NetPower DemoLab
A Test Bed Infrastructure for Security and Reliability Investigations of SCADA Systems

Markus Jostock
markus.jostock@uni.lu

Prof. Jürgen Sachau
juergen.sachau@uni.lu

Interdisciplinary Centre for Reliability and Trust, Systems and Control Group
University of Luxemboug, 6 rue Coudenhove-Kalergi, L-1359 Luxemburg

Abstract: The purpose of this paper is to present the capabilities of the new NetPower DemoLab of the Interdisciplinary Centre for Reliability and Trust at the University of Luxembourg, operated by the Systems and Control group, and to stimulate potential public or private collaborations in the area of SCADA security and reliability investigations.

Keywords: security, reliability, laboratory, smart grid, SCADA, DERlab, NetPower DemoLab

Smart Appliances and Systems

As energy efficiency and environmental compatibility is becoming more and more important, the electricity consumers of the future are becoming „smart“. This *intelligence* is enabled by the introduction of ICT (information and communication technology) hardware into formerly passive appliances. Sensors and actuators are connected to the ICT equipment and are generally described as *supervisory control and data acquisition* (SCADA) units.

Within a SCADA unit, physical quantities are digitalised, the values are processed by (potentially embedded) controllers and the aggregated information is sent via a communication link to other ICT nodes. There is a high diversity in hardware and software components on all levels. Processing of the collected data can be done by embedded micro controllers, PC104 industry computers or PLCs, running with a large number of different operating systems. Communication links can be copper based, fibre optics or wireless. Different protocols are used to wrap and send the data, partly directly linked to the physical media, like e.g. Profibus, EIB, real-time EtherCAT, IP or 802.11g.

SCADA Security and Distribution

In 2010 the Stuxnet computer worm infected thousands of computers to deliver its malware to a very specific SCADA platform, the Siemens Simatic S7 PLC. The PLC was connected via Profibus to frequency converters which controlled the speed and acceleration of electric motors spinning the centrifuges in an Iranian nuclear facility. The malware changed the internal PLC code to alter the spin frequency of the centrifuges out of the specified operating point in order to destroy the centrifuges.

Industrial production plants use SCADA installations in many configurations. ICT layers are added in factories for faster data management. Attacking a competitor's facility could cause enormous production losses.

In electric vehicles (EV) frequency converters control the car propulsion motors and will be able to perform ABS-breaking and to re-inject energy into the car battery. Pervasive computing will connect EV to the mobile internet, potentially allowing for software updates via an integrated internet connection. Vicious malware injected in an EV may cause a lethal threat.

In the course of the current transformation of the electricity grid in to an active grid or *smart grid*, households must be equipped with a *smart meter*. The smart meter market volume in the European Union until 2020 values approx. $25 billion[1] and an estimated number of 133-145 million smart meters will be installed. Manipulating the measurements may result in diverged accounting, eavesdropping on the data may allow conclusions on user profiles or presence detection for burglary.

As pervasive computing progresses deeper into our every day appliances (e.g. smart homes), attacks on specific SCADA systems may cause larger harm in the future.

A Security and Reliability Testbed for Smart Grids

The NetPower DemoLab intends to provide a test bed infrastructure in order to easily set up scenarios under investigation, based on a wide range of technologies, particularly in the emerging smart grid technologies.

Different types of grids can be modeled and investigated, like e.g.

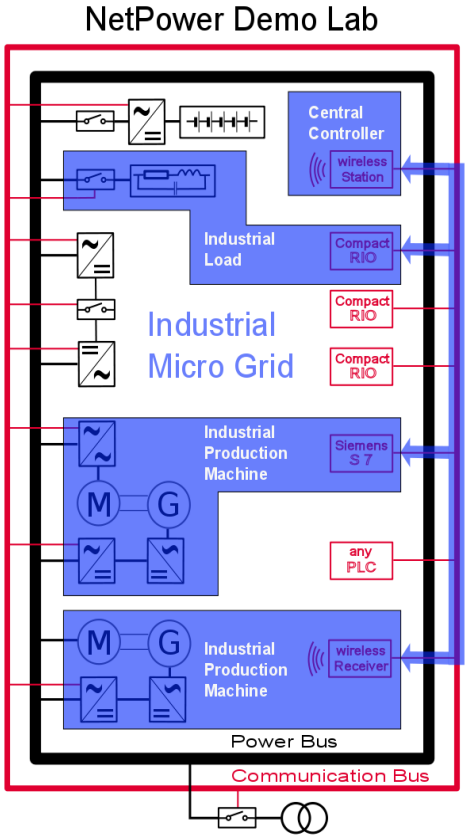
1. Local area power distribution grid (smart grids)
2. Domestic grid of a *Smart Home*
3. Industrial factory grid with energy feedback
4. Electric vehicle on board grid

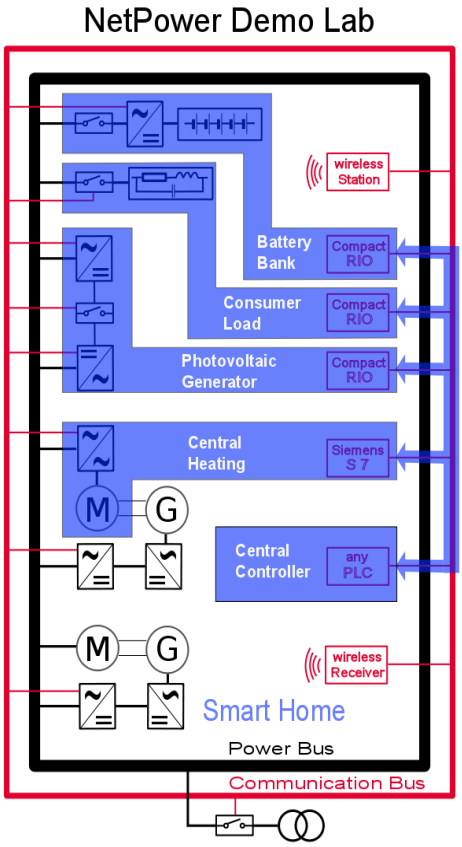
SCADA systems are always embedded in their physical

1 http://www.greenbang.com/research/smart-meter-outlook-2020

environment and are only one part of the complete system. The main focus of the NetPower DemoLab is on the system perspective and the interaction between communication infrastructure and the power infrastructure and the resulting security and reliability.

In the lab, a ring tube provides the physical framework for different communication or power busses. The configurable physical layout of the laboratory allows to easily integrate new physical wired media into the existing communication ring.





The NetPower Demolab structure for embedding constructive solutions in the computer aided engineering process is combining real and virtual testbeds, progressing from offline to online testing. For both hardware in the loop and software in the loop testbeds, realtime simulations up to MHz scan rates can be employed.

The NetPower DemoLab equipment covers realtime simulation backed up by fast FPGA-signal processing hardware, extended to real physics electrical power in the 100kVA range. This allows for close reproduction of grid dynamics, electricity storage, electromechanical conversion and power electronics units as well as of the major realtime field bus protocols, thus allowing for safety, security and reliability test runs of networked SCADA systems in realtime of complex virtual environment and failure scenarios.

A set of voltage source inverters units (VSI) capable of four-quadrant operation and coupled with a DC link and electrical machine units are available. The hardware can be configured in a flexible way by DC and AC coupling to emulate consumers, storage and generators or to build up an island grid. Different machine types are available, e.g. induction machines, synchronous machines or asymmetric permanent magnet out-runners to simulate an EV power train or a domestic or industrial consumer.

The Netpower Demolab is part of the education for Electrical Engineering and Informatics Bachelors and Master of Communicative Systems.

Currently a competence team is built up for

- Reliability and Vulnerability of Electricity Networks
- Multimodel Control Design for Reliability
- Reliable Distributed Cost Optimal Dispatching in Smart Grids
- Stability Verification of Nonlinear Automata Dynamics for Modular Solar Energy Systems
- Reliable State and Parameter Observation for Electrochemical Storage Units

The Netpower Demolab is a platform for cooperation with the European network of excellence DERlab, covering the security and reliability aspects of smart grids for renewable energy integration.

Within the Grande Region the Netpower Demolab offers the opportunity for mobility of researchers and European projects interested in exploiting the available infrastructure and is located at the Campus Kirchberg of the Interdisciplinary Centre for Security, Reliability and Trust at the University of Luxembourg.