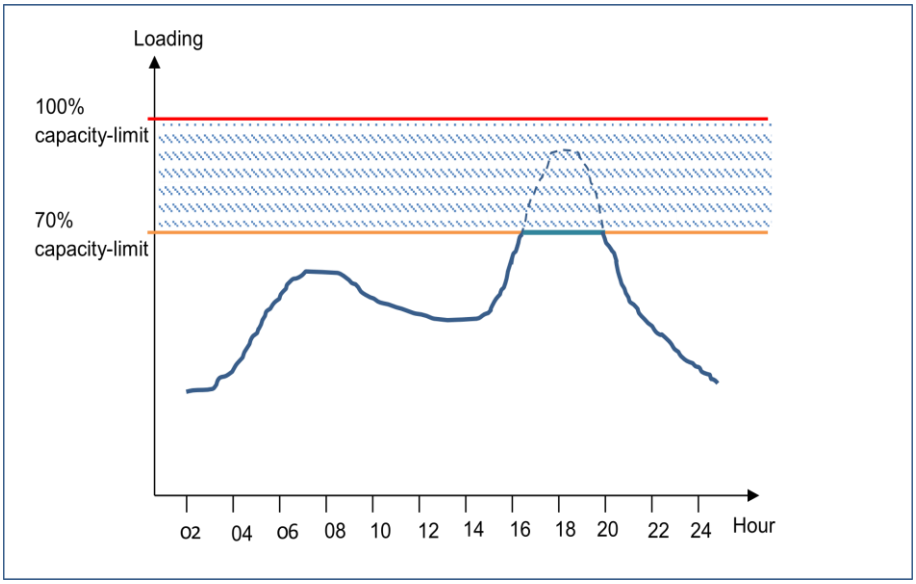

Figure 2: Illustration of the flexibility service function [Nor13]

Because of the stochastic nature of the individual units, they are bundled or aggregated in order to be able to offer a consistent service.

The full PowerCap scenario covers three phases or stages relevant from a communication/cybersecurity point of view:

- Scheduling, which covers the interactions before the operating hour, including the commitment/bidding processes for the service,
- Operation, which covers the real-time, closed-loop control process during the operating hour, and
- Settlement, which involves validation and billing of the delivered service.

The project will focus on the operation stage. Possible extensions of the scenario are listed further below.

1.2 Actors

The basic scenario has three actors:

- A DER owner. The DER owner operates a production, consumption or storage unit which is connected to the distribution grid. The unit usually fulfills a primary purpose for the owner; as a secondary purpose, flexibility in consumption of production patterns (such as e.g. time-shifting of consumption) can be provided to the grid as long as the impact on the fitness for the primary purpose is not affected.
- A distribution system operator (DSO). The DSO owns and operates the infrastructure required for power delivery. This includes measurement and control infrastructure (SCADA

and substation automation).

- An aggregator. The aggregator has contracts with a portfolio of DER units in which these DER units offer flexibility against payment. The aggregator operates the technical infrastructure to communicate with the DER units and is financially responsible in case of missing service delivery.

To cover the scheduling and settlement stages, additional actors might be added at a later point in time.

1.3 Data flow

For the operation case, the flow of data consists of the following steps:

1. The SCADA system reads measurement data from Remote Terminal Units (RTU) in the field (e.g. in substations) and delivers the data to the distribution management system (DMS).
2. A state estimator in the DMS calculates power flow estimates for all grid assets. If any of the assets are loaded above the limit, the DMS calculates the inverted difference as a reference signal.
3. The DMS sends a reference signal to one or several aggregators. In the case where several Aggregators are jointly providing the PowerCap service, the signal will be split and be sent to all contracted aggregators corresponding to each aggregator's proportional share in the installed capacity or service commitment.
4. The aggregator requests flexibility information from all DER units in its portfolio.
5. The DER units respond with a flexibility prognosis.
6. The aggregator performs an internal optimization of its portfolio, in order to be able to deliver the service in the cheapest and most optimal way.
7. The aggregator sends set-points to all connected units and requests flexibility updates.
8. The DER units respond with an updated flexibility prognosis.
9. Smart meters at the DER owner provide measurements to the DSO.

Items 1-3 as well as 4-8 are running continuously in two independent loops. Item 9 provides power measurement feedback directly from the DER owner. The data flow described above is depicted in Figure 3.

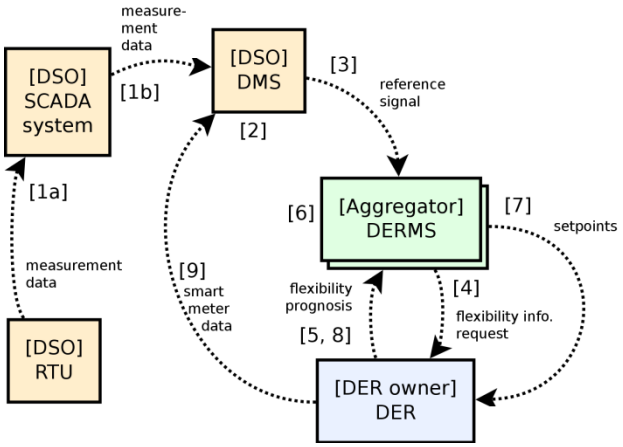

Figure 3: Data flow depiction

1.4 Overview model of the IT architecture

This section provides a brief picture of the IT architecture of the PowerCap scenario. The architecture consists of several subparts (SCADA, substation automation, AMI etc.) which can be varied in more detail, for example, how many substations the example includes. Moreover, the architecture presented here does not describe technical details and assumptions regarding the different systems, for example, what protocols are used, what types of hardware or software, etc. This will be done later in the project, to the extent needed for the specific purposes of WP 2, 3 and 4.

Figure 4 outlines the high level IT architecture of the proposed scenario. Parts of the outline is covered in Figure 5 (SCADA reference model), Figure 6 (substation IT architecture), Figure 7 (AMI reference model), and Figure 8 (Aggregator's IT architecture and DER control). The figures make use of acronyms, which are explained in chapter 4 (Glossary).

The models presented in this section are based on [Ene12], [Som10], [NIS14], among other.

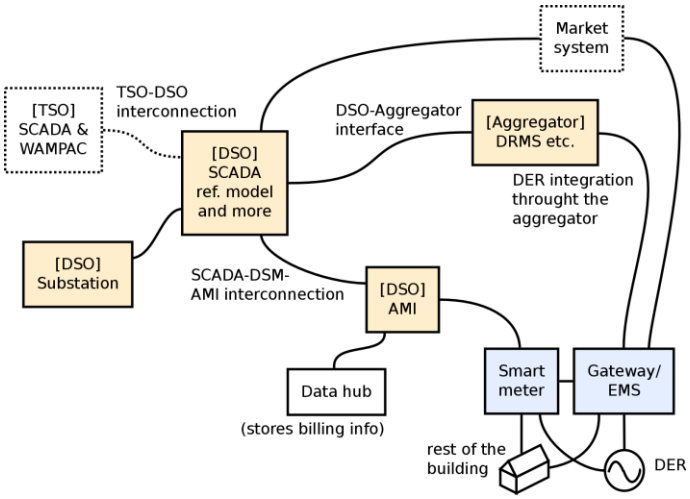

Figure 4: Overview of the IT architecture

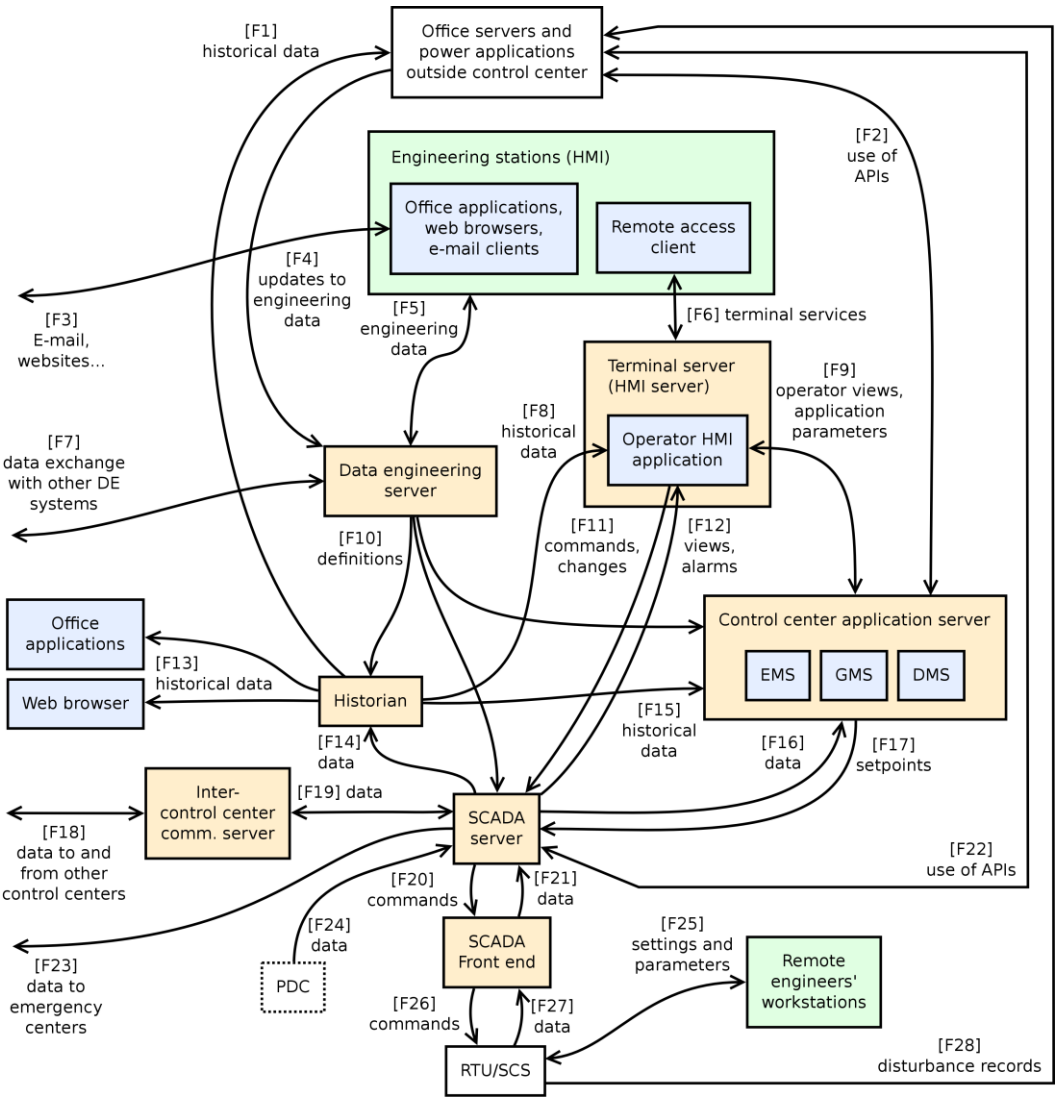

Figure 5: Overview of a SCADA reference model

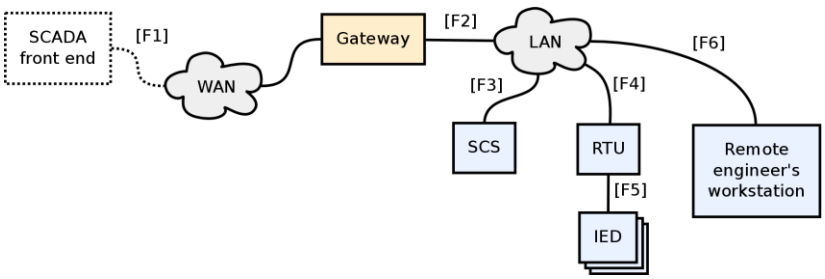

Figure 6: Overview of a substation IT architecture

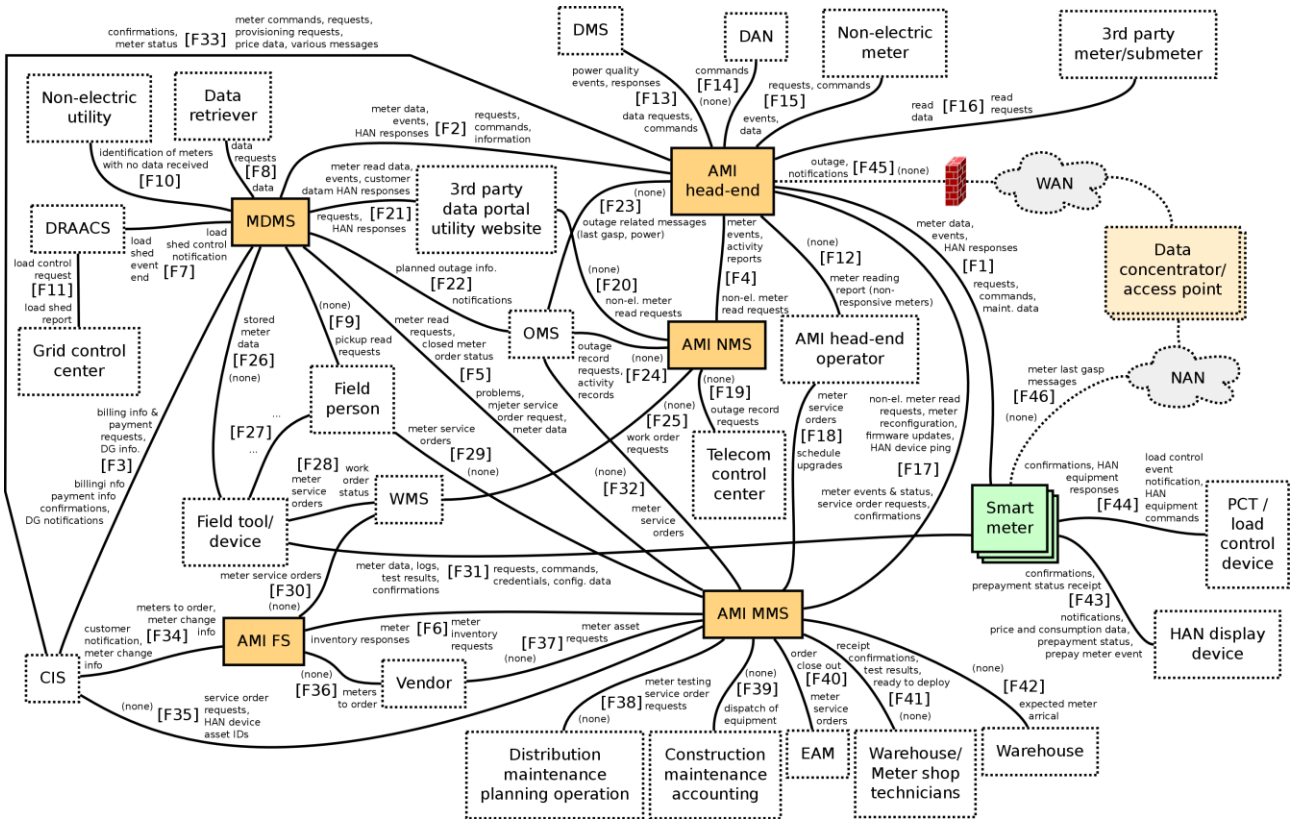

Figure 7: Brief overview of an AMI reference model

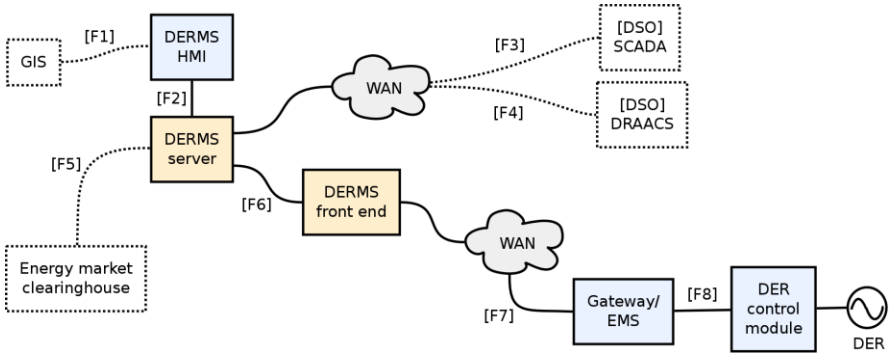

Figure 8: Assumed model of the process part of the aggregator's IT architecture and the DER control

1.5 Variations, extensions and further remarks

Within the above described PowerCap scenario, the following variations will be considered:

- In case of multiple aggregators, reference signal in step 4 is divided between several aggregators.
- Scheduling and settlement stages.

According to all of the three communication/cybersecurity stages of the PowerCap scenario (see higher above), a separate reference model for DRM (demand-response management) might be relevant to include.

In certain cases, DRM also uses AMI as its communication infrastructure between the DSO and its customers (e.g., to issue load shedding notifications to smart meters). Normally, DRM communication directed to and from DERs flows through the Aggregator.

Additional systems of supportive nature that might need to be considered upon need are the DSO's GIS (geographical information system), asset and facility management system, the DSO's and the aggregator's CIS (customer information system), and the DSO's and the Aggregator's office IT systems, which are, although less directly, related and connected to the process.

In likeness with the SCADA and AMI reference models depicted above, even office computers with applications might be beneficial to consider in other parts of the architecture (e.g., Aggregator).

4. Glossary

Acronym	Description
AMI	Advanced metering infrastructure (alt. SMI – Smart metering and infrastructure)
AMI FS	AMI forecasting system
AMI MMS	AMI meter management system
AMI NMS	AMI network management system
CIS	Customer information system
DAN	Distribution automation node
DE	Data engineering
DMS	Distribution management system
DRAACS	Demand Response analysis and control system
DRMS	Distributed resource management system
DSM	Demand-side management (related to demand-response management)
EMS	Energy management system
GIS	Geographical information system
GMS	Generation management system
HAN	Home area network
HMI	Human-machine interface
IED	Intelligent electronic device (further connected to sensors, actuators, other IEDs…)
LAN	[Substation's] local area network
MDMS	Meter data management system
NAN	Neighborhood area network
OMS	Outage management system
PCT	Programmable communicating thermostat
PDC	Phasor data concentrator (part of WAMPAC)
RTU	Remote terminal unit
SCS	Substation control system
TSO	Transmission grid operator
WAMPAC	Wide area monitoring, protection and control
WAN	Wide area network
WMS	Workforce management system

5. References

[Ene12] EnerNex Corporation. (2012). *Security Profile for Advanced Metering Infrastructure.*

[Han13] Hansen, L. H., Sundström, O., Harbo, S., & Villefrance, R. (2013). *iPower WP 4.8: FLECH - Technical Requirement Specification.*

[NIS14] NIST. (2014). *Guidelines for Smart Grid Cybersecurity.*

[Nor13] Nordentoft, N. (2013). *iPower WP 3.8: Development of a DSO-Market on Flexibility Services.*

[Som10] Sommestad, T., Björkman, G. (2010). *VIKING Report D2.3: SCADA system architectures.*