COORDINATION OF THE ISLANDING AND RESYNCHRONIZATION PROCESS OF MICROGRIDS THROUGH A SMART METER GATEWAY INTERFACE

Buchner Matthias[1], Manswet Banka[1], Rudion Krzysztof[1]

[1]Universität Stuttgart Institute of Power Transmission and High Voltage Technology, Stuttgart, Germany

Keywords: Microgrid, Islanding, Resynchronization, Smart-Meter-Gateway, Real-Time-Simulation

Abstract

Microgrids represent a promising way of integrating renewable energies and increasing security of supply. This is achieved by aggregating the producers and consumers into a controllable unit and the ability of island operation in case of failure. In order to implement these demanding processes, advanced communication technologies are necessary. Smart meter gateway technology is the ideal solution for this task, as it enables a secure channel down to the smallest unit in the energy network. In this paper the suitability of the smart meter gateway technology for controlling a microgird is investigated. In order to create a realistic test scenario, a microgrid, which is simulated on a real-time simulator, is controlled by a power grid control system via a smart meter gateway. The suitability of the smart meter gateway technology for this purpose was proven by the simulation of an islanding of the microgrid with subsequent resynchronization to the power grid controlled by the power grid control system.

1. Introduction

In recent years, distribution systems have been confronted with an increasing penetration of inverter-based, distributed generators and storage, which has enabled the operation of parts of the system as islanding-capable microgrids. The generation of electricity in microgrids, which is largely based on renewable energies and close to the consumption, and the intelligent integration of flexibilities through an energy management system actively reduce CO2 emissions and reduce operating costs. By operating microgrids as stand-alone units, the supply quality for the consumers can be improved and the supply reliability can be increased through the ability of islanding operation in the event of a fault [1]. This transition from interconnected to islanded operation and vice versa is a critical point in the operation of microgrids [2].

Information and communication technology is a critical component of future power networks. Beyond any doubt, the control and operation of the future power grids, including microgrids, needs to be supported by sophisticated information systems and advanced communication networks, which ensure a stable and secure communication. Currently, several technologies have been used or tested in distribution systems and it is expected that their usage will become more extensive during the coming years. [3].

The Smart Meter Gateway Technology (SMGW)[4] which is being developed into an infrastructure information system and a central communication and data platform as part of the C/sells project[5], is one way of satisfying the challenging requirements of microgrid communication. The SMGW is the central communication unit of an intelligent measurement system developed according to the specifications of the German Federal Office for Information Security (BSI) [6]. The main task of the SMGW is the secure data transmission in the intelligent measuring system.

Under these aspects, this paper aims to investigate the suitability of SMGW technology for controlling a microgird. For this purpose the system architecture of the SMGW technology is described and the structure of the experimental setup is described in section 2. In section 3 the simulation results are evaluated which is follow by a conclusion of the suitability of the SMGW technology for the control of microgrids in section 4.

2. Methodology

In this section the basic functions of the SMGW are explained. Furthermore, the experimental setup is described and the procedure for carrying out the experiment is explained.

2.1 The Smart Meter Gateway Architecture

The SMGW forms the central communication unit in an intelligent metering system. It ensures secure communication through an integrated security module and is the central component for receiving, processing and storing measurement data. The SMGW is able to connect different communication areas via 3 interfaces (see Fig. 1). It is responsible for encrypting all communication connections and for ensuring that only known participants and devices are trusted [7].

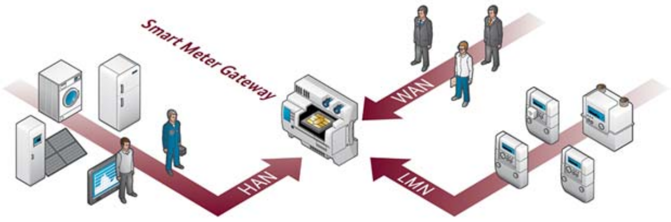

Fig. 1 The SMGW and its environment [6]

2.1.1 The Smart Meter Gateway Administrator (SMWGA): A SMGWA is a trustworthy entity, which has undergone a complex certification process at the BSI. They manage the authentication process of the encrypted transport channels between the SMGW and the remote site [6].

2.1.2 The Local Metrological Network (LMN): According to the technical guideline, the LMN interface can be designed either as a short-range radio interface (wireless Mbus) or as a serial interface[6]. Via the LMN interface the SMGW communicates with the connected meters (electricity, gas, water, heat) of one or more end consumers. The meters communicate their measured values via the LMN to the SMGW.

2.1.3 Wide Area Network (WAN): The WAN interface is designed as an IP interface. For security reasons, all communication connections originate from SMGW[6]. These connections can be established by the SMGW at specified times via a tariff application case. However, in order to be able to react to spontaneous events, the SMGW can be prompted to establish a connection via a wake-up by a SMGWA. Via the WAN interface the SMGW is integrated into a public key infrastructure and all communication is encrypted with TLS.

2.1.4 Home Area Network (HAN): The HAN interface is designed as an Ethernet interface and serves to integrate the SMGW into the customer's home network. Controllable devices such as intelligent household appliances or an energy generator can be connected to it. The HAN interface also includes a Controllable Local System (CLS) interface, which enables remote access to controllable generators (photovoltaic system, combined heat and power plant) and controllable load devices (charging station, night storage heating).

2.2 Structure of the Experimental Setup

The explanation of the experimental setup is divided into the description of the microgrid model, the islanding and resynchronization process and the hardware test setup.

2.2.1 Microgrid Model: The test network consists of a droop controlled battery see Fig. 2 which provides the voltage and frequency in island operation, a PV system, which feeds a specified power into the microgrid and a load [3]. A microgrid central controller (MGCC) offers an external interface and regulates the exchange power at the point of common coupling (PCC) by controlling the coefficients of the droop curve of the battery [3]. The MGCC is also responsible for the secondary control in isolated operation and coordinates the resynchronization of the microgrid with the power grid. A breaker performs the separation of the microgrid from the main grid and measures the current as well as the voltage on both sides for resynchronization purposes.

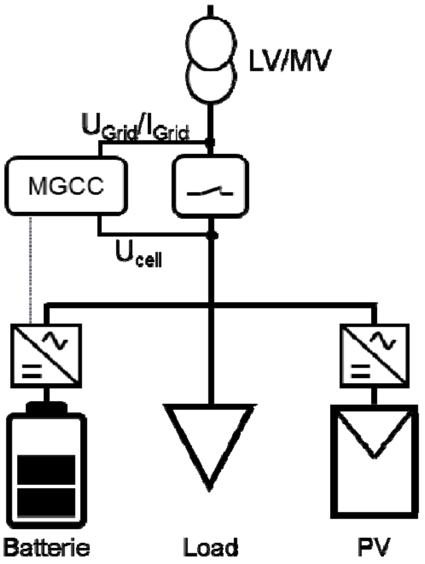

Fig. 2 Microgird test setup

2.2.2 Islanding and Resynchronization Process: In order to guarantee stable operation of the microgrid in interconnected and islanded operation as well as to ensure a smooth transition from interconnected to islanded operation and a seamless resynchronization of the microgrid with the interconnected grid, the process as in Fig. 3 was designed. The microgrid is initially in interconnected operation with the grid, in which the microgrid is perceived as a controllable unit from the viewpoint of the power system. In this mode the microgrid feeds or draws a specified power from the grid. When the command to form an island network is given, the MGCC reduces the exchange power with the power grid. When the islanding criterion is met, the breaker at the PPC opens, thus ensuring a smooth transition from interconnected to island operation. Once the decision to resynchronize has been made, the voltage amplitude, frequency and phase of the microgrid and the main grid are synchronized to the grid voltage to prevent damage to devices in the microgrid. When the differences in voltage amplitude, frequency and phase meet the resynchronization conditions, the breaker is closed and the microgrid returns to interconnected operation.

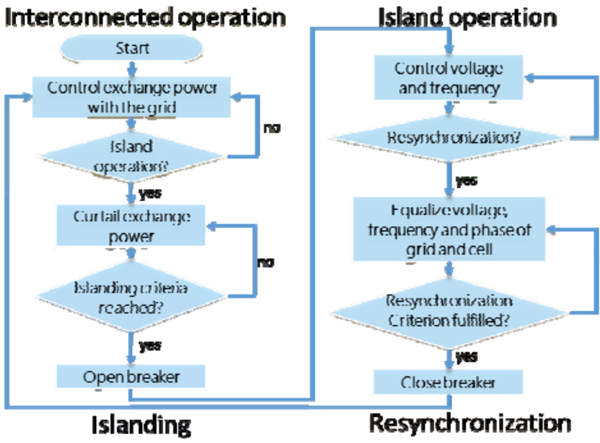
Interconnected operation
Island operation
Start
Control exchange power with the grid
Island operation?
no
yes
Curtail exchange power
Islanding criteria reached?
no
yes
Open breaker
Islanding
Control voltage and frequency
Resynchronization?
no
yes
Equalize voltage, frequency and phase of grid and cell
Resynchronization Criterion fulfilled?
no
yes
Close breaker
Resynchronization

Fig. 3 Islanding and resynchronization process

2.2.3 Establishment of a Communication Channel: The experimental setup is shown in Fig. 4. If the power grid control system (PGCS) wants to send commands to the MGCC, it must send a request to the SMGWA to establish a connection. The SMGWA checks the authorization of the request and sends a command to the SMGW to establish a TLS-channel to the PGCS. The PGCS is not able to establish a connection to the SMGW on its own, since the communication channel must always be established by the SMGW. Once the safe TLS channel is established, communication in both directions between the real-time simulator and the PGCS is possible. For this purpose, a CLS device converts the commands from the PGCS into TCP-Modbus and forwards them to the real-time simulator via the local network. In the opposite direction, the CLS device forwards the measurements from the real-time simulator to the PGCS via the HAN-interface of the SMGW.

For the experiment, a HIGH-LEIT PGCS and a ACOS730 CLS device are used. A ETH Smart Meter Gateway is applied and as real time simulator an Opal-RT 5600 is used.

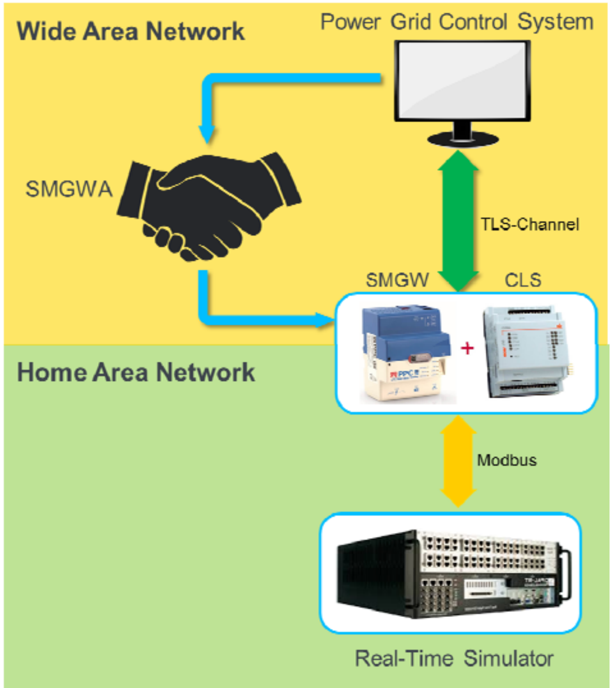

Fig. 4 Hardware test setup with SMGW-infrastructure and Real-Time Simulator

3. Results

The response of the individual components to the islanding and the resynchronization can be seen in Fig. 5.

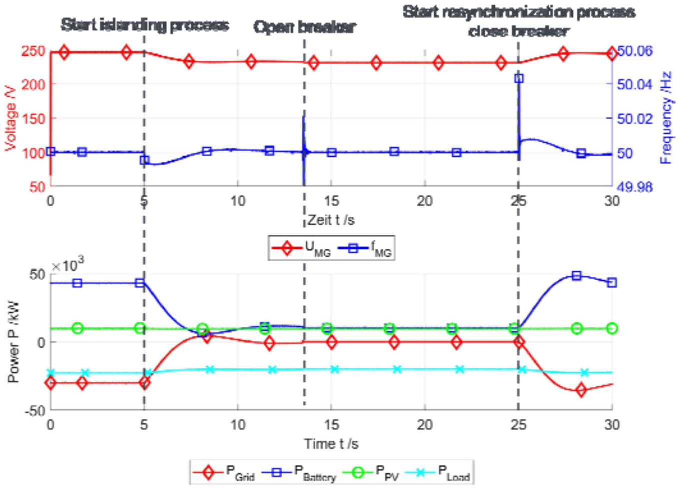

Fig. 5 Controlled islanding and resynchronization process of the simulated microgrid

U_{MG} stands for the voltage at the PCC and f_{MG} represents the frequency within the microgrid. P_{Grid} is the power exchanged from the microgrid with the grid via the PCC. P_{Load} is the power drawn from the load, $P_{Battery}$ is the power fed from the battery and P_{PV} is the power fed from the PV system into the microgrid. At the beginning of the experiment, the exchange power P_{Grid} is 30kW. It is represented as negative power flow out of the microgrid. The PV system feeds a constant power P_{PV} of 10kW into the microgrid over the entire experiment time period. The load draws a constant power P_{Load} of 20kW. With a power injection of 40kW, the battery maintains the balance of power. At time t = 5s the microgrid starts the islanding process. The exchange power with the power grid decreases until at t = 13.5s the islanding criterion is met and the breaker opens. The microgrid is now in island operation and the MGCC ensures that the voltage U_{MG} and frequency f_{MG} are maintained. At time t = 25s the resynchronization process is started. As the voltage U_{MG} had little time to move away from the grid voltage U_{Grid} the synchronisation condition is met immediately and the breaker is closed. The microgrid is back in interconnected operation and the MGCC immediately starts to regulate the set exchange power P_{Grid} of 30kW.

4. Conclusion

In this paper the suitability of the SMGW technology for controlling a microgrid was demonstrated. It was shown that the control of a microgrid via a SMGW is possible. The SMGW technology offers a promising platform for this purpose, which guarantees inherent secure communication as well as access authorization verification via the SMGWA. As this paper deals with the general feasibility of controlling a microgrid, there is still a need for further research. An investigation of the delays in the transmission of the control signals is of crucial importance, as too long delays can lead to instabilities. Another question is how fast and reliable the connection between the MGCC and the PGCS is. If the establishment of the connection takes too long or is unreliable, then SMGW technology is not suitable for time-critical applications such as the control of a microgrid.

5 Acknowledgements

This article was written as part of the C/sells project, which is funded by the German Federal Ministry for Economic Affairs and Energy.

6 References

[1] M. A. Hossain, H. R. Pota, M. J. Hossain, and F. Blaabjerg, "Evolution of microgrids with converter-interfaced generations: Challenges and opportunities," *Int. J. Electr. Power Energy Syst.*, vol. 109, no. October, pp. 160–186, 2019.

[2] T. L. Vandoorn, B. Meersman, J. D. M. De Kooning, and L. Vandevelde, "Transition from islanded to grid-connected mode of microgrids with voltage-based droop control," *IEEE Trans. Power Syst.*, 2013.

[3] N. Hatziargyriou, *Microgrids: Architectures and Control*, vol. 91. 2013.

[4] K. Förderer, M. Lösch, R. Növer, M. Ronczka, and H. Schmeck, "Smart Meter Gateways: Options for a BSI-compliant integration of energy management systems," *Appl. Sci.*, vol. 9, no. 8, p. 1634, 2019.

[5] M. Ronczka, R. Növer, A. Maximilian, T. Tröndle, and D. Stakic, "Aufbau eines Infrastruktur-Informationssystems zur Erschließung energetischer Flexibilität auf Basis intelligenter Messsysteme," Smart Energy Conference 2018 in Dortmund, 2018.

[6] Federal Office for Information Security, "BSI - Smart Meter Gateway." [Online]. Available: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/SmartMeterGateway/smartmetergateway_node.html. [Accessed: 21-Nov-2019].

[7] B. für S. in der Informationstechnik, "Technische Richtlinie BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines," *Bsi Tr-03109-1*, 2019.