# Co-simulation Aspects for Energy Systems with High Penetration of Distributed Energy Resources

Miloš Cvetković, Kaikai Pan, Claudio David López, Rishabh Bhandia, and Peter Palensky

***Abstract*— Distributed energy resources (DERs) have seen significant expansion in utilization over the past decade. This expansion is best observed with the rooftop solar panels whose penetration has substantially grown in terms of deployed MWs [1]. With the transformation of the grid towards more distributed supply of electricity, a new set of challenges arise. Although the challenges for adoption of DERs are plenty which span across technical, economical and policy domain, in this paper we discuss simulation challenges within two particular domains, cyber-security and voltage stability. For addressing each of these challenges, co-simulation has shown to be a promising path to take. Co-simulation (or combined simulation) represents the connection of two or more simulation tools with the goal of addressing a particular problem that neither one of these tools could address individually. Within each of these domains, we discuss the aspects for the design of co-simulation that one must consider when addressing the problem. The discussion is followed by short simulation examples.**

## I. Introduction

DERs come in all shapes and forms. Among different DER technologies, Photovoltaics (PVs) are the most prominent type constituting 80-90% of all DER generation in the USA [2], while the PV capacity in Germany amounts to the level of daily peak demand [3]. Combined heat and power technology is the second most dominant form of DER in many countries in the world [4]. Since notably different physical processes underline the operation of these distinct technologies, a major technical challenge for power engineers is to model and simulate the arising heterogeneity and to include it in the day-to-day operation of the grid [5].

At the same time, grid operators have started to rely more heavily on Information and Communication Technologies (ICT), Phasor Measurement Unit (PMU) measurements, and smart algorithms to perform their daily tasks. Since many of the operational strategies are supported by decision support tools and many of the monitoring and control actions are made by the smart algorithms, it is crucial to act based on the most accurate grid representation as possible.

Co-simulation arises as a natural solution to both of the previous challenges: 1) it eases the process of modeling the grid by interfacing already existing models encapsulated within domain-specific tools, 2) it provides a more accurate grid representation together with the supporting ICT infrastructure, which results in higher confidence in the results of decision support tools and monitoring and control algorithms.

The authors are with Electrical Sustainable Energy department of TU Delft, The Netherlands, (m.cvetkovic, k.pan, c.d.lopez, r.bhandia, p.palensky)@tudelft.nl

In this paper, we discuss the application of the co-simulation to two particular domains of interest for grid operation with large penetration of DERs. The considered domain challenges are: 1) Cyber-attacks against a monitoring system, and 2) Voltage stability in low inertia grids. Each of the domain studies is followed by simulation examples. Before diving into specifics of those two domains, we outline the general challenges for co-simulation of power systems with large number of DERs.

## II. Co-simulation Design Considerations

Efficient and accurate simulation tools are much needed to simulate the rising complexity of power systems due to the increased penetration of DERs. Such tools must not only represent the power system of today, but also include a diversified portfolio of models for capturing the intricacies of the DER technologies.

However, creating such comprehensive simulation environments is a challenging task. The difficulty arises from the need to develop detailed technical models of DERs and to integrate them within the existing methods for power system analysis. Since the underlying assumptions in many of these methods are not compatible with the models of DERs, the approach usually entails simplifications that either reduce the grid to a static equivalent model or average out the behavior of the DER units. In addition, the variety of control strategies and operation mechanisms must also be taken into account and included in the study to broaden the applicability of the results. Thus, a monolithic simulation environment that covers all relevant aspects of the problem is difficult to design and implement.

An alternative to creating a monolithic simulation is the co-simulation. In this approach, multiple simulation tools are combined to create a simulation environment that is more powerful than any of the simulators would be individually. One of the main advantages of this approach is that it makes it possible to couple heterogeneous models that would otherwise be incompatible. The most common example is the coupling of power system models, which are typically based on continuous equations, and communication network models, which are discrete event-based.

Examples of co-simulation applied to power system engineering are [6] where Electromagnetic transient and dynamic phasor simulations are coupled, [7] where real time simulation with distributed energy resources is carried out, and [8] where power system and communication network simulators are coupled.

Nevertheless, implementing a co-simulation does not come without its challenges [9]. When it comes to co-simulations for power systems with large number of DERs, some challenges are more prominent than the others:

- *Coupling heterogeneous tools containing DER models:* this is especially challenging when the involved tools are not meant to be used for co-simulation. Typically it is necessary to use whichever interfacing capabilities a tool provides and complement them with a set of workarounds to get the functionality needed. This can be extremely time consuming.
- *Coupling heterogeneous DER models:* to couple models it is necessary to set input values in them as well as to retrieve output values from them. In the case of continuous models, this can be challenging mainly because numerical stability/accuracy can be affected by the way inputs are set. In the case of continuous models coupled to discrete event models, a trade-off between accuracy and execution speed must be made.
- *Co-simulation size and scalability with large number of DER units:* if the number of involved tools/models is large, interconnecting them properly can be difficult. Further more, if more tools/models are expected to be added, the solution must be flexible enough to be easily scaled. Tools like mosaik [10] aim at mitigating this difficulty.
- *Time synchronization:* in a co-simulation all simulators must remain time-synchronized. This means that each of them must receive the inputs it needs, when it needs them. In the case of real-time co-simulation, time synchronization occurs naturally, so the challenge is to ensure all models are solved within one data exchange time step and to establish a communication challenge between each pair of connected simulators. In the case of non-real-time co-simulation, all messages must be time stamped and a master algorithm must ensure that they are provided to each simulator when required.
- *Result validation:* it is well known that co-simulations can suffer from lower accuracy than monolithic simulations. Since co-simulations are used when a monolithic simulation is not practical, there usually is no monolithic benchmark to compare the co-simulation results to. Determining whether the results are correct is a challenge on its own, which is even more emphasized in the case of a system with many distributed generation units.

## III. Cyber-Attacks Against a Monitoring System

Advanced monitoring schemes are being created to deal with the new challenges brought by increased integration of DERs in the electric energy supply. Monitoring systems such as Supervisory Control and Data Acquisition (SCADA) systems, rely on ICT infrastructure and their data is transported through communication networks to utility control centers. However, the ICT infrastructures within such cyber-physical systems are potentially vulnerable to a large number of security threats [11], [12]. Cyber-attacks against critical centralized monitoring schemes in Energy Management System (EMS) like State Estimation can result in poor situational awareness of the grids and affect power system reliability.

The typical security analysis methods used in power system field, such as vulnerability assessment, are based on the analytical treatment of the mathematical model that represents the power grid [13]. This type of assessment overlooks the ICT-specific aspects of the problem and is limited when it comes to quantifying the impact of the attack. A co-simulation platform that includes a power system simulator, a communication network simulator, and a monitoring scheme of choice (e.g., State Estimation), together with the other applications (e.g., Optimal Power Flow) that are relying on the monitoring scheme, could offer the capabilities for a more holistic security analysis and facilitate flexible modeling of DERs. To support the analysis of cyber-security, the communication network simulators within the co-simulation should have the capability to capture the properties of interest, such as the communication topologies and routing schemes, common protocols, flexible configuration of channels and modules, and even to support an attack library or framework that can be utilized to develop attack simulations.

Some co-simulation platforms have already been developed to analyze the interactions between physical power systems and cyber-networks, e.g., the electric power and communication synchronizing simulator (EPOCHS) in [8], the global event-driven co-simulation framework (GECO) in [14], and the integrated co-simulation of power and ICT systems for real-time evaluation (INSPIRE) in [15]. An example co-simulation of power systems and communication network is referred to [16]. Network simulators, e.g., OMNeT++, NS-3, OPNET, provide different choices for the discrete-event simulation of communication networks. In this paper, a co-simulation platform based on the integration of PowerFactor, OMNeT++ and Matlab is presented. Such co-simulation platform can support be used to assess the vulnerability of monitoring scheme to attacks and the quantify the attack impact taking into account the modeling of DERs. An illustrative example of data attacks against State Estimation and Optimal Power Flow is shown after the description of the co-simulation implementation.

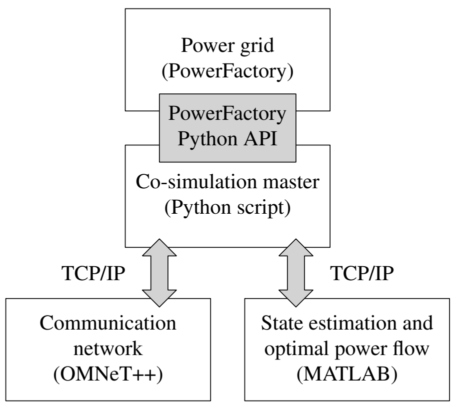


Fig. 1. Architecture of the co-simulation platform for cyber-security case study.

### A. Implementation of the Co-simulation Platform

A real-time co-simulation platform was implemented to analyze the consequences of cyber-attacks on the power grid. The platform is shown in Fig. 1. The components of this platform are the following:

*1) Power Grid Simulator:* PowerFactory is used to simulate the power grid through time series of DC power flow calculations. Every 30 s the power flow is re-calculated using a new value for distributed generation. The active power flowing in and out of each bus is measured and sent to the corresponding Remote Terminal Unit (RTU) in the communication network. In turn, PowerFactory expects set points for each generator as inputs. The data exchange is implemented using the provided Python Application Programming Interface (API).

*2) Communication Network Simulator:* The communication network that transmits power flow measurements between the power grid and the state estimator is simulated using the discrete-event simulator OMNeT++. The cyber-attack is implemented inside OMNeT++ by directly altering the contents of the messages that travel through the network. To enable data exchange between OMNeT++ and external simulators, a custom real-time scheduler was developed. The scheduler is in charge of receiving power flow measurements through a TCP/IP socket connection, forwarding the measurements to each RTU, and notifying them of every measurement arrival by creating a real-time event. OMNeT++ outputs the power flow measurements, either altered or intact, so they can be used for state estimation and optimal power flow calculations.

*3) State Estimation and Optimal Power Flow:* The state estimation algorithm is implemented in MATLAB, while optimal power flows are calculated using the MATPOWER package. A MATLAB script is in charge of receiving and sending data through TCP/IP sockets every 30 s. The received data are the power flow measurements as they leave the communication network simulator. The outputs are the generator set points that PowerFactory expects.

*4) Co-simulation Master:* The main goal of the master is to enable data exchange between simulators. The data exchange between the master and both OMNeT++ and MATLAB is done through TCP/IP sockets. However, the data exchange between the master and PowerFactory is done through its Python API, as the master itself is a Python script as well. The master must remain responsive to each simulator at all times, therefore dedicated threads for receiving data are created for each connected simulator.

### B. Case Study

We use the IEEE 9-bus system shown in Fig. 2 to perform cyber-attacks against the monitoring system and we demonstrate the impact in the developed co-simulation platform. This 9-bus system is modified with the integration of DERs, i.e., there is PV generation modeled as a positive load on Bus 5. The modeling of the communication network for the 9-bus system is depicted in Fig. 3. For the ease of illustration, we assume that each bus is equipped with an RTU and the communication between the RTU and the Master Terminal Unit (MTU) in the control center is simplistically modeled as a cloud.

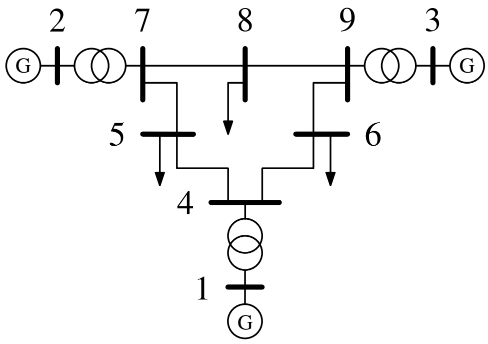


Fig. 2. One-line diagram of the IEEE 9-bus system.

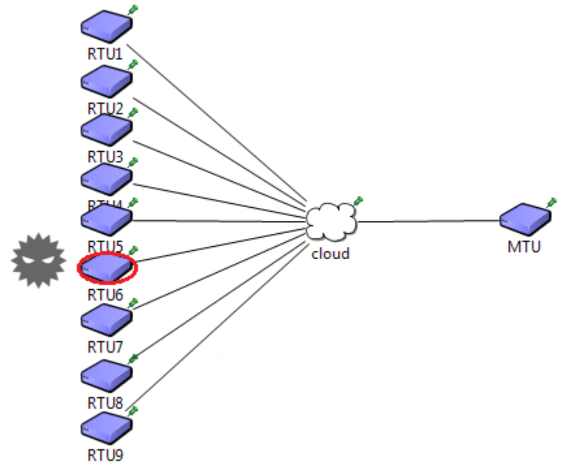


Fig. 3. Communication network as implemented in OMNeT++. RTU5 is under cyber attack.

An attack scenario where the RTU for load measurement on Bus 5 is manipulated by the attacker is considered. By accessing the RTU internals, the attacker can corrupt the integrity of the measurement data traveling through it. Here we show two cases where the load measurements on Bus 5 are corrupted 1) to be a constant value and 2) to be injected with false data. The attack in OMNeT++ is implemented by changing the behavior of the RTU5 module. The measurement data packets are tampered with before the module sends them out.

Fig. 4 shows the attack impact on the set points of the generators (i.e. the result of the optimal power flow algorithm) when the load measurements on Bus 5 are attacked to be a constant value. The results are parametrized by different levels of the PV penetration. Fig. 5 shows the attack impact on the true physical power flows on the transmission lines adjacent to Bus 5 when the load measurements on Bus 5 is injected with false data having different magnitudes but under a specific penetration level of PV power.

When the load measurements on Bus 5 are attacked to be constant while the actual power the PV system injects into

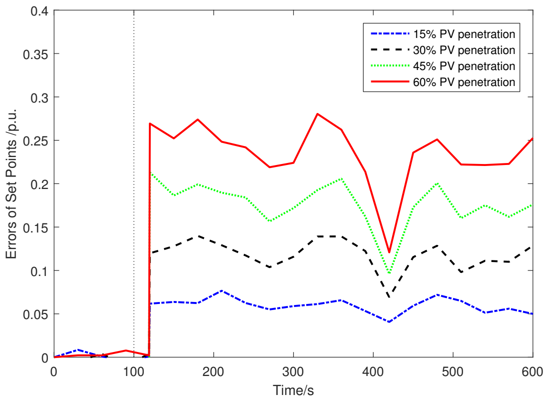


Fig. 4. The errors of set points are plotted versus the time. The attack occurs at 100s. The load measurements on Bus 5 are attacked to be constant.

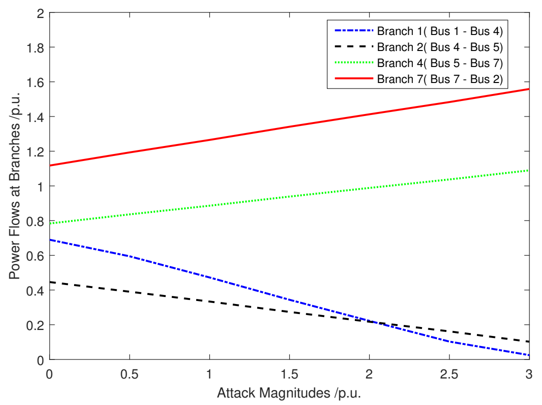


Fig. 5. The active power flows on the branches adjacent to Bus 5 are plotted versus the attack magnitudes. The load measurements on Bus 5 are injected with false data having various magnitudes.

Bus 5 is varying, the set points to the generators get *faked*. The total power generation according to the faked set points becomes larger when such attack is executed. As shown in Fig. 4, there are errors between the set points under normal conditions and the ones under attacks. With higher level of PV penetration, the errors become more significant. Thus the power grid with higher penetration of PV power is more vulnerable to this kind of integrity attack. The variation of the errors is due to the variable PV power with different radiance. In Fig. 4, the PV power has a sudden drop at 420s, and the errors under different levels of PV penetration also get smaller. This illustrates that the increasing integration of DERs brings vulnerabilities that can be utilized by the adversary. It should also be noted that though we only show the errors of set points, the attack impact can be further explored since the true generation profile determined by the faked set points may drive the power grid out of the safe state and into an unsafe one.

Next we conduct the attack scenario in which the load measurements on Bus 5 are injected with false data. Fig. 5 shows the active power flows on the branches close to Bus 5. The power flows get changed after redispatch according to the corrupted set points. With the increase of the attack magnitudes, the power flows on the Branch 4 (Bus 5 to Bus 7) and Branch 7 (Bus 7 to Bus 2) also increase, while the power flows on the Branch 1 (Bus 1 to Bus 4) and Branch 2 (Bus 4 to Bus 5) decrease. This implies that more power is injected in Bus 2 but less power is generated in Bus 1. Such physical impact on the transmission lines can cause damages especially if the false data injection attacks occur on a congested power system.

## IV. Voltage Stability in Low Inertia Grids

Conventional AC grids rely on inertial responses of generating units to regulate the power balance of the grid during any disturbance. A majority of non-conventional generators (including PV and wind) are interfaced to the grid through the electronic power converters, due to which they lack an inherent ability to contribute toward overall inertial response of the power system. This can lead to situations in which disturbances that were previously considered minor, such as tripping of some lightly loaded lines, are creating transient behavior of considerably higher magnitude leading to the loss of synchronism [17] and to other short term stability problems [18].

It is essential for wind turbines to provide power oscillation damping [19], [20], [21] under all conditions in the network and to suppress aerial power pulsations which would otherwise be directly transferred to the grid. Furthermore, wind turbines cannot provide voltage support on their own and often times must be paired with Dynamic Voltage Regulators in order to achieve desirable voltage behavior. The existence of the converter based interface allows for other control mechanisms that address power oscillations [22], [23].

On the other hand, the variability, intermittency and uncertainty in renewable generation create difficulties for nominal operation of the grid. With such characteristics of DERs, the system operators must procure significant amounts of reserves in order to be prepared for the rare occasions when renewable generation is low. The costs therefore shift from the fuel costs of fossil fuel plants to the reserve costs of the same plants which are at times even higher. Finally, higher uncertainty brings higher deviations from expected value which in turn brings higher risk of worse dynamic system response as well.

At the same time, a large number of DERs is interfaced with the grid through power electronic converters. Besides their primary purpose, to convert DC supplied power to the AC grid sine-wave forms, these devices have significant potential for dynamic stabilization of grid quantities. In this section we look into the potential of converter-interfaced PVs for improving voltage stability of the grid.

### A. Implementation of the Co-simulation Platform

The illustration of the co-simulation setup for this case study is shown in Fig. 6.

*1) Power Grid and Power Component Simulator:* this paper, we use Modelica language to encapsulate the domain-specific DER models. Modelica is a non-proprietary programming language whose use closely resembles the process

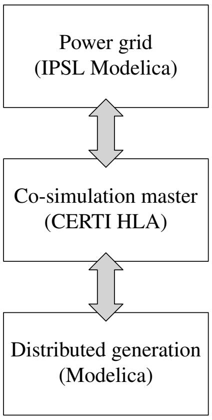


Fig. 6. Architecture of the co-simulation platform for the voltage stability case study.

that a researcher would undertake to set up a system of equations to describe the physics of a process of interest. These equations can be differential and algebraic. Modelica was created in the second half of 1990s to expedite the simulation process for researchers and alike who found it less natural to code mathematical models in pure programming languages such as C and Fortran.

To create a co-simulation, Modelica models are exported as Functional Mockup Units (FMUs). FMU is a standardized interface created to support co-simulation. According to this standard, each model that is packaged as an FMU provides a set of functionalities to the user that are invoked to engage the FMU into a co-simulation (for example, requesting the FMU to take a step forward in time or to return the first derivatives of all differential variables if an external numerical solver is used). Once all Modelica language models are encapsulated as FMUs their interconnection can be made formal easier.

Another benefit of using FMUs is that they ease the process of collaboration for domain experts from different fields. According to this modeling philosophy, a researcher from one domain does not have to understand the specifics of the other domains. In fact, the FMU encapsulation and standardization ensures that such collaboration is easily achieved.

*2) Co-simulation Master:* The High Level Architecture (HLA) standard is used as a master for the co-simulation to engage the relevant FMUs at the appropriate times. This standard defines the rules and services that ensure timely exchange of messages between the simulators and the synchronization of the simulator step execution. The HLA standard is implemented by a Run-time Infrastructure (RTI). A number of different open source and proprietary RTIs are currently available. In this paper, we opt out for CERTI [24], a C++ open source RTI whose performance for power system simulations have been recently evaluated in [10].

The most notable benefit of using HLA for simulations with DERs is its scalability in terms of number of components that it supports. In theory, the standard knows no limits. In practice, it depends largely on the underlying implementation of the RTI used. The HLA standard is created fashioning the publisher/subscriber design pattern in computer science. One benefit of this design pattern is its loose coupling between the engaged simulators which allows for easy reconfigurability of the co-simulation on the fly. Such pattern scales well if there are few publishers and many subscribers. However, since the co-simulations of power systems typically require symmetrical exchange of information, reaching considerably large scale implementations remains a practical computational challenge [25].

### B. Case Study

The power system model used in this case study is the IEEE 9-bus system from Fig. 2. This power system is modeled in Modelica language and it is available as a part of the IPSL Modelica library [26]. The power system is modified to resemble a power system with large penetration of DERs by reducing the inertia of the synchronous generators by tenfold. Although such a model is a crude approximation of a realistic wind power plant, we result to it to simplify the design process. In addition, the distributed PV generation is represented as variation on the loads at different nodes in the system. These nodes are then simulated remotely through the use of co-simulation.

Three different cases are considered for comparison. In Case I, the unmodified IEEE 9-bus system is simulated as a benchmark. Case II considers the system with inertia reduced as previously explained. In Case III, we add the impact of voltage support of distributed PVs.

A short-circuit event is simulated at Bus 9 in duration of 0.1 s. This event leads to a stable behavior in all three cases. However, Case II shows much worse behavior than Cases I and III. This is due to the smaller inertia of the wind generating units and the lack of control in the distributed PV units.

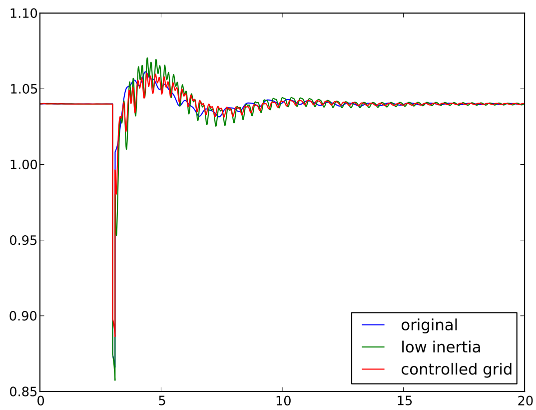


Fig. 7. The voltage profile at Bus 1 for the three different cases.

## V. Conclusions

In this paper, we review two distinct DER integration challenges and reflect on the needs of co-simulation environments to accurately simulate the grid behavior. A higher penetration of DERs can make situational awareness more difficult in case of cyber-attacks. In the case of voltage stability, while lower inertia of DERs worsens the dynamic performance, the opportunity for control implementation within the converter-based interfaces improves the situation. Finally, although co-simulation is a powerful tool for analyzing complex power systems with DERs, there are still many practical challenges ahead for this method to be deployed at scale.

## REFERENCES


[1] GTM Research/SEIA, "U.S. Solar Market Insight report", 2016.

[2] "A Review of Distributed Energy Resources", prepared by DNV-GL, September 2014.

[3] "The Integrated Grid", prepared by EPRI, 2014.

[4] Kyle Siler-Evans, M. Granger Morgan, Inłs Lima Azevedo, Distributed cogeneration for commercial buildings: Can we make the economics work?, Energy Policy, Volume 42, March 2012, Pages 580-590, ISSN 0301-4215.

[5] "Distributed Energy Resources Connection Modeling and Reliability Considerations", February 2017.

[6] F. Plumier, P. Aristidou, C. Geuzaine and T. van Cutsem, "Co-Simulation of Electromagnetic Transients and Phasor Models: A Relaxation Approach," in IEEE Transactions on Power Delivery, vol. 31, no. 5, pp. 2360-2369, Oct. 2016.

[7] Büscher, A. Claassen, M. Kube, S. Lehnhoff, K. Piech, S. Rohjans, S. Scherfke, C. Steinbrink, J. Velasquez, F. Tempez, and Y. Bouzid, Integrated smart grid simulations for generic automation architectures with RTLAB and mosaik, in 5th IEEE International Conference on Smart Grid Communications. IEEE, 11 2014.

[8] Hopkinson, K., Wang, X., Giovanini, R., Thorp, J., Birman, K., and Coury, D. (2006). EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components. IEEE Transactions on Power Systems, 21(2), 548-558.

[9] P. Palensky, A. A. van der Meer, C.D. López, A. Joseph, and K. Pan, "Cosimulation of Intelligent Power Systems: Fundamentals, Software Architecture, Numerics, and Coupling", IEEE Industrial Electronics Magazine, Vol. 11 (1) , pp. 34-50, 2017.

[10] C. Steinbrink, A. A. van der Meer, M. Cvetkovic, D. Babazadeh, S. Rohjans, P. Palensky, S. Lehnhoff, *Smart Grid Co-Simulation with MOSAIK and HLA: A Comparison Study*, D-A-CH+ Energieinformatik, Lugano, Switzerland, October 2017.

[11] "Cyber Security for DER Systems", prepared by EPRI, 2013.

[12] Chen, Thomas M and Abu-Nimeh, Saeed, "Lessons from stuxnet", Computer, Vol.44(4), pp.91-93, 2011.

[13] K. Pan and A. Teixeira and C. D. Ló pez and P. Palensky,"Co-simulation for Cyber Security Analysis: Data Attacks against Energy Management System," Accepted in 8th IEEE Int. Conf. Smart Grid Communications (SmartGridComm 2017), 2017.

[14] H. Lin, S. Veda, S. Shukla, L. Mili, and J. Thorp, "GECO: Global event-driven co-simulation framework for interconnected power system and communication network," IEEE Trans. Smart Grid, vol. 3, no. 3, pp. 14441456, May 2012.

[15] H. Georg, S. Muller, C. Rehtanz, and C. Wietfeld,"Analyzing cyber-physical energy systems: The INSPIRE cosimulation of power and ICT systems using HLA," IEEE Trans. Ind. Inform., vol. 10, no. 4, pp. 2364-2373, June 2014.

[16] P. Palensky, A. A. van der Meer, C.D. López, A. Joseph, and K. Pan, "Applied Cosimulation of Intelligent Power Systems: Implementing Hybrid Simulators for Complex Power Systems", IEEE Industrial Electronics Magazine, Vol. 11 (2) , pp. 6-21, 2017.

[17] M. Benidris, S. Elsaiah, S. Sulaeman and J. Mitra, "Transient stability of distributed generators in the presence of energy storage devices," 2012 North American Power Symposium (NAPS), Champaign, IL, 2012, pp. 1-6.

[18] A. Junyent-Ferr, Y. Pipelzadeh and T. C. Green, "Blending HVDC-Link Energy Storage and Offshore Wind Turbine Inertia for Fast Frequency Response," in IEEE Transactions on Sustainable Energy, vol. 6, no. 3, pp. 1059-1066, July 2015.

[19] J. G. Slootweg W. L. Kling "The impact of large scale wind power generation on power system oscillations" , Electr. Power Syst. Res., vol. 67 no. 1 pp. 9-20 Feb. 2011.

[20] G. Tsourakis B. M. Nomikos C. D. Vournas "Contribution of doubly fed wind generators to oscillation damping", IEEE Trans. Energy Convers., vol. 24 no. 3 pp. 783-791 Sep. 2009.

[21] Y. Wang, J. Meng, X. Zhang and L. Xu, "Control of PMSG-Based Wind Turbines for System Inertial Response and Power Oscillation Damping," in IEEE Transactions on Sustainable Energy, vol. 6, no. 2, pp. 565-574, April 2015.

[22] L.H. Hansen L. Helle F. Blaabjerg E. Ritchie S. Munk-Nielsen H. Bindner P. Srensen and B. Bak-Jensen "Conceptual survey of Generators and Power Electronics for Wind Turbines" Ris-R-1205(EN) 2001.

[23] F. Iov, M. Ciobotaru and F. Blaabjerg, "Power electronics control of wind energy in distributed power systems," 2008 11th International Conference on Optimization of Electrical and Electronic Equipment, Brasov, 2008, pp. XXIX-XLIV.

[24] E. Noulard and J.-Y. Rousselot and P. Siron, *CERTI, an Open Source RTI, why and how*, Spring Simulation Interoperability Workshop, 2009.

[25] Palmintier, B. and Krishnamurthy, D. and Top, P. and Smith, S., *Design of the HELICS High-Performance Transmission-Distribution-Communication-Market Co-Simulation Framework*, Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, Pittsburgh, PA, 2017.

[26] L. Vanfretti, T. Rabuzin, M. Baudette, and M. Murad, iTesla Power Systems Library (iPSL): A Modelica library for phasor time-domain simulations, SoftwareX, Available online 18 May 2016, ISSN 2352-7110, DOI: 10.1016/j.softx.2016.05.001.