Smart Grid Cyber-Security Simulation Environment

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Norbert Wiedermann
norbert.wiedermann@aisec.fraunhofer.de
Fraunhofer AISEC

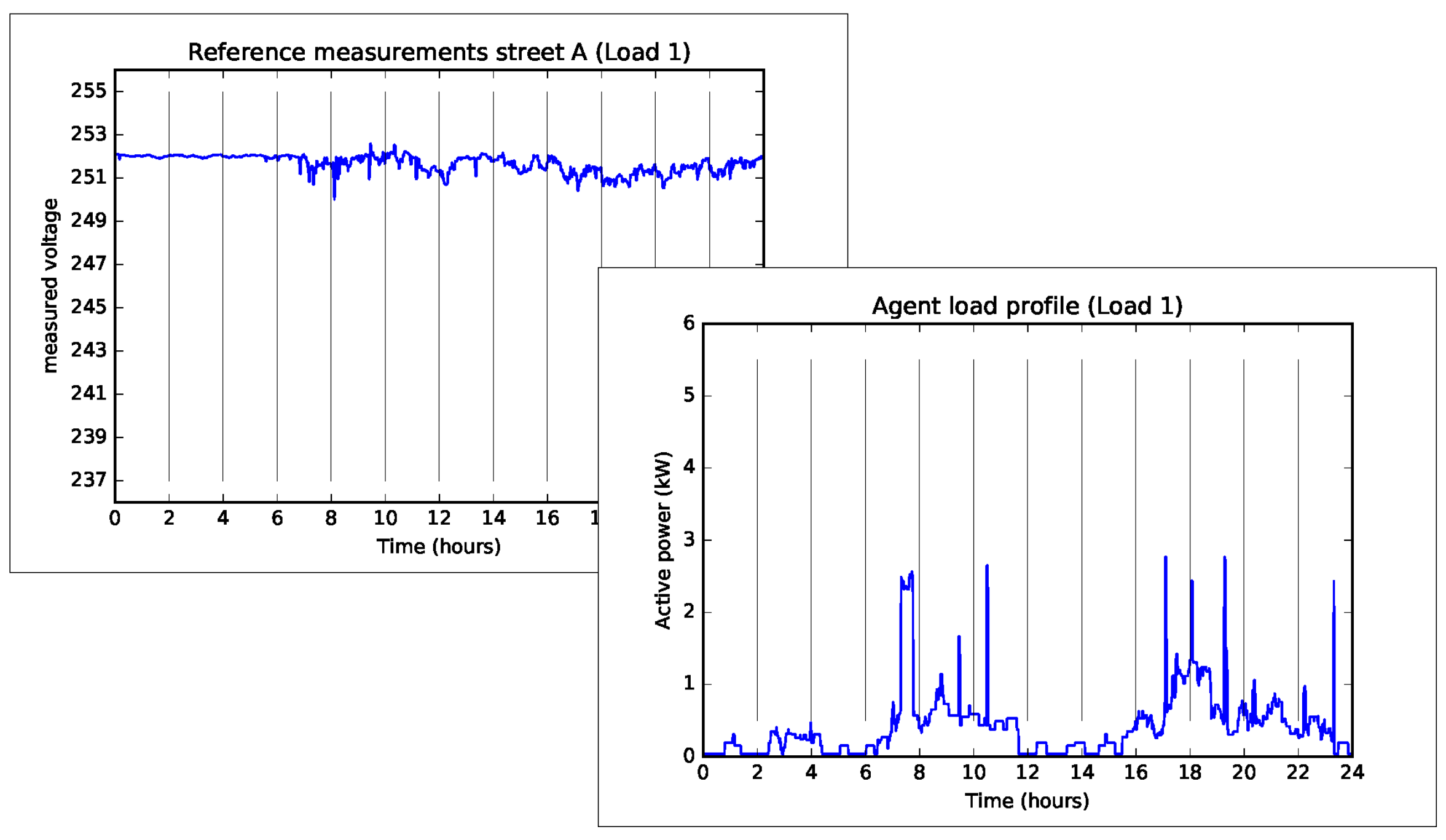
Mislav Findrik
Mislav.Findrik@ait.ac.at
Austrian Institute of Technology

Overview

The current power grid is going to be extended with various field devices, which will under the control of the Distribution System Operator (DSO) be responsible to efficiently handle the demand and supply of electricity. This new system requires more interconnected ICT components than there are now, in order to have all required and necessary measured values to perform grid control operations in a fast and effective way. It becomes very important to assess **the impact cyber-attacks** might have on the participants of the grid and the electrical infrastructure itself, in future smart grid scenarios. In this poster, a **software-software co-simulation environment** for the impact assessment of cyber attacks is presented, together with **software/Hardware-in-the-loop (HIL)** conceptual realization of a **testbed environment** dedicated for development and evaluation of security countermeasures.

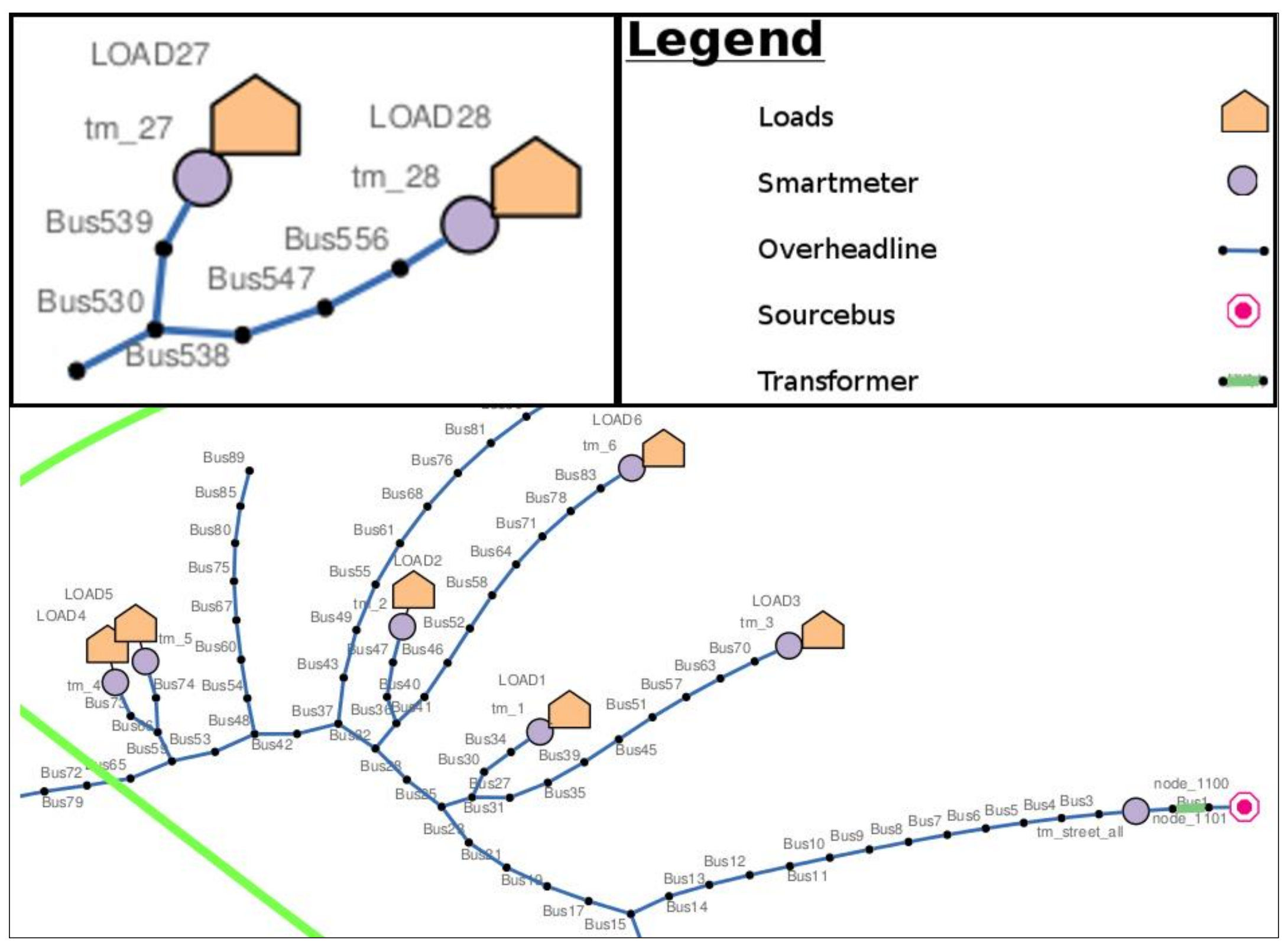
Consumer Pattern

Consumers use electricity described by a load profile. Reference measurements serve for attack evaluation.



Power Grid

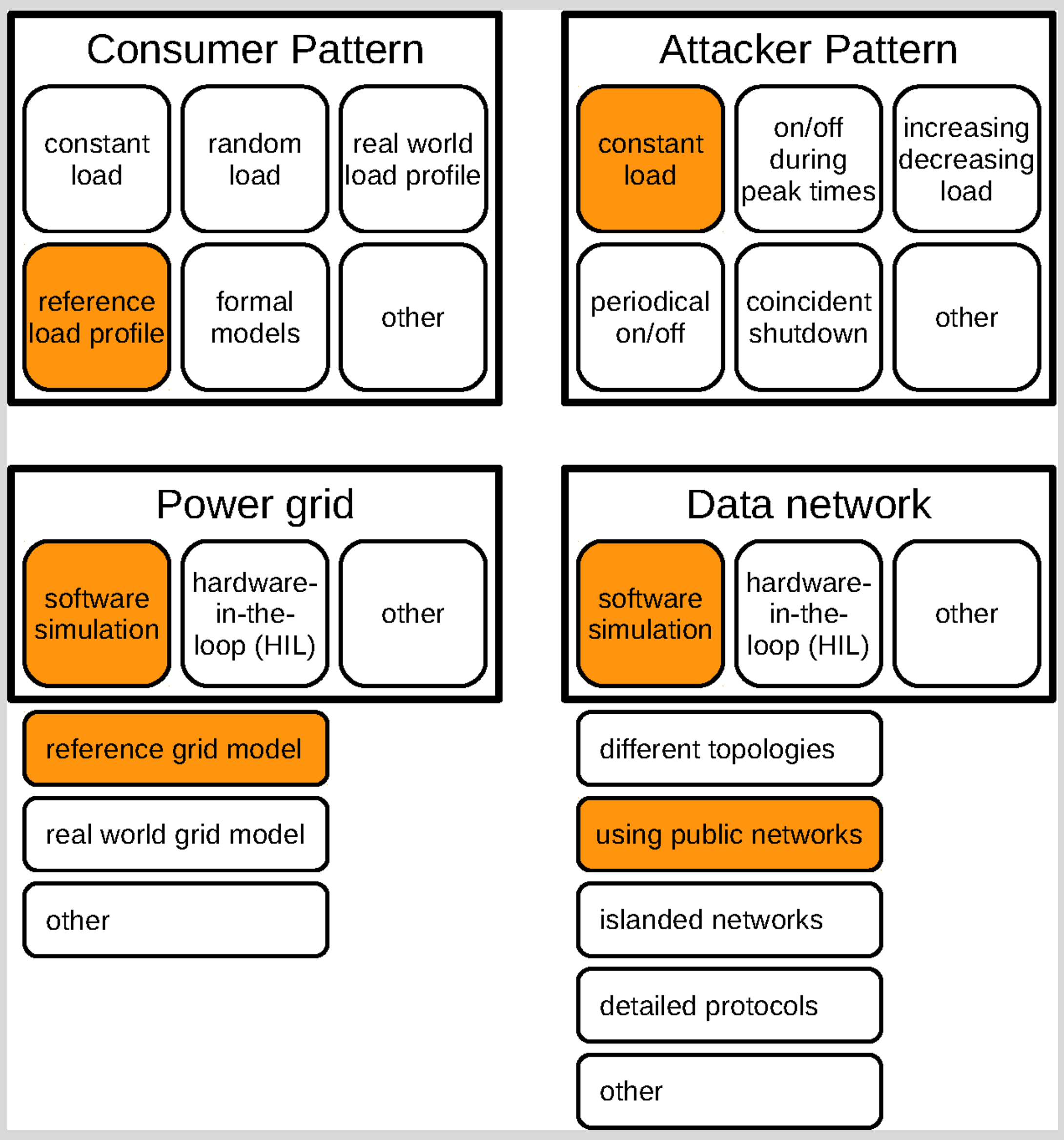
A power grid model based on the IEEE low voltage reference grid for European power grid infrastructure.



SPARKS Conceptual Simulation Environment

A conceptual simulation environment is constructed using four building blocks specifying the Smart Grid environment in which the systems' behavior, in case of cyber-attacks can be analyzed.

- A co-Simulation framework is an instance that integrates interactions between the building blocks.
- The Consumer and Attacker pattern represent physical parameters of a future Smart Grid.
- The Power grid and Data network blocks can be realized using specialized tools for each domain.



Consumer Pattern: constant load; random load; real world load profile; reference load profile; formal models; other

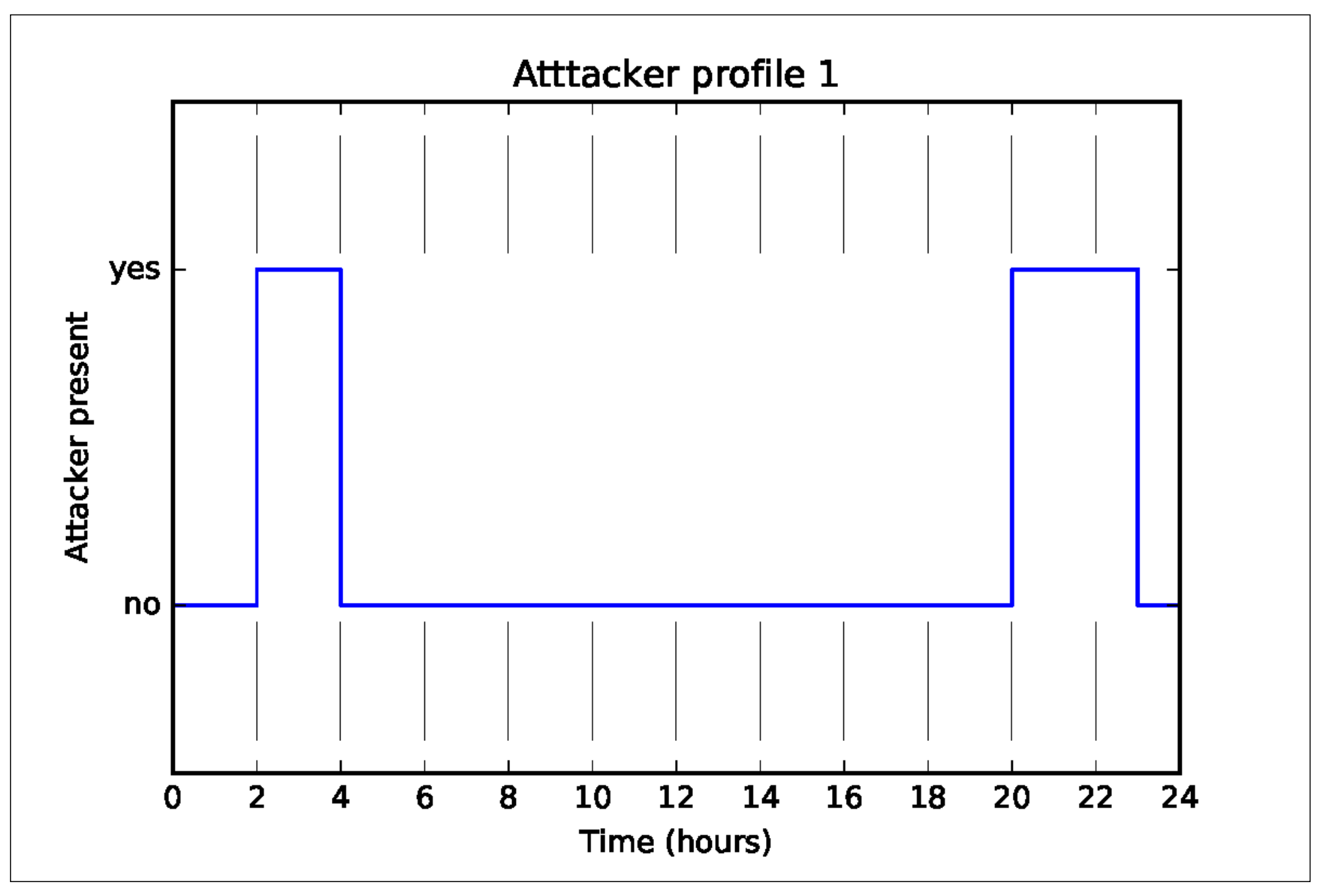
Attacker Pattern: constant load; on/off during peak times; increasing decreasing load; periodical on/off; coincident shutdown; other

Power grid: software simulation; hardware-in-the-loop (HIL); other; reference grid model; real world grid model; other

Data network: software simulation; hardware-in-the-loop (HIL); other; different topologies; using public networks; islanded networks; detailed protocols; other

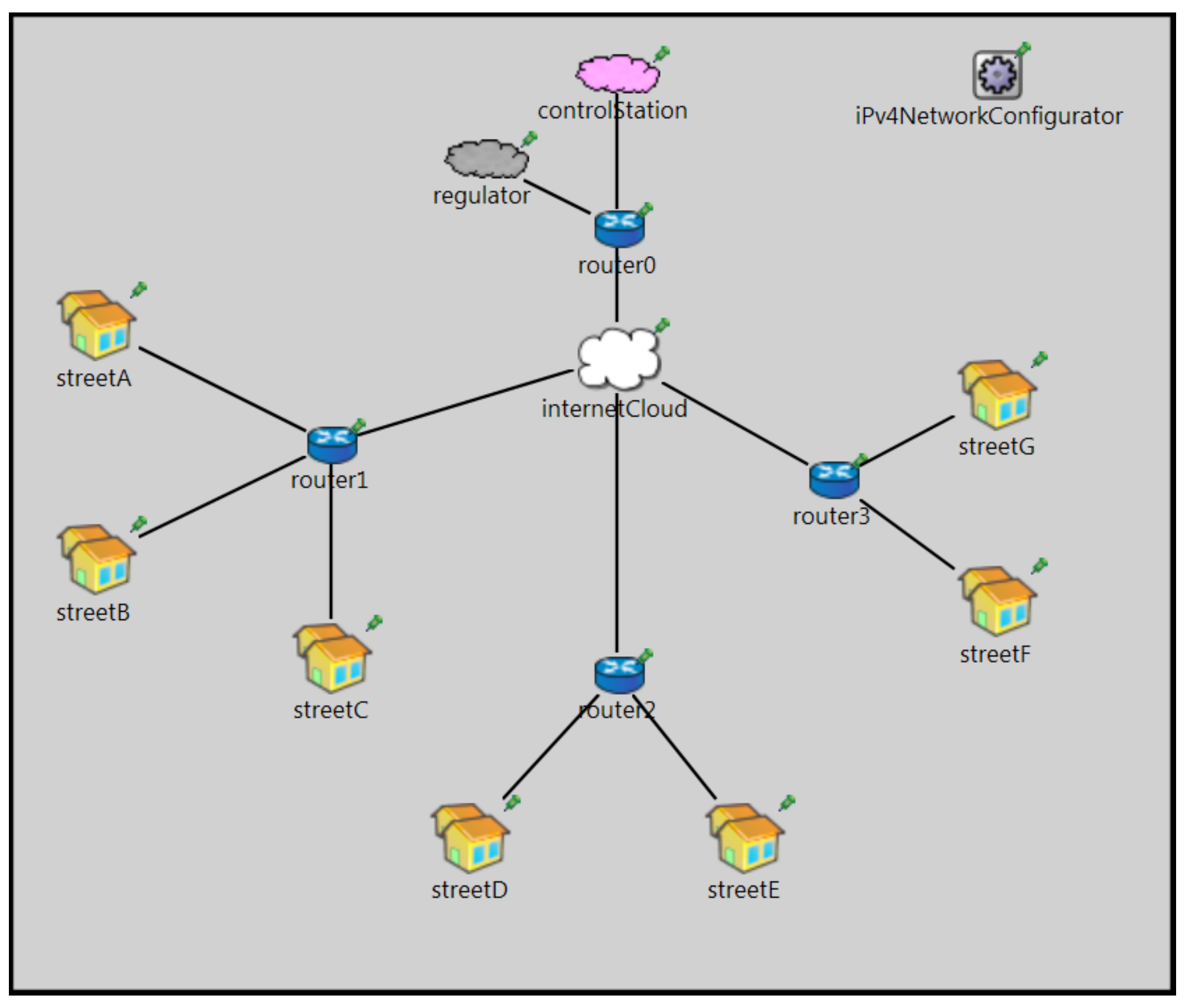
Attack pattern

Transmitted price information from the DSO to the household controllers is manipulated by a MITM attack.



Data network

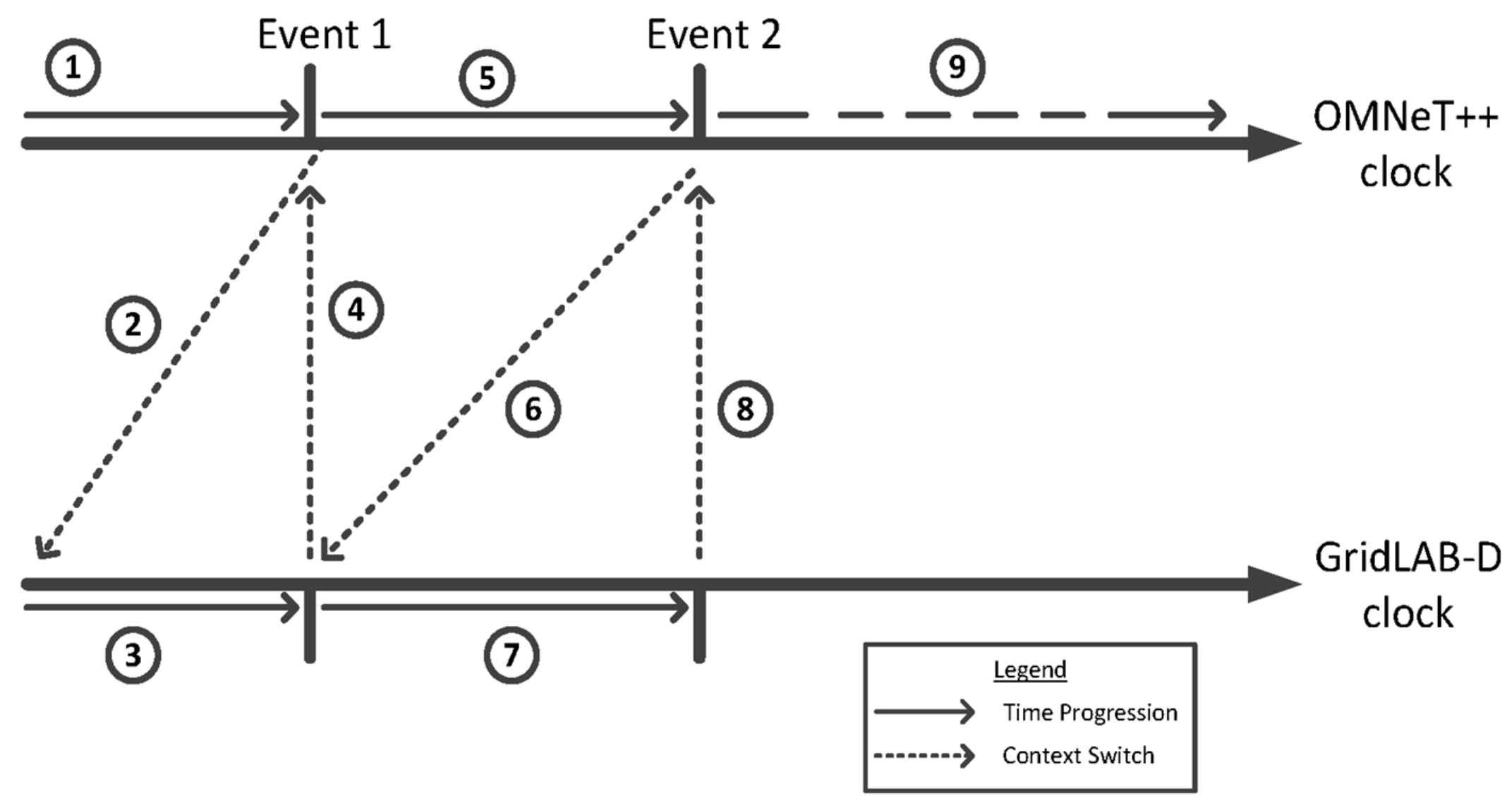
A suitable communication network model for control message exchange is developed.



Performing Co-Simulation: Applying the Attacker pattern to the Smart Grid infrastructure

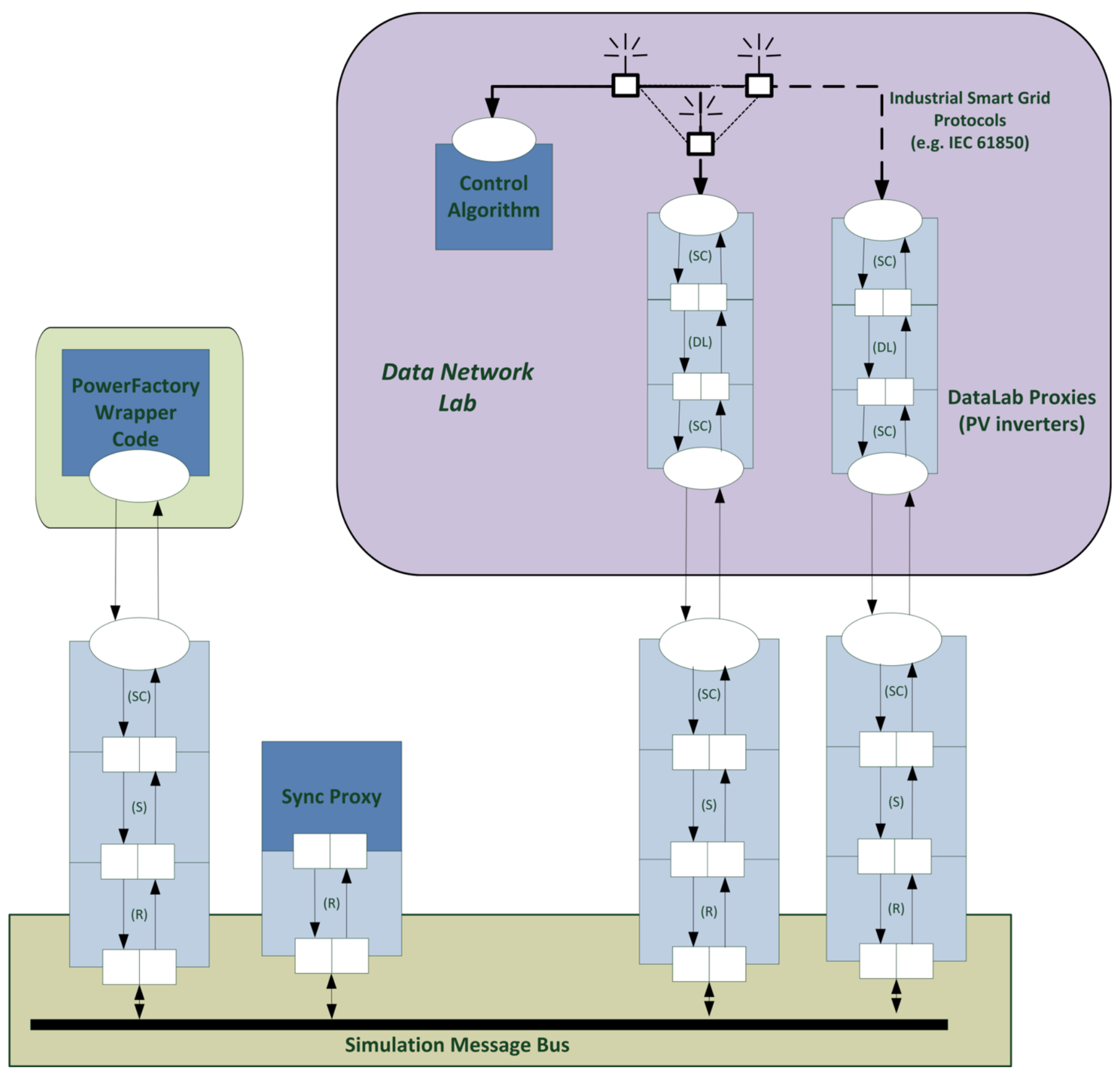
Co-Simulation environment

Coupling of the **OMNeT++** communication network simulator with the **gridLAB-D** electrical grid simulator in an event-based asynchronous simulation.



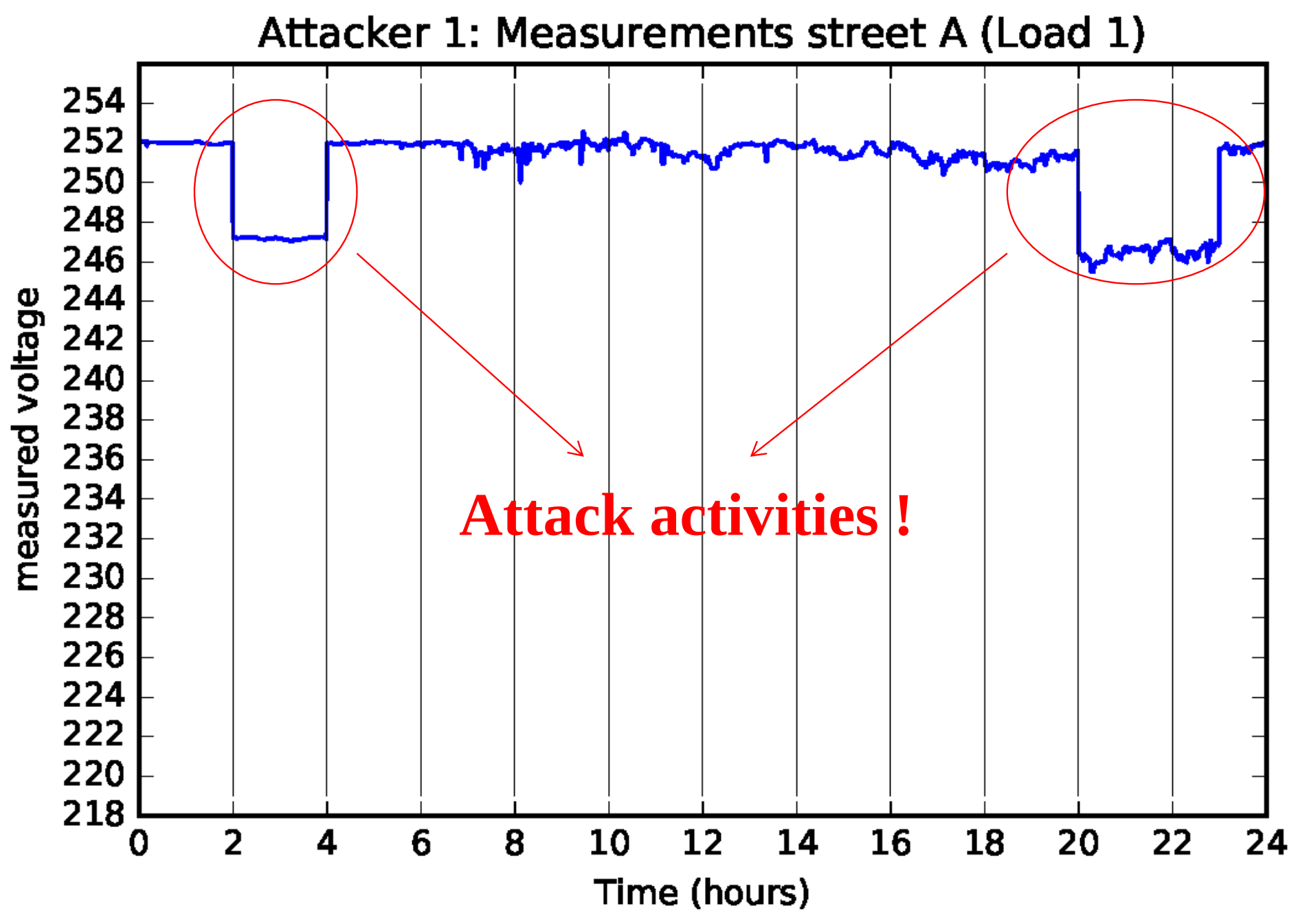
Hardware-in-the-loop (HIL) testbed

- The HIL testbed is called SmartSecLab. It allows development and evaluation of security countermeasures against cyber attacks.
- The SmartSecLab is built around the Simulation Message Bus (SMB) software which allows integration of a power simulator (PowerFactory) and its integration with HIL components in the Data network lab.
- In the Data network lab it is possible to instantiate components simulated in the PowerFactory using the DataLab Proxies.
- The DataLab Proxies communicate with the controller algorithm using industrial protocols over real-networks.


Industrial Smart Grid Protocols (e.g. IEC 61850)
Control Algorithm
Data Network Lab
DataLab Proxies (PV inverters)
PowerFactory Wrapper Code
(SC)
(DL)
(S)
(R)
Sync Proxy
Simulation Message Bus

Results

- The attack causes voltage drops at the attacked households.
- Measured voltage drops can be mapped to the impact level and describe effects for quality of supply.
- Impact levels can be used for further risk assessment.
- The co-simulation can be used for risk estimation and provides input for impact assessment.



Street	Voltage drop	Impact level
A	-4 Volts	LOW (1)
B	-10 Volts	HIGH (3)
C	-16 Volts	CRITICAL (4)
D	-8 Volts	MEDIUM (2)
E	-8 Volts	MEDIUM (2)
F	-16 Volts	CRITICAL (4)
G	-16 Volts	CRITICAL (4)

The SPARK project is supported by the EU FP7 Programme under Contract No. 608224.
Start Date: 1st April, 2014; Duration: 3 years

Contact Information

Website: https://project-sparks.eu
Twitter: @eusparks
Email: paul.smith@ait.ac.at