The FUSE testbed: establishing a microgrid for smart grid security experiments

E. Xypolytou OVE, J. Fabini, W. Gawlik, T. Zseby

Reliable and efficient energy supply is based not only on local control but also on remote sensor data and measurements, making communication one of the important components. The increasing threat of possible attacks is the motivation behind the main purpose of the FUSE testbed—an experimental microgrid for smart grid research—to conduct experiments on smart grid security, grid optimization, stabilization and islanding. This work, after providing an insight of the current state of the art concerning research on microgrids, describes the FUSE experimental facility as well as first experiments including partial measurement equipment installation and data collection and analysis.

Keywords: microgrids; smart grid security; energy supply; ICT; islanding; PMU; time synchronization; decentralization; attacks; renewable energy; reliability; self-organizing energy networks

Das FUSE Testbed: Aufbau eines Microgrids für Smart Grid-Sicherheitsexperimente.

Eine zuverlässige und effiziente Energieversorgung basiert nicht nur auf einer lokalen Steuerung, sondern auch auf gesammelten Sensordaten und Messungen an verteilten Standorten. Daher gewinnt die Übertragung von Sensordaten mittels geeigneter Kommunikationsnetze an Bedeutung. Die damit zunehmende Bedrohung durch mögliche Angriffe ist einer der Hauptgründe für den Aufbau des FUSE Testbeds – ein experimentelles Microgrid für Smart Grid Forschung. Mit dem FUSE Testbed sollen Experimente im Bereich Smart Grid Sicherheit, Netzoptimierung, Stabilisierung und Inselbetrieb durchgeführt werden. In diesem Artikel wird, aufbauend auf dem aktuellen Stand der Technik in der Microgrid-Forschung, das FUSE Testbed vorgestellt. Weiters werden erste Versuchsanordnungen im FUSE Testbed mit Schwerpunkt Teil-Installation von Messgeräten und Komponenten zur Datenerhebung und -analyse beschrieben.

Schlüsselwörter: Microgrids; Smart Grid Sicherheit; Energieversorgung; Kommunikationsnetz; Inselbetrieb; PMU; Zeitsynchronisation; Dezentralisierung; Angriffe; erneuerbare Energie; Versorgungszuverlässigkeit; selbst-organisierende Energienetze

Received November 17, 2016, accepted January 9, 2017

1. Introduction

The current electricity infrastructure is evolving. Decentralized power generation demands more sophisticated control methods, Information and Communication Technology (ICT) components increase the risk for cyber-attacks and classical hierarchical top-down structures tend to be substituted by cell-based architectures, based on microgrids. A microgrid consists of several distributed generators as well as loads, storages and information and communication technology for monitoring and control operations. Through the Point of Common Coupling (PCC) it can connect to (grid connected, parallel mode) and disconnect from (islanding, autonomous operation) the main grid [7]. The ability of a microgrid to separate itself from the main grid and operate autonomously is very useful in case of faults and disturbances in the main grid.

In decentralized approaches system-parts, e.g. generators, loads, storages, microgrids and grid controllers need to communicate with each other and interact with each other. The next generation grid is being formed; the smart grid. Major challenges in ensuring a reliable and efficient energy supply include, but are not limited to: the growing complexity of the grid due to the increasing number of renewable and distributed energy sources, the necessary energy saving and demand response strategies to optimize the energy flow, as well as the various components, protocols and sensors involved in the data transfer, protection and control actions. Communication is a crucial component for a proper and reliable operation of a smart grid. However, this leads to new vulnerabilities due to possible attacks. In order to investigate attack scenarios and their impact on grid operation and control actions, an experimental microgrid facility is being established at the TU Wien for research on Future Self-Organizing Energy Networks (FUSE, https://fuse.project.tuwien.ac.at/).

2. FUSE goals

The FUSE project's main goal is to support the investigation of smart grid research questions by experiments in a real testbed with microgrid components. The project focuses on research questions on decentralized grid structures that consist of interconnections of microgrids. Microgrids are the key components in decentralized grid topologies and offer a broad range of opportunities for a flexible grid operation, which ideally uses self-organization to react to

Xypolytou, Evangelia, TU Wien, Institute of Telecommunications, Gußhausstraße 25, 1040 Vienna, Austria (E-mail: evangelia.xypolytou@tuwien.ac.at); **Fabini, Joachim,** TU Wien, Institute of Telecommunications, Gußhausstraße 25, 1040 Vienna, Austria (E-mail: joachim.fabini@tuwien.ac.at); **Gawlik, Wolfgang,** TU Wien, Institute of Energy Systems and Electrical Drives, Gußhausstraße 25, 1040 Vienna, Austria (E-mail: wolfgang.gawlik@tuwien.ac.at); **Zseby, Tanja,** TU Wien, Institute of Telecommunications, Gußhausstraße 25, 1040 Vienna, Austria (E-mail: tanja.zseby@tuwien.ac.at)

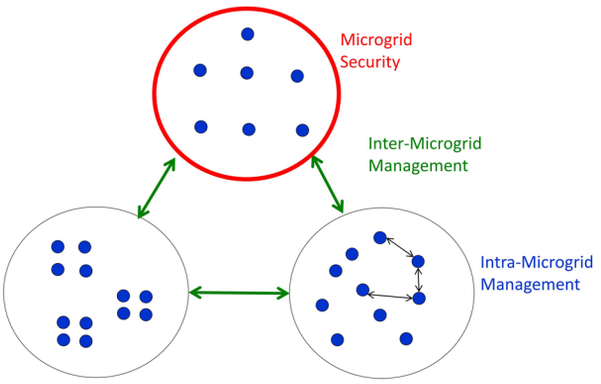

Fig. 1. FUSE objectives

changing boundary conditions. Nevertheless, self-organization requires situational awareness. Internal microgrid operation as well as the controlled interconnection of microgrids is challenging regarding supervision and control. Expertise in both fields, i.e. in energy and communication, is required to address those challenges.

The FUSE project has its focus on the following key research aspects:

- *Intra-Microgrid Management:* Exploration of methods for microgrid self-management (stabilization, optimization) based on data collection and situation-dependent decision processes.
- *Inter-Microgrid Management:* Investigation of methods to autonomously control the interactions in a grid of microgrids, which includes processes for situation-dependent decisions regarding interconnections and islanding options.
- *Microgrid Security*: Investigation of security methods to prevent, detect and mitigate attacks as basis for self-protection functions in intra- and inter-microgrid communication.

Future challenges in smart grid technologies require experts familiar with both, the energy and the communication domain. Therefore, besides the scientific objectives of the project it is also planned to exploit data and infrastructure in research-oriented teaching and establish research and teaching resources that can be shared with others (Fig. 1).

3. State of the art: microgrids and grid monitoring

A microgrid, as already mentioned, is an energy system that is connected to the main grid through one or more Points of Common Coupling (PCC). It usually consists of several distributed generators as well as loads, storages and information and communication technology for monitoring and control operations. A microgrid can operate in two different modes: grid-connected (parallel mode) and islanded mode (autonomous operation) [7]. The ability of a microgrid to separate itself from the main grid and operate autonomously is very useful in case of faults and disturbances in the main grid. After normal operation of the main grid has been restored, the microgrid can be reconnected to it. While detailed simulation models of microgrid components exist and can be used for analysis and planning of microgrids, real infrastructure is required, not only to validate the simulation models, but also to improve them and to allow investigations of the complex interaction of smart grid components and ICT infrastructure [8], especially related to advanced methods of microgrid control [9–12].

The communication network is a key component for a reliable and robust power grid. Important information about the status of the power grid, as well as failures or attacks can be extracted from measurement data, which is why their correct transmission through the communication network is of great importance. Measurement data recorded by metering equipment must not only be accurate and reliable but also provided in real-time in order to contribute to diagnostics and control actions. Every power system nowadays is equipped with SCADA (Supervisory Control and Data Acquisition) systems. Remote Terminal Units (RTUs) [1] support the reading of unsynchronized measurement values for a specific time interval. The measurement of complex power flows enables the calculation of bus voltages as a basis for state estimation.

Recently deployed Wide Area Measurement Systems (WAMS) use Phasor Measurement Units (PMUs) to measure voltage phasors directly. In theory such a WAMS infrastructure can offer an accurate snapshot of the network state at any point in time without state estimation. The deployment of PMUs on one hand increases demands with respect to the capacity and latency of communication networks [2]. On the other hand, the ability of PMUs to measure fine granular time-synchronized information is advantageous for grid management. PMUs sample the sinusoidal waveforms and estimate a synchrophasor equivalent of an alternate current waveform, while using the Global Positioning System (GPS) technology to accurately timestamp phasor measurements [3–5]. The C37.118.1 standard addresses the measurement aspects of voltage phasors, frequency, rate of change of frequency, while the C37.118.2 standard addresses the communication aspects for data exchange. Analytics and diagnostic applications based on PMU data include phase angle deviations, oscillation monitoring, voltage stability monitoring, fast frequency decline, sudden change of active/reactive flows, cascading events, topology detection and others, whereas control applications may include microgrid controlling, intentional islanding, and Volt-Var optimization [1, 6].

However, in practice, the limited number and high cost of PMUs result in SCADA measurement data to be mixed with PMU data for state estimation purposes in today's systems. In the FUSE network PMUs will be installed, among other sensors.

4. Overview of the FUSE experimental facility

The FUSE microgrid experimental facility will consist of renewable generators, among which photovoltaic appliance and wind emulator, storages, controllable loads, sensors and actuators. The FUSE facility is established within a cooperation of three research groups and two Institutes of the Faculty of Electrical Engineering at TU Wien, Austria. Figure 2 depicts the components and structure of the FUSE microgrid.

4.1 FUSE energy grid

The PV generation will consist of two or three PV appliances with an individual rating of 1 kW_{peak} to approximately 10 kW_{peak}, i.e. ratings which can be expected for such installations in urban and suburban grids to be operated as a microgrid in the future. Wind energy conversion will be emulated with a wind energy emulator that has a power rating of approximately 25 kW, suitable to represent small wind turbines under different control regimes. The storage capacity of the battery storage will also be used for tests for the integration of charging stations and battery electric vehicles (BEV) into the distribution grid, and thus will be of a size comparable to those found in current state of the art over BEV, i.e. 20–30 kWh. Load behavior of the microgrid will be emulated using an electronically controllable load in the range of 10 kW to 12 kW. Parallel operation of the microgrid with the main grid can be either simulated by using a real time network simulator and a 4 quadrant amplifier or the microgrid can be directly connected to the existing low voltage grid on site.

4.2 FUSE ICT architecture

In order to fulfill the goals of the FUSE testbed for microgrid self-management (stabilization, optimization), situation-dependent decisions regarding interconnections, islanding, detection and mitigation of attacks, data collection is a necessity. Data from each consumer, producer and storage of the testbed will be recorded by smart meters. Apart from that, PMUs will be installed for a synchronized and highly accurate measurement of frequency, voltage and current phasors. The PMUs will have an important role on the decisions regarding islanding, synchronization of the microgrid with the main grid and reconnection.

All IP connections between grid components in the FUSE experimental testbed will run over switched 1 Gbit/s Ethernet copper wires or, alternatively, optical lines to span distances that exceed the maximum Ethernet range. In order to model more realistic WAN scenarios, including higher latencies because of the microgrid's geographical distribution, a Linux NetEm [13] based WAN emulator will be tightly integrated with the FUSE ICT network. The emulator features an extendable number of Ethernet interfaces and acts as an Ethernet bridge, which is why it is fully transparent to the end systems communicating over IP. Emulator features include symmetrical or asymmetrical, deterministic or statistical delay, loss, and delay variation. Therefore, the testbed will be able to emulate communications with sensors and actuators over typical asymmetrical access networks like 3G, 4G or VDSL. We expect the communication delays to be a decisive factor that influences the performance of grid control algorithms and limits the achievable grid stability.

The analysis of grid communications and security aspects is supported by the ability to accurately capture time-stamped packets on all WAN emulator ingress and egress interfaces. For the moment, tcpdump captures can be started remotely on any emulator interface and write the resulting capture files to the WAN emulator file system. The resulting files are valuable for both, real-time and post-event analysis. In addition, it is planned to use the resulting data files as input for control algorithm simulations and for the testing of anomaly detection algorithms.

4.3 Time synchronization

The main prerequisite for accurate correlation of network events is a common synchronized time base for all components that generate events and network traces. FUSE relies on Global Positioning System (GPS) Pulse per Second (PPS) based time synchronization for accurate clock synchronization of PMUs and the WAN emulator. PMUs and the WAN emulator use separate, dedicated GPS antennas and GPS/PPS DSPs for local clock synchronization. Linux-based computers in the FUSE testbed acquire the accurate GPS/PPS time signal delivered by Copernicus II DSPs through the computer's serial RS232 interface and the LinuxPPS kernel driver.

5. Planned experiments

The FUSE testbed provides a highly flexible environment and allows the possibility to perform a variety of experiments. We describe below three examples of experiments that are already planned in the project proposal and are significant for testbed requirements and the testbed design.

Experiment Set 1: grid stability control

In this set of experiments various control algorithms are tested on failures or attacks that endanger grid stability. It is investigated how fast failures can be detected and how fast countermeasures (such as load shedding) can be invoked and if (and how fast) grid stability can be re-established.

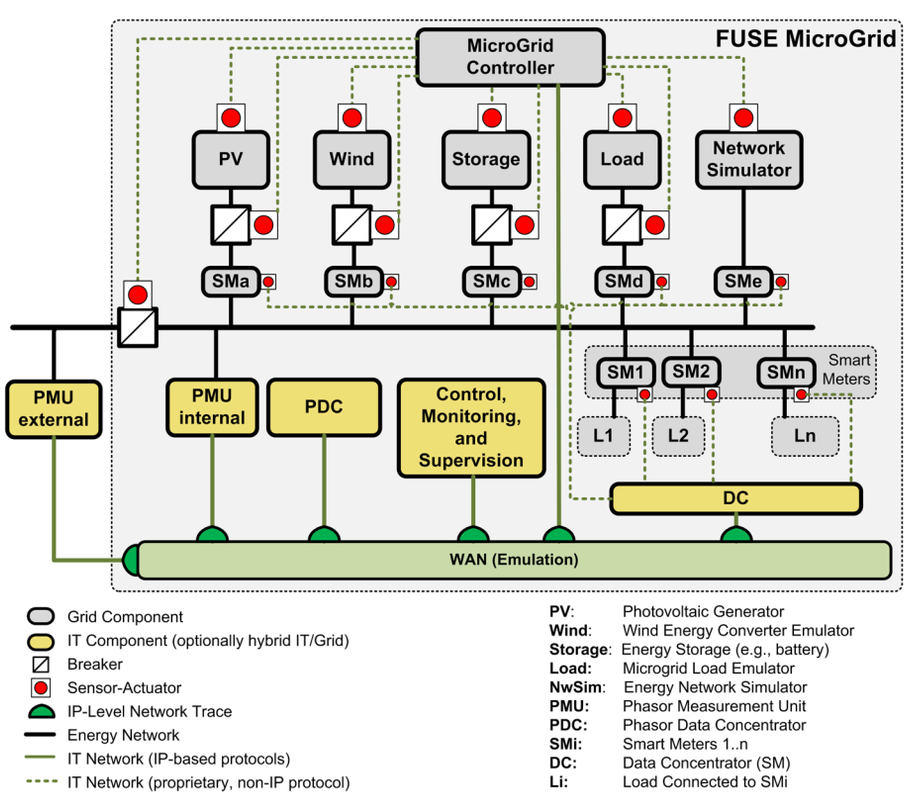

Fig. 2. FUSE experimental facility

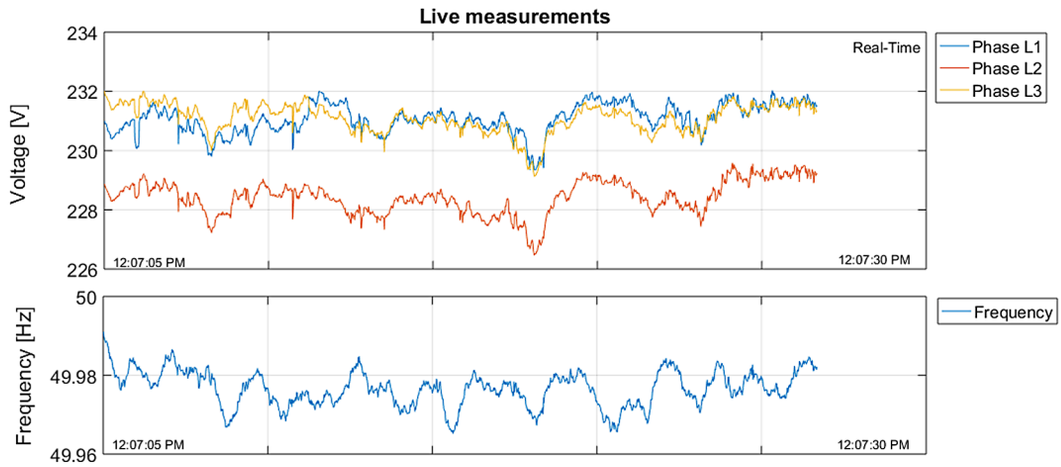

Fig. 3. Live PMU measurements using openPDC for showing voltage and frequency variations over time

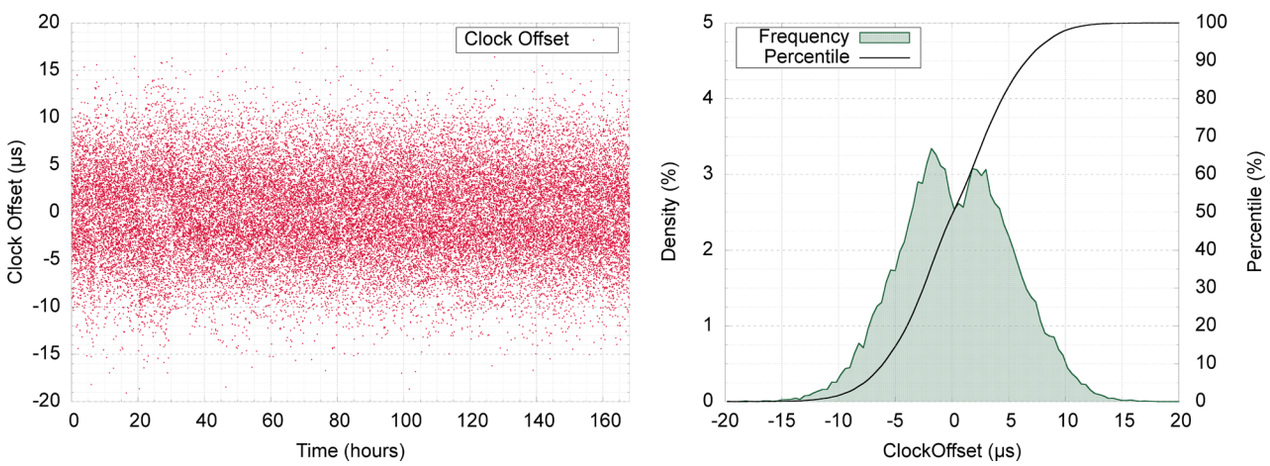

Fig. 4. System clock time synchronization performance

- *Data required from testbed:* Sensor data from PMUs and other metering devices, accurate time measurements, packet-delay measurements
- *Collected results:* Detection rate, stabilization time, accurate fine grained supervision data from all phases
- *Testbed requirements:* Islanding capability, capability to invoke failures and unstable situations without influencing the public power grid, accurate clock synchronization, capability to combine simulation, emulation and testbed devices

Experiment Set 2: behavior models

In this experiment set collected data will be used for the development of models and training of model parameters for normal grid operation. These models will provide the basis for prediction methods and the detection of deviations from normal operation.

- *Data required from testbed:* Sensor data from several distributed sensors, accurate time measurements from devices
- *Collected Results:* Grid behavior models and model parameters
- *Testbed requirements:* Capability to set different grid states, accurate clock synchronization, capability to combine simulation, emulation and testbed devices

Experiment Set 3: cross layer detection algorithms for cyber security

In this set of experiments cross layer anomaly detection will be tested. Anomalies can be caused by failures, misconfigurations or by malicious attacks. For this, data is gathered from sensors, log files, system data and network data from different layers in the FUSE testbed and will be analyzed and correlated. Although physical attacks are also possible, the FUSE project will first concentrate on attacks on IT components and communication. Different scenarios and use cases will be selected, including various IT infrastructure attacks, such as Denial of Service, eavesdropping, data injection and data modification. Since devices can always have undetected vulnerabilities, we also assume zero-day exploits in the scenarios. The detection quality and speed of different methods will be compared and evaluated. Combined models for the detection of anomalies both in communication network and electrical (micro)grids contribute significantly towards proactive planning and self-organizing energy networks.

- *Data required from testbed:* Sensor data from several distributed sensors, log files from devices, network measurement data (different layers), accurate time measurements
- *Collected Results:* Detection speed, detection quality

- *Testbed requirements:* Islanding capability, capability to invoke passive and active attacks (eavesdropping, man-in-the middle, denial of service), capability to combine simulation, emulation and testbed devices, accurate clock synchronization

In all three experiment sets, clock synchronization plays an essential role. It is needed to accurately monitor grid states and correlate distributed information to achieve situational awareness across multiple devices. In real environments, it is unlikely to have accurate time information available at all devices. In the FUSE testbed we equipped devices with GPS clock sync and distribute network time protocol information in the local network. This makes it possible to establish a fine grained view for situational awareness and to accurately correlate information from system logs, network measurements and grid sensors.

In the current testbed (as of December 2016) the following components have been already installed: a set of smart meters, a meter data collector, a phasor measurement unit (PMU), a phasor data collector (PDC), several GPS receivers with connections to servers and PMU, hardware and software components for the sensor data collection, including a storage solution and a data processing cluster. Further PMUs and the interconnection of the components to further equipment is currently in progress.

6. Initial experiments for testbed establishment

An experimental set up of a single PMU (Arbiter 1133A) has been installed in the Institute of Telecommunications' Cyber-Physical Systems (CPS) laboratory. Initially, the communication between the corresponding PMU and a computer was tested through PMU model specific software. In the case of Ethernet connection, the properties of the communication can be alternated as far as the protocol is concerned (TCP/UDP), the number of frames per second, the device ID and others. Live visualization of the measurements (voltage and current magnitudes and angles) as well as data storage is possible. However, this serves only for the configuration, data visualization and storage of a single PMU device. For the scope of the FUSE testbed, a Phasor Data Concentrator (PDC) is necessary, which collects, visualizes, stores, aggregates and if needed sends the data from multiple PMUs to further concentrators (e.g., Super Phasor Data Concentrator, SPDC) or a central control center. Voltage and current phasors, frequency and statistical information (e.g., frames per second, time quality errors) are some of the data the PMU sends to the PDC. For this purpose, the open source software openPDC is deployed in the CPS laboratory. Data storage can be configured through historian adapters for various output streams that range from local comma separated value (CSV) files to remote SQL databases and other storage options. Power output calculation adapters are also provided by the software. Visualization of live measurements is also enabled, Fig. 3.

The data collected from the PMU devices and smart meters will be used as a basis for developing and investigating methods to detect failures and attacks. The ability of the PMUs to measure synchronized phasors with high resolution and accuracy enables not only the investigation and development of algorithms, which can detect slow evolving abnormal changes of metrics like, e.g., voltage magnitude or phase, frequency and others, but also the analysis and correlation of measurement data, which can only be realized in such a testbed. Preliminary tests of the WAN emulator clock synchronization performance on a 19″ HP Proliant DL120G6 with Celeron 2.2 GHz CPU running Linux confirm the expected, satisfactory accuracy as shown in Fig. 4. The results are based on the Network Time Protocol (NTP) daemon's loopstats log file. Analysis of an exemplary chosen weekly NTP log file for week 40, 2016, confirms that the system clock is at any time within a window of ±20 µs to UTC. Moreover, the Cumulative Distribution Function (CDF) in Fig. 4, right, illustrates that 90 % of all system clock values stay within a narrow window of 15 µs (±7.5 µs) to UTC.

7. Conclusion

The experimental FUSE microgrid facility is described and first experimental installation of measurement equipment, data collecting and storing are presented. Based on the collected data from measurement equipment, methods and algorithms to detect anomalies both in the electrical and the communication networks will be developed and tested in the experimental facility. Security, timely data transfer and reliability of communications will be evaluated in the testbed in order to enhance situational-awareness as a step forward in evolving grids into self-organizing networks.

Acknowledgements

Open access funding provided by TU Wien (TUW). The research in this paper is supported by the TU Wien Project "Future Self-Organizing Energy Networks" (FUSE, https://fuse.project.tuwien.ac.at/).

References

1. Savulescu, S. (2014): Real-time stability in power systems: techniques for early detection of the risk of blackout. Berlin: Springer.
2. Deng, Y., et al. (2012): Networking technologies for wide-area measurement applications. In Smart grid communications and networking. Cambridge: Cambridge University Press.
3. Sridhar, S., Hahn, A., Govindarasu, M. (2012): Cyber-physical system security for the electric power grid. Proc. IEEE, 100(1), 210–224.
4. Martin, K. E. (2011): Synchrophasor standards development—IEEE C37.118 amp; IEC 61850. In 44th Hawaii international conference on system sciences, HICSS (pp. 1–8).
5. Franco, R., et al. (2013): Using synchrophasors for controlled islanding—a prospective application for the Uruguayan power system,". IEEE Trans. Power Syst., 28(2), 2016–2024.
6. Yhou, Y., et al. (2016): Abnormal event detection with high resolution micro-PMU data. In 19th power systems computation conference.
7. Siemens (2011): Microgrids. White paper.
8. Li, W., et al. (2014): Cosimulation for smart grid communications. IEEE Trans. Ind. Inform., 10(4), 2374–2384.
9. Bertagna De Marchi, S., Ponci, F., Monti, A. (2013): Design of a MAS as Cloud Computing Service to control Smart Micro Grid. In IEEE PES ISGT Europe 2013, Lyngby (pp. 1–5).
10. Dragicevic, T., et al. (2014): Advanced LVDC electrical power architectures and microgrids: a step toward a new generation of power distribution networks. IEEE Electrif. Mag., 2(1), 54–65.
11. Papathanassiou, S., Hatziargyriou, N., Strunz, K. (2005): A benchmark low voltage microgrid network. In Proceedings of the CIGRE symposium: power systems with dispersed generation (pp. 1–8).
12. Dragicevic, T., Guerrero, J. M., Vasquez, J. C. (2014): A distributed control strategy for coordination of an autonomous LVDC microgrid based on power-line signaling. IEEE Trans. Ind. Electron., 61(7), 3313, 3326.
13. Hemminger, S. (2005): Network emulation with NetEm. In Proceedings of the 6th Australia's national Linux conference, LCA2005, Canberra, Australia.

Authors

Evangelia Xypolytou
received her diploma degree in electrical and computer engineering at the polytechnic school of the Aristotle University of Thessaloniki, Greece, and a master degree in the field of automation from the National Technical University of Athens, Greece. She worked as supervisor of electromechanical installations in commercial buildings and hardware-software developer for automation systems. She is currently a Ph.D. candidate at the Vienna University of Technology, Austria, in the field of Smart Grids, early detection of cascading events, microgrids and energy forecast.

Joachim Fabini
holds a diploma degree (Dipl.-Ing.) in technical computer sciences and a Ph.D. (Dr. techn.) in electrical engineering, both from Vienna University of Technology (TU Wien), Austria. After five years of R&D in telecommunications industry he joined the Institute of Telecommunications (formerly Institute of Broadband Communications) at TU Wien in 2003, where he is teaching master-level courses and leading applied research projects. Since 2013 he has been Senior Scientist with the Communication Networks group at the Institute of Telecommunications. His main research interests include measurement methodologies and metrics in packet-switched networks, time synchronization, and network architectures for secure communication in critical infrastructures.

Wolfgang Gawlik
graduated from Friedrich-Alexander-University (FAU) Erlangen-Nuremberg, Germany, in electrical engineering, focus on energy technology. Until his appointment as University Professor for Energy Systems Technology at the Institute of Energy Systems and Electrical Drives at Vienna University of Technology, Austria, in 2011 he was Senior Key Expert System Dynamics and Project Manager at Siemens Power Technologies International. His research interests are Supergrids, Smart Grids/ Microgrids and Electromobility, Universal Grids and software for network analysis, planning and steady state and dynamic modeling.

Tanja Zseby
is a Full Professor of communication networks and Head of the Institute of Telecommunications at the Faculty of Electrical Engineering and Information Technology at Vienna University (TU Wien) of Technology, Austria. She received her diploma degree (Dipl.-Ing.) in electrical engineering and her Ph.D. (Dr.-Ing.) from TU Berlin, Germany. Before joining TU Wien she led the Competence Center for Network Research at the Fraunhofer Institute for Open Communication Systems (FOKUS) in Berlin and worked as visiting scientist at the University of California, San Diego. Her research focus is network security, anomaly detection and secure smart grid communication.