SCALABLE POWER SYSTEM COMMUNICATIONS EMULATION WITH OPC UA

Marius STÜBS[†*] Paulius DAMBRAUSKAS[‡] Mazheruddin H. SYED[‡] Kevin KÖSTER[†]
Hannes FEDERRATH[†] Graeme M. BURT[‡] Thomas STRASSER[§]

[†] University of Hamburg, Germany
*stuebs@informatik.uni-hamburg.de
[‡] University of Strathclyde, U.K.
[§] AIT Austrian Institute of Technology, Austria

ABSTRACT

The dependability on real-time control is significantly increasing due to the transition from synchronous grids to converter-dominated grids. Distributed control schemes can significantly decrease the degree of single-points-of-failure of Smart Grid control schemes, thereby introducing new complexity of power system communications. We propose a scalable approach for validation of distributed control schemes by emulating the communication in a decentralised manner, utilising the Open Platform Communications Unified Architecture service-oriented architecture in a controller-hardware-in-the-loop environment. As a proof-of-concept, we apply communication delay Denial-of-Service attacks to a converter-dominated communication-heavy and consensus-based microgrid control algorithm and thereby elaborate how scalable power systems communications emulation can help selecting appropriate mitigation strategies for telecommunication-based stress conditions.

INTRODUCTION

The power grid is changing with new technologies being constantly introduced into the system. Two of the major changes are the increasing penetration of non-synchronous generation and the increasing use of and dependence on internet protocol (IP) based telecommunications systems as shown in Figure 1. These new technologies provide with functionality to im-prove the reliability and efficiency of the power system but at the same time introduce concerns in terms of stability and security. Thus, power systems, as critical infrastructures in general, are increasingly susceptible to cyber-attacks. Since the first politically-motivated targeted attack against power grids in 2015, resulting in outages affecting 230,000 people, awareness for security counter measures has risen. It is well established that control algorithms utilised by the grid require thorough testing before its large scale roll out and deployment. Yet, the established testing procedures for validation of existing Smart Grid functionalities focus primarily on basic robustness requirements and rarely address the telecommunications performance and cyber security related concerns [1]. The missing awareness for cyber security risks is also reflected by its missing consideration in the Technology Readiness Levels (TRL) acquisition process.

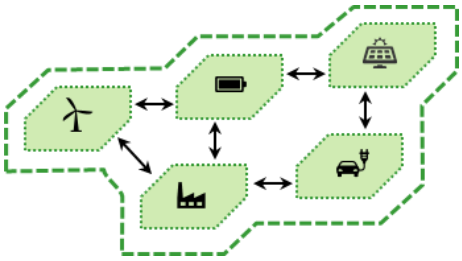

Figure 1 - Exemplary Micro Grid with five nodes and partially meshed peer-to-peer communication

Open Platform Communications Unified Architecture (OPC UA) is an industrial machine to machine communication protocol comprising robust security considerations and a flexible information model [2]. Its use for semantic Smart Grid services is a promising approach for future distributed control algorithms. We propose a framework based on a distributed publisher-subscribe implementation of OPC UA for testing of wide area telecommunications dependent control systems. The framework provides with ability to automatically apply various telecommunications-based stress conditions like the effects of a denial-of-service attack, loss of communications, loss of data, corruption of data, etc.

To advance the knowledge on reliable power systems performance and security assessment in the face of cyber-attacks, we propose a data and communication model that is suitable for the assessment of security of future Smart Grid controls, focusing on evaluation of the performance in the telecommunication between the power system's nodes and the effects on reliability of insufficient performance due to disturbances on the communication links, which may or may not be caused by denial-of-service attacks. We further propose a decentralised approach on assessment of power system performance and security. Our main contribution is to show the suitability and requirements of OPC UA as a distributed service in the context of industrial use, by implementing both OPC UA server and client on each node, thus creating a fully distributed telecommunications architecture. Since in this setup neither OPC UA nor the framework are dependent on any central component, the approach is highly scalable and therefore suitable for emulation of communications and integration into test-beds for investigation of large smart grids.

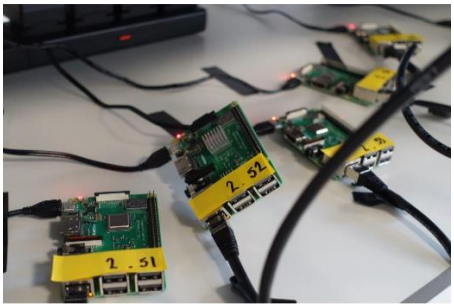

Figure 2 - Five Raspberry Pi embedded devices, each controlling one of the power converters.

To demonstrate the applicability of this approach, we investigate a distributed consensus algorithm for secondary frequency control in an islanded micro-grid as proposed in [3]. Five agents are used in a Controller-Hardware-in-the-Loop (CHIL) setup controlling battery energy storage systems (BESS) on a 400V radial distribution network running on a Real Time Digital Simulator (RTDS). We present a general approach of scalable power system communications emulation with OPC UA and its contribution to the standardisation of Smart Grid control validation and testing.

EMULATION OF TELE-COMMUNICATIONS NETWORK PERFORMANCE

IP based telecommunications networks follow a similar architecture in terms of performance as the power grid, with networks of greatest capacity spanning over long distances, which then branch out into shorter range lower capacity networks all the way to the customer. The communications networks used in traditional power systems only utilised the long-range networks but with the introduction of smart gird, the power system telecommunications are expected to expand all the way to the customer premises. Telecommunications network categories along with their expected performance are shown in [4] which are separated into the following categories:

1) Core Network
2) Wide Area Network (WAN)
3) Neighbourhood Area Network (NAN)
4) Home Area Network (HAN)

Also, the performance within the categories can vary greatly based on the specific technology used. The assumed communications network for the use case in this paper is a NAN utilising Power Line Communications (PLC) technology via a radial 400V power line connecting all of the houses in a neighbourhood. The capacity of a PLC system over 400V would have an expected bandwidth of around 128kbit/s shared between all the houses in the neighbourhood thus depending on how communications traffic intensive an application is and how many devices communicate, the overall performance of such a communications network can vary greatly. The best way to measure this performance is by observing the delay which is added to the application by the communications network. Theoretically a 100-byte packet travelling over such a network, assuming no other traffic is present, would experience around 6.25ms of serialisation delay and less than 100µs combined from propagation, queuing and processing [4]. This communication technology has very low bandwidth when compared to most of modern telecommunications systems thus the performance degradation of PLC can be quite rapid and can potentially reach a latency of multiple seconds. In the rest of the paper, latency will be used as a representation of the communications network performance and will be used to analyse the resiliency of the control algorithm to the degradation of communications network performance and for the more extreme levels of latency as a potential denial of service cyber-attack.

POWER SYSTEM AND USE CASE

Fast and stable frequency control is particularly important in islanded microgrids since it is unlikely that the available generation in such a power system will be synchronous. In a low inertia power system, the frequency can be quite volatile and thus a telecommunications-enabled automatic secondary frequency control is necessary in order to maintain an operational microgrid. Thus, to evaluate the proposed communication emulation architecture for smart grid applications, we investigate a use case of distributed and communications dependant secondary frequency control in an islanded microgrid with converter-dominated power generation. The power network consists of a single three phase 400V power line with five BESS operating as

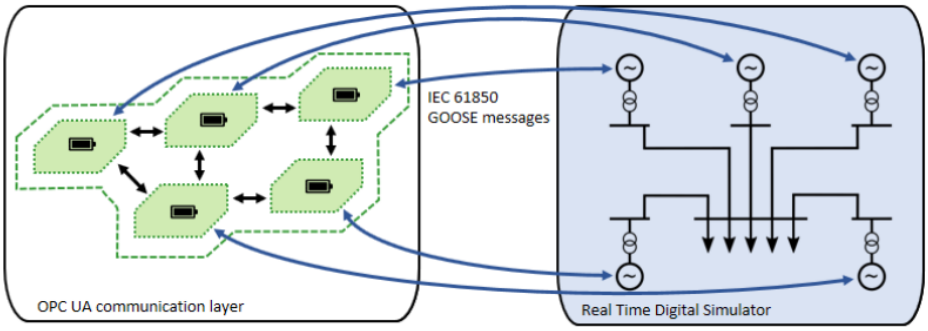

Figure 3 - Communication relations of the experiment setup.

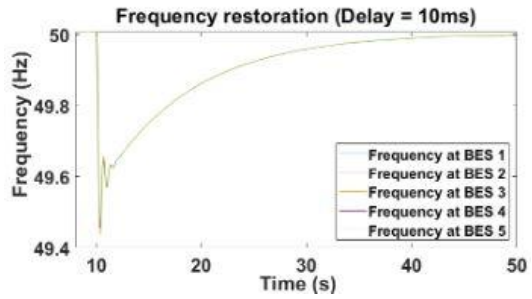

Figure 4 - System frequency deviation and near optimal response.

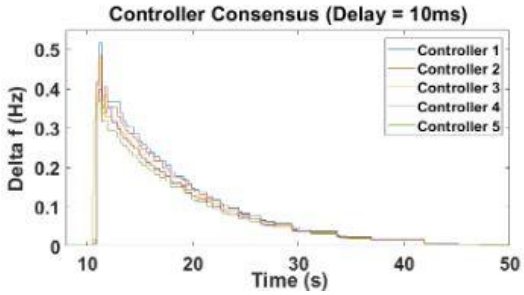

Figure 5 - Controller consensus steps near optimal in case of 10 ms delay.

converter connected generation with parameters shown in Table I. The batteries and converters are simulated in RTDS and controlled in real time by five Raspberry Pi (RPI) embedded devices, as shown in Figure 2, each controlling one of the microgrid's converters via the IEC 61850 GOOSE messages in a CHIL setup as shown in Figure 3. The RPIs provide the secondary frequency control using a communications dependant consensus algorithm for coordinating the response of each BESS similarly to the use case presented in [3] with the addition of the telecommunications emulation between the controllers which is facilitated by the OPC UA framework. Each run of the experiment is recorded for 200 seconds. At first, the frequency is exactly at 50 Hz, as desired.

At *t=10s*, the power load is activated, resulting in a drop of frequency, as shown in Figure 4. The primary frequency control stops the drop of frequency at 49.6 Hz and at this point the operation of the secondary frequency control begins and restores the frequency to its nominal value within a 50s period. This power system frequency disturbance is achieved with a load step of 20kW going from 40 kW to 60 kW as the total load, such a load change could be achieved by turning on a fast electric vehicle charger [5]. The distributed consensus algorithm for secondary frequency control as shown in previous publications, adjusts the power output of the BESS proportionally to the consensus reached on the magnitude of the current frequency deviation from the observation point of each individual BESS as shown in Figure 5. Such control provides a smooth frequency restoration to the nominal frequency as previously proven in [3].

Device	Parameter	Value	Parameter	Value
Inverter 1	Power	3 kW	Droop	100 Hz/kW
Inverter 2	Power	8 kW	Droop	200 Hz/kW
Inverter 3	Power	11 kW	Droop	50 Hz/kW
Inverter 4	Power	10 kW	Droop	100 Hz/kW
Inverter 5	Power	9 kW	Droop	250 Hz/kW
Secondary controller (PI)	k_p	0.01	k_i	0.12

Table I - Converter Parameters

SCALABLE TESTING FRAMEWORK ARCHITECTURE

To scalably evaluate the resilience of power systems, we elaborate the architecture of a testing framework with the following properties:

Multi-Stage Testing: Established communication simulation frameworks such as OMNeT++ are limited to show properties of a simplified model of the investigated control. After validating these models, the actual implementation is still subject to the simplifications of the power system and control. Therefore, CHIL testing [6] can provide the necessary fidelity in all aspects which is an important feature to validate the control architecture design on every step of the development.

Real-time Capability: The proposed framework is implemented using an event-based architecture, enabling real-time response to messages by an actual cyber-physical system.

Distributed Operation: The framework allows to compile the investigated communication emulation configuration to single executables that run for example on x86 and on ARM processors. Thus, the controller logic can distributed on the embedded devices. Maximum scalability can be achieved by using as many embedded devices as power nodes are in the cyber-physical system.

Efficiency: With code written in C++, the measurable delay between an input from the cyber-physical system and the framework's response is less than a micro second on the used RPi type 3B embedded devices.

Configurable Multi-Stage Stress Conditions: The proposed communication emulation architecture supports normal operation with default ethernet delay as well as configurable delays, message drops and message duplication on the Open System Interconnection (OSI) model application layer. The behaviour can be remotely switched between a set of configurations, realising a multi-stage testing environment.

Extensibility and Open-Source: Providing the source code of the testing framework allows for increased extensibility and more specific test-cases [7].

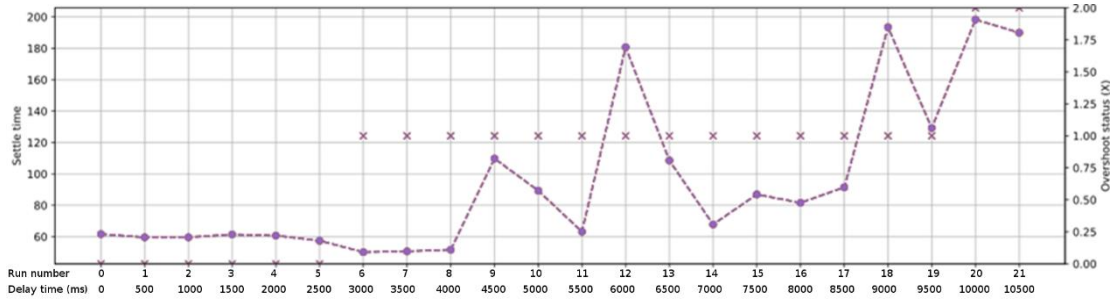

Figure 6 - Settle time and overshoot indicator for an exemplary set of runs.

Setup Phase

In the setup phase, the configuration for the communication emulation is loaded into the utilised instances, in our example realised by directly copying the adjusted configuration files on each embedded device. Note that it is also possible to use Docker container to run the emulation entirely as a simulation.

OPC UA Server-Push Message Delivery

OPC UA is a server-client based communication protocol. Thus, it consists of two separated parts in the communication strategy. The server is delivering values, while the client is retrieving messages. Our approach thus combines the server part and the client part in each node. Any node's client connects to the server value register and subscribes to the desired value, thus getting updates immediately. Any message to be sent is written into the value register and updated on change, thus delivering the message to the subscribed clients. This approach is robust to Denial-of-Service (DoS) attacks, since the submitted value is persistent at the server and can be retrieved at any later time, as opposed to one-time-messages. This type of server-client architecture is commonly established in the Internet of Things (IoT) domain, where weak and/or sporadic connectivity is a common property.

Multi-stage communication testing

In our multi-stage testing, we investigate the effect of OSI application layer message delays. In each stage of the experiment, the applied communications delay is increased, starting from no delay in steps of 500ms up to 10 seconds of delay for the last run.

RESULTS AND DISCUSSION

The optimal solution *d* [Hz per second] is found with zero delay, when all participating nodes agree to gradually change the micro grid's measured frequency towards the nominal frequency of 50 Hz. The gradual adjustment *d* is applied until the next iteration of consensus is reached. The settle time of the algorithm in respect to applied communications latency is depicted in Figure 6. The Figure can be divided into three zones. The first includes run 0 to run 5, with delays of up to 2500ms, where no observable effect on the outcome can be seen. The algorithm is therefore found to be resilient against this kind of delay. The second zone includes 6 to 8 represent delays between 3000ms and 4000ms. In this zone the algorithm reaches the nominal frequency of 50 Hz actually faster than normal, but with the disadvantage of overshooting the 50 Hz line, as depicted in Figure 7. Due to the delay in communication, the executing of the assumed optimal solution *d* turns out to even be counter-effective. This effect is observable in Figure 8 in second 40. The applied delay is 6500 ms. Using the delayed data from second 33.5, the erroneously assumed optimal solution *d* is to further increase the frequency, although in second 40 the system frequency is already above 50 Hz.

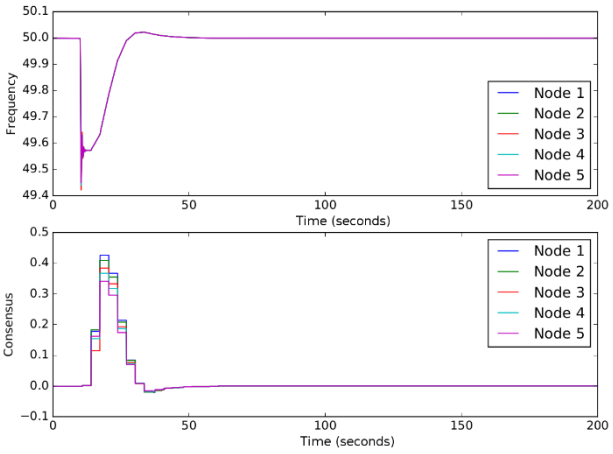

Figure 7 - Slight overshoot in Run 6 with delay 3000 ms.

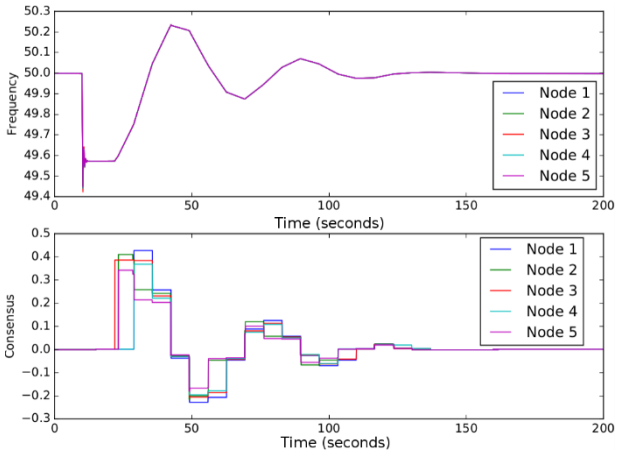

Figure 8 - Multiple overshoots in Run 13 with delay 6500 ms.

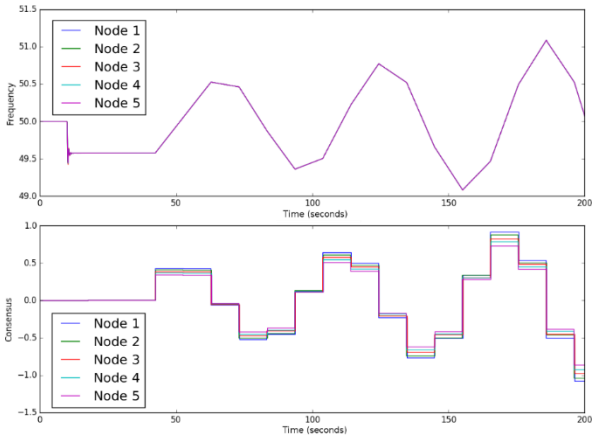

Figure 9 - Run 20, with 10000 ms of communication delay.

The third zone includes runs 9 to 17. Between 4500ms and 8500ms delay applied to the reference implementation of the investigated control scheme, the overshoot is significant, and the convergence time increases beyond acceptable values. The fourth zone includes all runs from run 18. From 9000ms on, multiple overshoots can be observed systematically, as depicted in Figure 9. Also, the convergence time exceeds the 200s observation time, indicating that no convergence can be reached at all.

From the experimental results, we can derive two main suggestions for improvement of the investigated control scheme. First, it is necessary to apply an additional data validation logic that prevents the execution of obviously wrong decisions, e.g. further increasing the frequency when exceeding the nominal frequency. This means using locally available information to override false, global decisions. The second recommended measure is to introduce timestamps to the messages. Although this poses additional requirements, such as timing synchronization between the substations, it also eliminates the delay or replay of outdated measurements.

RELATED AND FUTURE WORK

Recent publications describe several Smart Grid testbeds for validation of control schemes, but it generally lacks for testbeds for real-time multi-agent-based control schemes [8]. Our approach aims to progress the state-of-the-art by introducing a new focus on scalability and distributed execution. Scalability testing does not stop at distributing the grid operation towards the actual energy generating resources. It also requires smart decisions towards dynamic hierarchical structuring of multiple micro grids. Our next step will be to describe the inter-operability between multiple microgrids and investigate their resilience regarding DoS attacks on a larger scale. Also, false-data-injection is a serious threat that needs further investigation. In our following research, we will use our framework to investigate existing data validation schemes to show that scalable resilience testing is also applicable and necessary for defending against malicious participants within Smart Grids.

CONCLUSIONS

Control of distributed cyber-physical systems is in transition. In this paper, we show that the resilience of Smart Grid control is more and more dependent on the performance of the communications system. Our research aims to improve the methodology of communications resilience testing and to improve the understanding of interdependencies between power systems and communications. We show that a focus on scalability even increases the applicability of our methods. The proposed testing architecture provides an additional tool to aid the research community and to unifying CHIL testing on the different levels during development. This progresses the joint efforts towards making the Smart Grid a reality.

REFERENCES

[1] M. Maniatopoulos et al. “Combined control and power hardware in-the-loop simulation for testing smartgrid control algorithms”. In: IET Generation, Trans-mission & Distribution 11.12 (2017), pp. 3009–3018.

[2] A. Claassen and S. Rohjans and S. Lehnhoff, “Application of the OPC UA for the Smart Grid”. In: 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, pp. 1–8.

[3] T. L. Nguyen et al. “Agent based distributed control of islanded microgrid-Real-time cyber-physical implementtation”. In: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2017 IEEE PES., pp. 1–6.

[4] P. Dambrauskas et al. “Impact of realistic communications for fast-acting demand side management”. In: CIRED - Open Access Proceedings Journal 2017.1 (2017), pp. 1813–1817.

[5] S.-H. Ahn et al. “Implementation of 60-kW fast charging system for electric vehicle”. In: Industrial Electronics Society, IECON 2013 - 39th Annual Conference of the IEEE. IEEE. 2013, pp. 7256–7261.

[6] T. Strasser et al. “Applying open standards and open source software for smart grid applications: Simulation of distributed intelligent control of power systems”. In: Power and Energy Society General Meeting, 2011 IEEE. IEEE. 2011, pp. 1–8.

[7] M. Stübs and K. Köster. “OpenDISCO – Open simulation framework for distributed smart grid control”. In: Energy Informatics 1.1 (2018), pp. 343-348.

[8] M. H. Cintuglu et al. “A Survey on Smart Grid Cyber-Physical System Testbeds.” In: IEEE Communi-cations Surveys and Tutorials 19.1 (2017), pp. 446–464.

ACKNOWLEDGEMENTS

This work has been elaborated within the ERIGrid project / TA programme, supported by the H2020 Programme under Grant Agreement No. 654113, and by the German Federal Agency for Economic Affairs and Energy.