Practical Implementation of Optimal Voltage Control in Distribution Network – System Verification, Testing and Safety Precautions

Kalle Ruuth
Electrical Engineering
Tampere University
Tampere, Finland
kalle.ruuth@tuni.fi

Antti Supponen
Electrical Engineering
Tampere University
Tampere, Finland
antti.supponen@tuni.fi

Sami Repo
Electrical Engineering
Tampere University
Tampere, Finland
sami.repo@tuni.fi

Kenneth Røsland Rosenørn
Danish Energy Association
Frederiksberg, Denmark
krr@danskenergi.dk

Philip Douglass
Danish Energy Association
Frederiksberg, Denmark
pdo@danskenergi.dk

Michael Møller
Operations
RAH
Rinkøbing, Denmark
mm@rah.dk

***Abstract*— The focus of this paper is to provide information about the required testing methods for integrating smart control devices into part of substation automation. In the long-term demonstration, Substation Automation Unit (SAU) is utilized for Optimal Voltage Control (OVR) in 60 / 10 kV substation. The paper is providing verification and testing procedures beyond the algorithm testing to full-scale field demonstration of optimal voltage control. The proposed testing methods and innovations ensures robust, reliable and fail-safe optimal voltage control. The OVR system is installed in parallel with the conventional Automatic Voltage Regulation (AVR) system. System core functionality is to monitor and control the network state to achieve voltage levels throughout the network as close to nominal as possible. Despite the extensive system verification and testing, optimization errors, network topology changes or any kind of disturbance or fault condition in network, power system or in SAU must not cause voltage level violations or wrong operation actions. Information security vulnerabilities especially related to General Data Protection Regulation (GDPR) must be minimized with cyber security precautions.**

Keywords*— *Cyber security, GDPR, Optimal Voltage Control, Practical Implementation, Substation Automation, System Verification

I. Introduction

Recent development in energy production from centralized units to Distributed Generation (DG) with e.g. wind turbines or solar panels is changing the traditional radial distribution networks in many ways including voltage management. The load demand is also increasing due to heat pumps and electric vehicles and turning more and more into flexible load due to utilization of demand response, self-generation and storage. These new challenges are encouraging new smart control systems to be developed [1].

The focus of the OVR project [1] is to utilize previously designed optimization algorithms to develop and demonstrate a smart voltage regulation system that will optimize the voltage level in whole distribution grid. The demonstration focuses on secondary voltage control utilizing an enhanced control of the AVR of the On-Load Tap Changer (OLTC) using network-wide information. The idea may be extended to all voltage controllers in distribution grid [2, 3] but only the AVR of OLTC is included in the demonstration. The decision to control the tap changer is influenced firstly by the primary substation voltage and secondly by voltages in every node of the network, losses of the network, near future control needs, etc. The secondary control will enhance the hosting capacity of distribution network for DG and other Distributed Energy Resources (DERs) like electric vehicles, heat pumps and electricity storage. The same system might also be utilized to minimize network losses, degradation of voltage level quality and number of OLTC actions [4]. The same system might also be utilized to minimize network losses, degradation of voltage level quality and number of OLTC control actions.

The project utilizes the existing hardware installed at the MV substation (60 / 10 kV) with few additional computing and communication components and making active use of smart meter data. The main functionalities hosted in SAU are production and load forecasting, network State Estimation (SE) and Optimal Power Flow (OPF) calculation. In addition, SAU also hosts functionalities to ensure decent quality of data, logging and collection of historical data and making control decisions. Detailed description of SAU may be found here [5]. The system needs to continue operating correctly under any kind or power system or control system failure.

No data used for control should be vulnerable for cyber-attacks. Additionally, the General Data Protection Regulation (EU 2016/679) (GDPR) places high demand for system data integrity and security since preparation of demonstration system contained data that could be associated to individual electricity user. The handling of the sensitive data must fulfill the requirements of the projects data agreement and furthermore the GDPR requirements.

In this paper, the testing methods and implementations with safety precautions needed for maximizing the robustness of the parallel voltage control systems are described. The aim of the proposed system design, implementations and test is to ensure secure and safe long-term demonstration in a substation, parallel with the existing AVR system but also develop system verification principles to any other smart grid applications. Even very complex control algorithm's and system design tests can be relatively simple with software and hardware-in-the-loop simulations [6] but when implementing the system for a field demonstration the situation changes. The system tests must cover all the aspects from hardware-in-the-loop simulations to signal cable protection, communication, and correct operation of the control in any system, communication or grid condition.

II. DESCTIPTION OF OPTIMAL VOLTAGE CONTROL SYSTEM

The OVR AVR is operating in parallel with the existing RAH (DSO in the project) AVR as shown in Fig. 1. The existing system consists of RAH AVR and the Motor Control Unit (MCU). Both AVRs are similar TAPCONs from Maschinenfabrik Reinhausen GmbH in order to prevent unexpected responsiveness. Parallel operation ensures that smart control system is unable to realize out of limits control actions and if it does not operate for any reason, there is always RAH AVR to control in traditional way.

For busbar voltage, the OVR AVR is exploiting the same measurement instrument as the RAH AVR. A National Instruments CompactRIO data logger provides feeder current measurements for the control system. The data logger was needed since cyber security policy of RAH prevented to receive measurements directly from substation automation to SAU (non-certified device), and Supervisory Control and Data Acquisition (SCADA) export could not provide measurements frequent enough. Data logger has two features; logging and averaging the measurements and act as an MMS Server, which publish all the feeder current measurements for SAU.

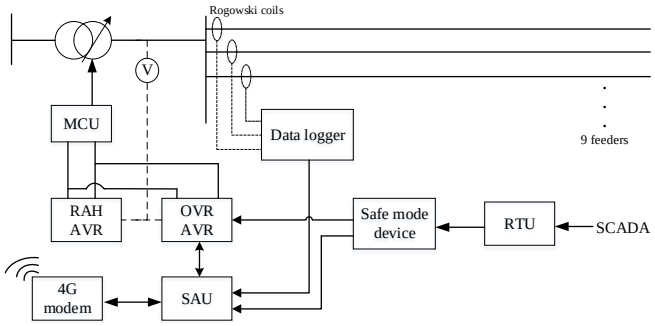

Fig. 1. Overview of the control system components

SAU is receiving secondary substation measurements through 4G modem. These measurements are provided by eight Power Quality (PQ) measurement devices Unipower PQ Secure UP-2210, measuring phase voltages and currents of secondary transformers. PQ-meters are located along medium voltage feeders in strategically selected locations from optimal voltage control viewpoint. These measurements provide important real-time inputs for SE in addition to primary substation measurements. However, most of the measurements in the SE are so called pseudo-measurements, which are taken from customer load profiles [7, 8]. Load profiles were created offline by clustering smart meter data of all customers of RAH based on data from one year. In the demonstration, load profiles utilized in the SAU are aggregated to secondary substation including only information about the number of different types of customer groups and the corresponding profiles. Therefore, the privacy risk at SAU is already reduced. 4G modem is utilized for remote control and supervision of SAU. Continuity of the demonstration is important, because the aim is to collect as much data as possible for statistical analysis of smart control system and grid voltages during the optimal voltage control. The safe mode device is the interface between SCADA and the smart control system. It is the critical safety feature to prevent any voltage violations in the grid. The SCADA control of the safe mode device allows the operator to select smart control system or traditional fixed voltage value. The blocking signal from RAH AVR has been implemented to prevent counteractions from OVR AVR. When RAH AVR is set to manual mode, it will automatically restraint all operation of OVR AVR.

Smart control system includes supervision of internal processes and if they are stopped or do not converge, they are automatically terminated and restarted. The normal interval of functions is one minute and if the termination or restarting process fails, an alarm will be sent if SE or OPF results are not received in two minutes. The smart control system may also have logical misbehavior during disturbances or conditions, which have not been tested, and therefore additional supervision is aiming to detect these situations for continuous development of the system during the demonstration. The remote access to system enables also updating the software and grid models in the SAU (due to extension of grid in the demonstration or the location of normally open switch changes). Automatic update of grid model in SAU is not implemented in the demonstration system but should be included in commercial product.

III. TESTING AND VERIFICATION

The system verification is extremely important when we are turning the scientific algorithm design and simulations into practical demonstration to ensure secure and safe long-term demonstration in the field. The designed system required some improvements, which were discovered during the Hardware-in-the-loop simulation laboratory testing.

A. Hardware-in-the-loop simulations

For preventing any issues in the operation principals, the control system requires functional and non-functional testing as identical operating environment as possible before taking it into the demonstration site. Real-Time Digital Simulation (RTDS) gives valuable feedback of the planned system operation. Utilizing RTDS for Hardware-in-the-loop (HIL) simulations, we can see the real-time effect of the parallel-connected control system utilizing the same implementation than in the demonstration and identify weak spots by stressing the complete system for different kind of disturbances and conditions.

In the HIL simulation, the OVR AVR and the safe mode device are connected to the RTDS. The simulation contains a simple network model with supplying grid, primary transformer including the tap changer, few feeders and a modelled AVR of OLTC (represents RAH AVR). The HIL setup is shown in Fig. 2. With signal amplifiers, identical voltages and currents from RTDS to the OVR AVR was created, which it will operate in the demonstration site. To avoid any unnecessary complexity in testing i.e. errors, the HIL simulations were conducted in different stages with identical control settings to the demonstration site.

Since SAU is constantly monitoring its own state and communications between interfaces, SAU and real-time measurements were tested separately. If SAU can't provide sufficient set point, it will automatically give the predetermined fixed set point. If SAU (MMS Client) is unable to read the real-time measurements, the fixed voltage value is set. If there is a power supply failure in SAU, the safe mode device activates the fixed set point value adjusted in TAPCON.

Second stage was to test the behavior of two parallel AVRs. The aim was to confirm that the two AVRs may operate in parallel with selected control parameters and smart

control system does not affect the reliability of the voltage control compared to traditional control system. The reliability was achieved with the implementation of safe mode device and the blocking signal from RAH AVR. When the RAH AVR is set to manual mode, interlocking of OVR AVR is activated.

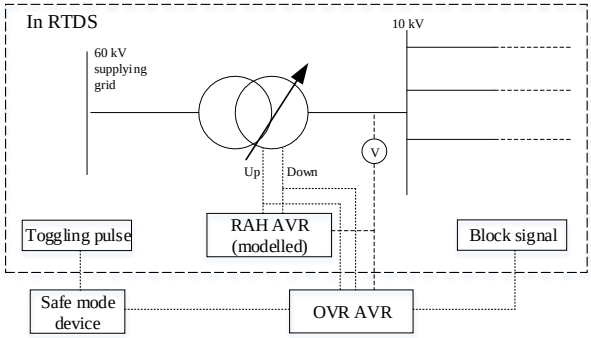

Fig. 2. HIL simulation setup

One major defective behavior founded during the HIL simulation was the tap position hunting. This means that the two AVRs are trying to counteract each other's control actions. Since RAH AVR has fixed voltage set point and the OVR AVR is continuously receiving different set point. The difference between these two can be enough to activate both controllers. This would harm the motor by increasing the tap position changes and shorten the OLTC lifespan dramatically. This creates also unwanted voltage variation into the network. The tap position hunting is prevented with modifications to the control software in SAU. The hunting is prevented by hardcoding bandwidth limits, which are not allowed to exceed, for the set points of OVR AVR in the SAU's MMS client communicating with OVR AVR. Although OPF or any other part of the system gives incorrect set point, it is not delivered to OVR AVR due to limits in MMS Client. This is a double precaution, because OPF has constraints for AVR set point and therefore it should not provide converged solution with incorrect set point. Discussions with the DSO responsible in the demonstration led to this arrangement, since they wanted to avoid any disturbance to grid operation during the demonstration. The simulation results of a successful tap position hunting test are shown in Fig. 3.

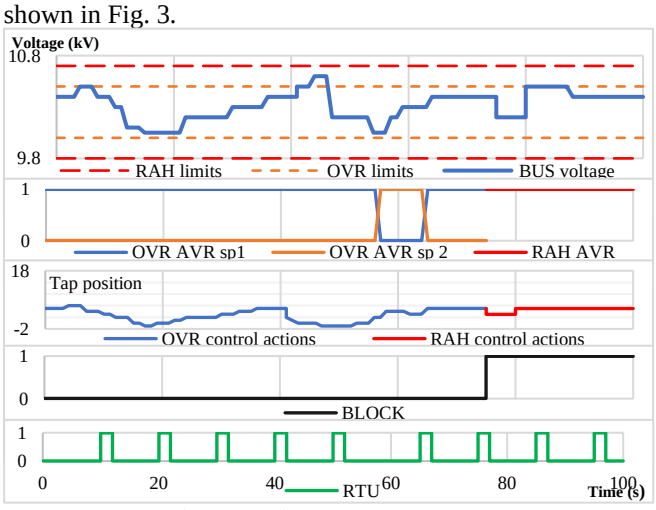

Fig. 3. Functional safety results from HIL-simulations

In the first graph the bus voltage level is presented in respect to the RAH and OVR bandwidth limits. The second graph is presenting the current active control mode (OVR setpoint 1&2 and RAH control). The OVR setpoint 1 is the smart control, which remain active when the Remote Terminal Unit (RTU) pulse from SCADA is in the accepted period (Fig. 5) and blocking signal is not active. Safe mode device won't be activated due to non-convergence solution, but SAU will send the same, fixed voltage setpoint as is activated by safe mode. With hardcoded restriction (OVR limits) to the control value, we are not violating the system requirements in any system malfunction event. This kind of behavior is automatically avoided in the simulations, but in practice, e.g. misreading from the measurement setup or other malfunction like communication error might eventually occur.

B. Interoperability testing

The data stored in SAU is modelled so that it conforms to the latest standard data models, IEC 61850 and IEC Common Information Model (CIM), to ensure interoperability and scalability [4]. Data handling and storage is done by using a relational database as an intermediate link between different parts of the system and functions. The main functions of the SAU are acquiring, storing and reporting measurements, production and load forecasting, SE, state forecasting and real-time power control by utilizing OPF. In addition, SAU needs a wireless internet connection to the cloud service called AirVantage where all measurements from PQ meters are collected. SAU (AirVantage Client) is periodically requesting data from the cloud service and the data is stored in the SAU database. In a similar way, the SAU (Data logger MMS Client) request periodically values from MMS Server of data logger and stores the values to the database. The third external interface is the OVR AVR MMS Client, which is writing new set point to OVR AVR and request the voltage measurement from it. In addition to external interfaces, SAU database is utilized by internal functions like SE and OPF. The illustration of SAU functionalities is presented in Fig. 4. In addition, SAU database includes off-line data e.g. MV network topology, impedances and location of aggregated customers etc. for network analysis and load profiles to create different customer groups.

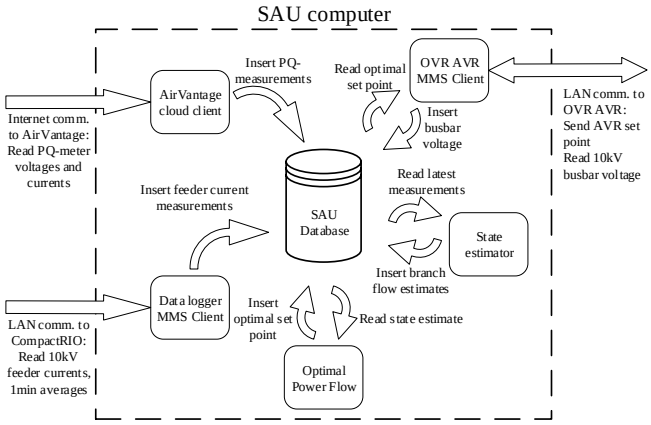

Fig. 4. SAU functionalities and data flow

The implementation of MMS Clients in SAU is based on open source library libIEC61850 [9] and the implementation of AirVantage Client is a tailored software. SAU database is utilizing Postgres, SAU is operated in Ubuntu (Linux) 18.04 and internal functions are running in MATLAB. All the functions and interoperability of database are tested in the

laboratory before installation tests. By utilizing Redundant Array of Independent Disks (RAID) for internal storage ensures data integrity and continuity of the operation even one of the used hard drives fails. This method mirrors the data for two physical disks, which will prevent data loss but also increases the reading speed. SAU is also programmed to be capable to continue providing control values even after unforeseen blackout by implementing task management after reboot.

C. *Safe mode device*

In the system design, the safe control mode was planned and when in safe mode, the control mode is the existing voltage regulation practice (with RAH AVR) at the demonstration site to maintain tolerable voltage level in every node. Since SAU is making decisions autonomously and for the demonstration it is not trivial to update the topology information of MV network on SAU in all practical cases, the demonstration will focus only on normal topology which will be in use most of the time. Information concerning topology changes was planned to be delivered through SCADA and RTU.

During the HIL simulations the detection of the need for particular system safety and controllability by network operator, the development of the safe mode device was conducted. Safe mode device is the interface between the SCADA and OVR control system to allow the system operator to decide whether the OVR system is allowed to operate or not and report the status to SAU. The operation principle is illustrated in the following Fig. 5.

The analog toggling pulse was implemented with RTU. In SCADA the control is only a toggle switch but the RTU is delivering a pulse (0-5 V), with interval less than 10 s. The reason for pulsing the signal is to prevent any communication issues between the control signal and Safe mode device. For example, if the smart system allowing pulse would be zero volts and the communication is lost, the five volts will not be delivered to activate safe control mode. Safe mode device receives the pulse and calculates whether the pulse period is less than the required. With pulse less than 10 s time between consecutive pulses, the safe mode device is allowing the OVR AVR to operate with variable set point and reports system status to SAU. The toggling pulse can be used by network operator e.g. when non-normal topology or any other occasion when the safe control mode is needed. With the functional verification in HIL simulations, the need for two operation schemes was discovered.

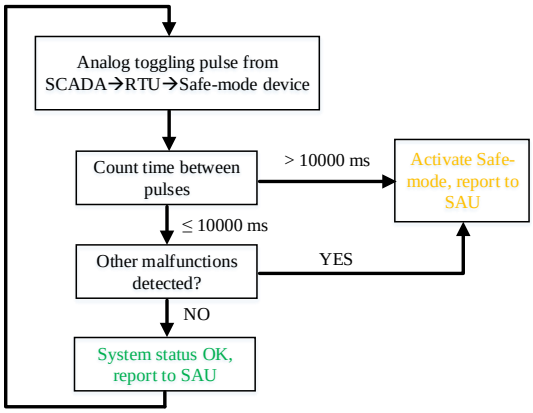

Fig. 5. Safe-mode device's operating principle

Smart control mode is accepting the set point changes for achieving the optimal voltage estimated by SAU. In safe control mode the OVR AVR has the same fixed voltage value, which is traditionally used in the RAH AVR i.e. with the implemented system, the safe control mode is utilized with safe mode device and OVR AVR. The RAH AVR is operated only when OVR AVR is blocked or out of power. For allowing SAU to control the set point value (i.e. OVR sp1) the OVR AVR digital input requires 220 VDC to remain in the set point 1. This method ensures the fail-safe operation and any malfunction in the control system won't violate the requirements.

After development and assembly of the Safe mode device, it requires testing as identical operating environment as possible (Fig. 2). All necessary inputs and outputs are connected into RTDS and OVR AVR, and their planned operation schemes with Safe mode device can be ensured already in the laboratory. In the field, Safe mode device is powered and communicating through SAU USB-port. This ensures the activation of safe mode when SAU is out of power but also allows serial communication through USB. OVR AVR registers 0 VDC as OVR AVR set point 2, i.e. traditional fixed voltage set point control. This method ensures the activation of the safe mode in any fault scenario.

D. *Development of the feeder current measurement system*

The measurement setup was developed with LabVIEW and CompactRIO (cRIO-9039). Installation included one Rogowski coil (Magnelab RCS-1800) for each phase of every demonstration network feeder. Since the IEDs and SAU data model are already using IEC 61850 protocol, the data logger is also configured to act as IEC 61850 MMS Server. The resolution of the measurement is 1-second RMS, but the bundle values updated to MMS Server are 1-minute average of the 1-second RMS values. By implementing the measurement setup, the installation site comes also into play. The feeder current measurement point and the data logger are located within 10-meter distance. The signal cables are vulnerable for electromagnetic fields occurring in the substation. The measured currents are delivered as a voltage signals from the coils to the data logger with twisted pair cable, which included foil shielding. The shielding is grounded from one end to eliminate potential for noise inducing loops.

IV. Cyber security and GDPR

The background and online data used in this project is considered sensitive and thus, by GDPR requirements, precautions are needed in order to ensure data protection and privacy. The main data that can be directly linked into a natural person is the Automatic Meter Reading (AMR) measurements collected from electricity users in the demonstration network and the physical locations of these measurement points. Additionally, the network model of the demonstration system only contains the MV network part with the low voltage level loads, which could be associated with a natural person, aggregated into a single medium voltage load. In this way the both, the location data and the energy consumption data of a single electricity consumer are not visible in the demonstration system [9].

Public internet connection to cloud services utilizes SSL encrypted HTTP protocol, which is generally considered to

be secure for this kind of application. The system maintenance requires remote connection to SAU, which is realized using Secure Shell (SSH) remote terminal login. The modem firewall in the system only accepts SSH connections from predetermined range of IP addresses and the SAU itself only allows logins for authenticated user. As the final security measure, the SAU hard drives utilize asymmetric encryption to prevent data compromise by theft.

V. Installation and Field Testing

Algorithms and functional parts of the smart control system are tested and confirmed to be working before taking the system into demonstration substation. However, on the demonstration site all communication and functional parts of the system requires testing. In the measurement setup, approval of the system operation requires testing in multiple pieces. The simplified list of functional and non-functional installation tests for the whole system are listed in Tab. 1.

TABLE 1. FUNCTIONAL AND NON-FUNCTIONAL TESTS

CASE SPECIFIC TEST (GENERAL CORRESPONDANCE)	DESCRIPTION	CASE SPECIFIC SUCCESS CRITERIONS(S)
Feeder current probe test (Measurement device test / calibration)	The instrument output is verified with oscillosscope	All probe outputs must produce a sinusoidal voltage signal
Feeder current measurement system tests (Real-time measurement setup verification)	The datalogger is connected to the probes turned on. The data logger output is then read with SAU	Data logger is delivering current values to external device via MMS Server. All probe outputs must be within the probe error tolerance (1 % of nominal). Currents must match SCADA measurements
Safemode device test (Critical system safety feature test)	The Safe-mode device will be fed a voltage pulse from waveform generator	When pulse is fed to the device the Safe-mode output must turn on. When pulse is discontinued the output must turn off
Demonstration LAN test (Local communication test)	All devices are connected to demonstration LAN (except for Safe-mode device and converter)	All devices answer ping. Remote connection to SAU from restricted IP-addresses is possible
OVR AVR active set point test (Control variable adjustment)	A new voltage set point is sent to OVR AVR via demonstration LAN	OVR AVR accepts the new setpoint
OVR AVR input test (Verification of control device's input signals)	OVR AVR is fed the voltage signal from substation voltage transducer. OVR AVR is given the tap position signal from tap changer	Voltage reading is correct. Tap position reading is correct
Tapcon block signal test (Manual override test)	Blocking signal is sent to OVR AVR	OVR AVR ceases all tap changer operation
OVR AVR safemode tests (Control device handling tests)	Safemode signal is discontinued from Safemode device to OVR AVR	OVR AVR changes to preset set point value and ignores any set point changes
AirVantage communication (Network communication test)	Try to reach out to the AirVantage service	Communication can be established, data can be stored to database
Remote communication	Try to establish connection from allowed PC	Connection successful and data exchange is possible

Every devices interoperability and functional and non-functional tests are carried out in the laboratory, but the system requires verification with identical tests at the operating environment with the full assembly of the system.

In the laboratory, e.g. SCADA control and communication between the two AVRs could not be tested (simulated and real hardware) but the functionality of the Safe mode device with the control signals during the HIL simulation was carried out. After the installation of all the hardware into the rack, the tests presented in Tab. 1 were carried out. Before advancing to the system commissioning, the system operation will be monitored with a "dry run", i.e. the system will be in operation, but the control signals to the tap changer are still disconnected.

VI. Conclusion

This paper has presented the outline for system verification and testing for implementing an experimental voltage control setup in field demonstration. The testing workflow should include laboratory verification for devices behavior in as identical operating environment as possible. The system validation should follow the following guidelines: First, the verification of system design on offline simulation testing. Second, the individual testing of system components, and finally the testing of the full system at field.

The information security should be considered through the whole system design and testing. The GDPR imposes strict regulation on data associated with an individual person. The best approach is to omit using data that can be associated to single natural person in these kinds of demonstrations by aggregating and anonymizing the data as much as is practically possible.

The presented tests on safety and system security and reliability are in a sense generalizable in comparable systems, although some aspects of the tests presented are case specific and only applicable to this demonstration as such. The analysis of system limits, like in this case the control voltage band, should be considered regardless the control variable.

Acknowledgment

We would like to thank the Energy Technology Development and Demonstration Program (EUDP) who have funded and made this research possible.

References

[1] Optimal Voltage Regulation homepage. [Online]. Available: https://www.optimalvoltage.com

[2] A. Kulmala, M. Alonso, S. Repo, H. Amaris, A. Moreno, J. Mehmedalic, Z. Al-Jassim: Hierarchical and Distributed Control Concept for Distribution Network Congestion Management, IET Generation, Transmission and Distribution, 2017. [Online]. Available: https://doi.org/10.1049/iet-gtd.2016.0500

[3] H. Reponen, A. Kulmala, V. Tuominen, S. Repo, Distributed automation solution and voltage control in MV and LV distribution networks, IEEE PES ISGT Europe 2017 Innovative Smart Grid Technologies Conf., 26-29 September 2017, Torino, Italy.

[4] A. Kulmala, S. Repo and J. Pylvänäinen, Generation curtailment as a means to increase the wind power hosting capacity of a real regional distribution network, CIRED - Open Access Proceedings Journal, 2017. [Online]. Available: http://doi.org/10.1049/oap-cired.2017.0925

[5] A. Angioni, S. Lu, H. Hooshyar, I. Cairo, S. Repo, F. Ponci, D. Della Giustina, A. Kulmala, A. Dede, A. Monti, G. Del Rosario, L. Vanfretti, C.C. Garcia, A distributed automation architecture for distribution networks, from design to implementation, Sustainable Energy, Grids and Networks, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.segan.2017.04.001

[6] V. Tuominen, H. Reponen, A. Kulmala, S. Lu, S. Repo: Real-time hardware- and software-in-the-loop simulation of decentralized distribution network control architecture, IET Generation, Transmission and Distribution, 2017. [Online]. Available: http://dx.doi.org/10.1049/iet-gtd.2016.1570

[7] A. Mutanen, P. Järventausta, S. Repo, Smart Meter Data-Based Load Profiles and Their Effect on Distribution System State Estimation Accuracy, International Review of Electrical Engineering, 2018. [Online]. Available: https://doi.org/10.15866/iree.v12i6.13419

[8] A. Mutanen, M. Ruska, S. Repo, P. Järventausta: Customer classification and load profiling method for distribution systems, IEEE Transaction on Power Delivery, 2011.

[9] Open source libraries for IEC 61850 and IEC 60870-5-104. [Online]. Available: https://libiec61850.com/libiec61850

[10] General Data Protection Regulation (EU) 2016/679 [Online]. Available: http://data.europa.eu/eli/reg/2016/679/2016-05-04