Accepted for publication. Author copy. Do not redistribute.

Real-Time Co-Simulation Testbed for Microgrid Cyber-Physical Analysis

Venkatesh Venkataramanan, *Student Member, IEEE,* Anurag Srivastava, *Senior Member, IEEE,* and Adam Hahn, *Member, IEEE*

***Abstract*—This paper provides an overview of the development of a real-time cyber-physical testbed for analyzing the impact of cyber events on the critical loads in a microgrid. A real-time, cyber-physical co-simulation testbed utilizing a Real Time Digital Simulator (RTDS) for simulating the power system, Common Open Research Emulator (CORE) for emulation of the communication network, and a TCP/IP based interface is used in this work. The testbed is used to simulate a Army microgrid based model for validation. Cyber-physical system simulation results demonstrate the ability of the testbed to implement the cyber attacks and analyze the impact on microgrid.**

***Index Terms*—CORE, Cyber-Physical Test Bed, Cyber Security, Microgrid Reconfiguration, Microgrid Resiliency, Real Time Digital Simulator, Smart Grid.**

I. Introduction

To analyze the impact of cyber events on the physical microgrid system performance, testbeds are needed with detailed modeling/emulation of closely coupled cyber and physical systems. This is specifically applicable to microgrids given low inertia, higher resistance to inductance ratio, distributed/embedded control and dynamic interplay between cyber and physical systems given smaller geographical boundary. Real-time integrated co-simulation/emulation with hardware in the loop simulation is much neededd for cyber-physical microgrid analysis.

The CERTS microgrid [1] is a good example of an hardware testbed focused on control and operation of microgrids. There are also various microgrid testbeds that focus on other areas such as inverter control and integration of renewables [2]–[5]. However, these testbeds operate actual hardware, and testing might be expensive. There are a number of existing testbeds that consider both power system simulation and communication architectures for the transmission level power system. Examples for some of these are the testbed from Iowa State University [6], testbed from Florida State University [7], CESI RICERCA from Milan, Italy [8], University of Illinois at Urbana-Champaign [9], KTH's VIKING testbed [10], Gulliver testbed [11], and EPIC [12]. Our research group at Washington State University have developed variation of testbeds mainly focused on transmission system [13]–[15].

Venkatesh Venkataramanan, Anurag Srivastava, and Adam Hahn are with Washington State University, Pullman, WA 99163 USA. (E-mail: vvenkata@eecs.wsu.edu)

This work is partially supported by the US Department of Energy under Award Number DE-OE0000780. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

None of these testbeds provide detailed modeling of physical system and its associated control while also providing detailed modeling of cyber system to model networking, cyber attacks, and defense mechanisms. There is a need to develop a real-time cyber-physical microgrid co-simulation testbed with the ability to simulate both the power system, control system and the associated communication architecture in real-time. The testbed should allow the flexibility to model and implement different cyber attacks, defense mechanisms and study system performance.

The objectives of this paper are:

1) To model the power system and control in the microgrid,
2) To model the associated communication architecture,
3) To develop an interface between the power system and communication system simulators, and
4) To analyze the impacts of different cyber attacks on the microgrid.

Future work will include modeling cyber defense mechanisms and analyzing impact of cyber events on operational performance.

II. Testbed Components and Design

The microgrid co-simulation testbed has the following main components:

1) Power system simulation using Real Time Digital Simulator (RTDS) [16],
2) Communication network emulator using CORE (Common Open Research Emulator) [17],
3) Interface between the two simulators,
4) Open Platform Communication (OPC) based on FreeOPCUA [18], and
5) Control algorithms such as resiliency based reconfiguration [19].

A. Real-Time Simulation Using RTDS

The power system model has been developed in RTDS which offers the flexibility of connecting hardware components to the simulated power system. Also, the control algorithms used in the simulation can be validated to work in real-time. RTDS simulates the system with a time step of 50 μs [16]. The power electronic components are simulated using a special feature in RTDS called the "small_dt" simulation with a timestep of 1.4 to 2.5 μs. RTDS uses a special solver and allocates a separate processor for the power electronic components.

B. Communication Emulation Using CORE

For a cyber-physical co-simulation testbed, the simulation or emulation of the communication network is very important. In simulation, the communication network is modeled using nodes and connections, but the nodes themselves cannot be accessed or used. On the other hand, emulation models the network such that the communication nodes are capable of emulating the actual hardware device. An emulator builds a representation of a real computer network that runs in real-time, as opposed to simulation, where abstract models are used [20].

There are a variety of existing emulation tools such as CORE or DeterLab. For this work, CORE has been chosen as the emulation tool because of its lower computation requirement, and the emulation can be done in a single computer instead of a server cluster as required by DeterLab. CORE has been developed by a network technology research group that is part of Boeing Research and Technology division. CORE provides an environment for running real applications and protocols. It uses a backend daemon to manage the emulated networks, and uses kernel virtualization for node emulation and bridging. Various scenarios are emulated in CORE by packet manipulation in virtual networks by the daemon. The architecture is modular and hence CORE can be combined with other network tools such as EMANE and NS-3. The CORE API is sockets based, and allows for connecting to different components on different physical machines.

C. Open Platform Communication for Data Exchange

In substations, the measurements from various sensors are usually wrapped in a specific format so that they can be used for various applications [21]. This typically involves tagging the data for the control center and the user, time stamping the data, making the data easier to read for other devices, and for archiving. There exist a variety of different substation protocols such as IEC 61850, DNP3, OPC, and MODBUS.

In this work, the OPC protocol [22] has been implemented for data exchange. OPC stand for OLE (Object Linking and Embedding) for Process Control. It is a substation protocol that is routable, provides time stamping of data, and can be implemented in a client-server architecture. OPC is implemented inside the interface and the data is wrapped using the OPC protocol and routed through the CORE network.

The wrapping up of data in OPC is achieved through another open source Python library called “FreeOPCUA” [18]. In FreeOPCUA, the server is implemented inside the interface, and is responsible for wrapping up the data from the Runtime to OPC. OPC clients are implemented inside the CORE network, which subscribe to the change in the data value from the server inside the interface. A server is also implemented at the control center node in CORE, which provides the breaker status according to the output of the reconfiguration algorithm. This updated status is subscribed to by the client and is sent back to the simulated power system, hence completing the feedback loop.

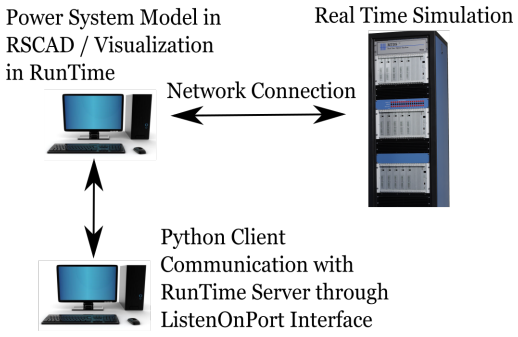

Fig. 1. RTDS ListenOnPort

D. Interface Between Power and Communication Network Simulators

For the purpose of impact analysis of cyber attacks on the power system, it is important to consider the power system as a cyber-physical system. Hence, interfaces need to be developed to bring together all these modeling tools into a single environment that is suitable for resiliency analysis.

The main concept behind the interface between the power system simulator RTDS and the communications network emulator CORE can be considered as TCP/IP [23]. A RTDS feature called ListenOnPort is used to establish socket communication with applications running in the same network. RTDS’s output is visualized in its RunTime screen. The RunTime is in the same machine in which the RSCAD is installed as shown in Fig. 1. The RunTime allows the user to use a scripting interface to provide commands in real time.

The steps of communicating with the Runtime server can be summarized as follows:
1. A port is opened in the Runtime computer, and the port number is decided by the user. The RTDS simulation is not yet started.
2. The external application, in this case the Python script, establishes the basic client socket.
3. The client application communicates with the server port of the Runtime. The socket communication is now established.
4. The socket and time libraries are imported, and the socket is instructed to use internet protocol (IP) for address (AF_INET), and TCP for streaming (SOCK_STREAM).
5. Now the connection is established to the Runtime server by specifying its IP address and port number.

Once the connections is established, the client can be used to send commands to the Runtime. These commands are processed as script commands in the Runtime server. For example, the command “Start;” will start the RTDS simulation. Similar commands are used to read system measurements from the simulation, and send back control signals. Since the client coordinates the time for various commands, it is important to allow enough time for the server to process the command and provide the output. This is managed through the ”Time” library in Python which is used to control the time taken to send and receive data from the server.

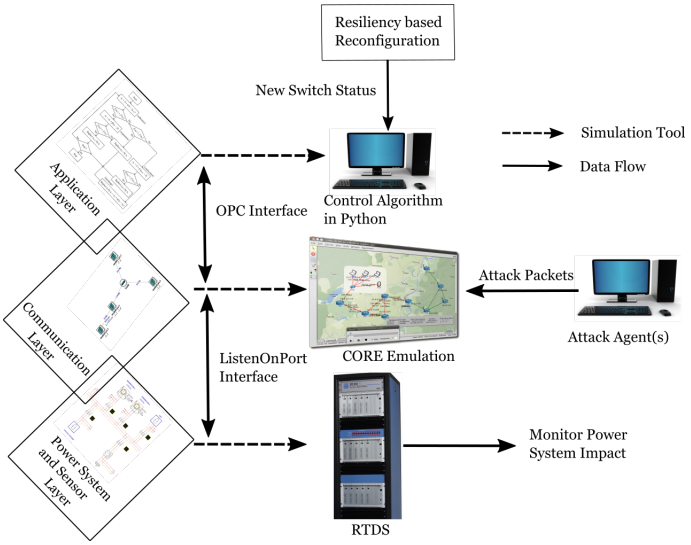

Fig. 2. Microgrid Cyber-Physical Co-Simulation Testbed

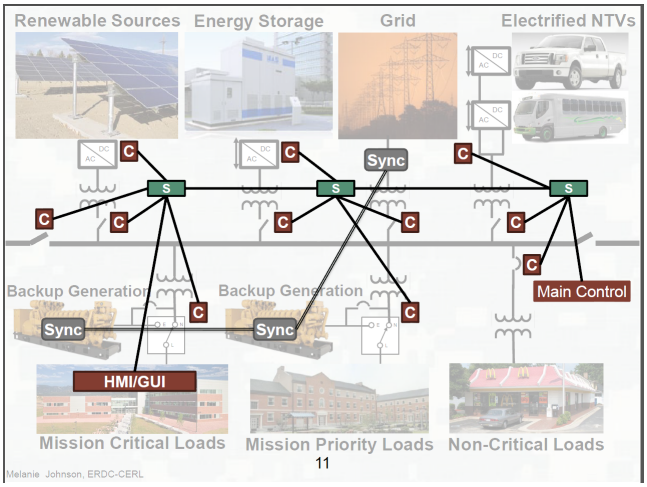

Fig. 3. Army Microgrid Layout [24]

E. Control Algorithm for Microgrid Resiliency

The control algorithm for resilient reconfiguration of the microgrid is based on our work in [19]. The reconfiguration algorithm is used for the test system and the results are obtained. These results are stored in the form of a lookup table in the main controller node in the CORE network. When the reconfiguration algorithm is triggered by a change in the breaker status, the reconfiguration algorithm determines the most resilient configuration. The new status is then given to the switches in the simulated power system. The testbed is flexible enough to separate all the components into different layers, and hence other applications can also be implemented using the proposed testbed.

The complete microgrid cyber-physical co-simulation is represented in Fig. 2.

III. Modeling and Simulation of Army Microgrid

A. Power System Modeling

The microgrid used in this work is based on the model of an Army microgrid [24], [25]. The Army microgrid is chosen because of the following reasons.

1) Microgrid architecture, which allows redundant paths for reconfiguration,
2) Presence of critical loads and priority loads,
3) Strong emphasis on cybersecurity being a critical infrastructure [26].

This work primarily uses a design based on the Fort Carson microgrid. This microgrid is already established, and some details of the microgrid has been made public. A conceptual overview of the microgrid's architecture is also available in public domain [25], which has been used to design the microgrid for this paper.

The details about the microgrid components from [25] have been listed here:

1) 1.1 MW of critical load, and 1 MW of priority load,
2) 3.25 MVA of existing diesel generation,
3) 1 MW of Solar array,
4) 5 electric vehicles.

Also, the basic layout of the Fort Carson microgrid is shown in Fig. 3. In this work, a solar PV array grid tie inverter is modeled in small time step environment. Smaller time step simulation provided by RTDS guarantee that the gating pulses and the operation of the inverter is simulated accurately [27].

The following modifications has been made to the microgrid model from the Fort Carson microgrid:

1) The energy storage and the renewable source (PV) has been combined into a single unit, to make the model simpler and to compensate for the variability of the PV.
2) A non-critical load has been added to the system to demonstrate the effect of reconfiguration.
3) The backup generation which are associated to each individual load has been modified for system level access so that the loads can be shared even when the microgrid is in islanded mode.
4) The priority load does not have its own auxiliary generator, but is tapped off from the main feeder. The critical load has an auxiliary diesel generator that is normally in reserve (connected through a normally open breaker), but can be connected through the reconfiguration algorithm.
5) The electric vehicles have not been modeled as the electric vehicles are rated much smaller than the other generation/load present in the system.

The microgrid model used in this work is simplified and represented in the Fig. 4

In the microgrid model 4, the critical load is at the far left, and it has an auxiliary generator connected to it. The PV panel right above it and the priority load is right next to it, but is not connected to its own auxiliary generator. This part of the microgrid is followed by a sectionalizing switch which can be used to further isolate the sensitive loads from the rest of

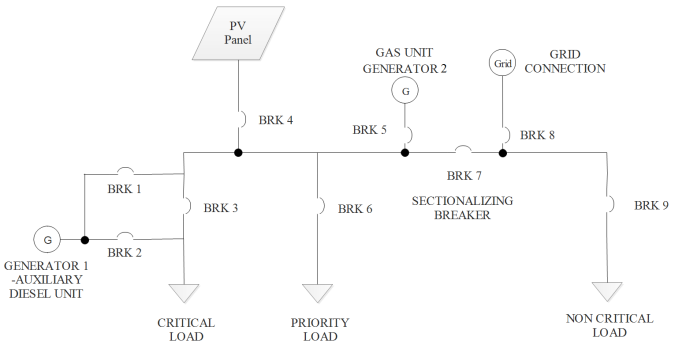

Fig. 4. Microgrid Model

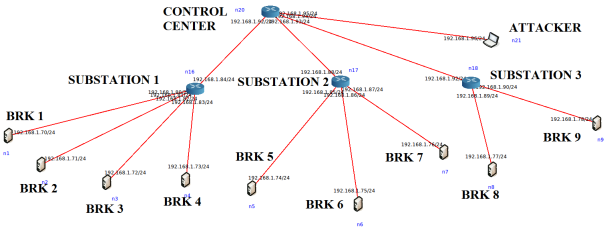

Fig. 5. Microgrid Communication Model

the microgrid. The non-critical load is in the extreme right, and is being fed by the grid. In normal operation, the grid is connected to the microgrid, and most of the loads is supplied by the grid and the PV array. The generator 2, which is a gas turbine based generation is normally open, and has the first priority to be connected to the system. Generator 1 is an expensive diesel unit, that only supplies the critical load during emergency, following contingencies.

B. Communication Network Modeling

The communication network for this microgrid is modeled in CORE and its modeling is discussed. The Fig. 3 indicates several boxes marked 'S' which stands for substation. Each substation is associated with several breakers, and this architecture is reflected in the developed communication model. The CORE model is shown in Fig. 5. The core model shows several nodes in the bottom of the figure, which represent the different relays that control the breakers in the simulated system. Each of these relays are connected to a substation gateway in the substation, which is 'S' as discussed above.

When the simulation is started, data from the power system simulator is obtained, and is routed through this network model to the control center, which runs the control algorithm for reconfiguration. This algorithm receives the data, analyzes it, and sends the new switch status as necessary.

IV. Simulation Results

This section presents the simulation results from the RTDS for different attack scenarios. The breaker status obtained from the reconfiguration algorithm for different cases is shown in Fig. 6.

A. Denial of Service (DoS) Attack

In the DoS attack, a combined cyber and physical attack is considered. The attacker carries out a physical attack against the grid tie breaker, and then performs a DoS on the same breaker. Due to a shortage in generation, the secondary protection acts and opens the sectionalizing switch which isolates the critical and priority load from the rest of the microgrid, and sheds the critical load. The power output of the gas unit after being switched ON is shown in Fig. 7. Finally, the voltage profile before and after the non-critical load shedding is shown in Fig. 8.

B. Man in the Middle Attack

In this attack, the attacker gains access to the sectionalizing switch and trips the breaker. This triggers the reconfiguration algorithm. The reconfiguration algorithm now closes the breaker for the gas unit, and uses the PV and the gas unit to supply the critical load and the priority load. The non-critical load is supplied by the grid. Hence no load is lost in this scenario. The gas unit response is shown in Fig. 9.

C. Coordinated Attack

In the coordinated attack, the attacker is assumed to have prior knowledge about the system, and have multiple time coordinated agents. Hence the attacker at first tries to isolate all loads by tripping its individual breakers. However, since the auxiliary generator's breaker is not affected, the critical load is still being supplied. The power output of the auxiliary generator is shown in Fig. 10. The resiliency for this configuration is 0.5234.

In a typical system, the auxiliary generator does not have a remote controlled breaker. The only way to isolate the critical load from the system would be to perform a physical attack. A cyber-physical attack could isolate the critical load and the power output goes to zero as shown in Fig. 11.

It can be seen that for the coordinated attack, the attacker can trip all the breakers in the system but cannot isolate the critical load unless the attacker also manages to gain physical access to the breaker connecting the auxiliary generator to the critical load.

D. Limitations of Proposed Testbed

The proposed microgrid cyber-physical testbed is able to integrate different simulators and analyze microgrid resiliency in real time. However, there are a few limitations to this testbed. The size of the system that can be simulated is limited due to

1) The computation limit of the RTDS to simulate in real-time,
2) The amount of data that the ListenOnPort interface can support.

The average amount of latency in this approach is higher than expected delay of a real system. For example, the average latency of a packet to go from the relay to the controller is around 90 ms. Wrapping up the data in OPC, and the time for the reconfiguration to receive the data, and provide new

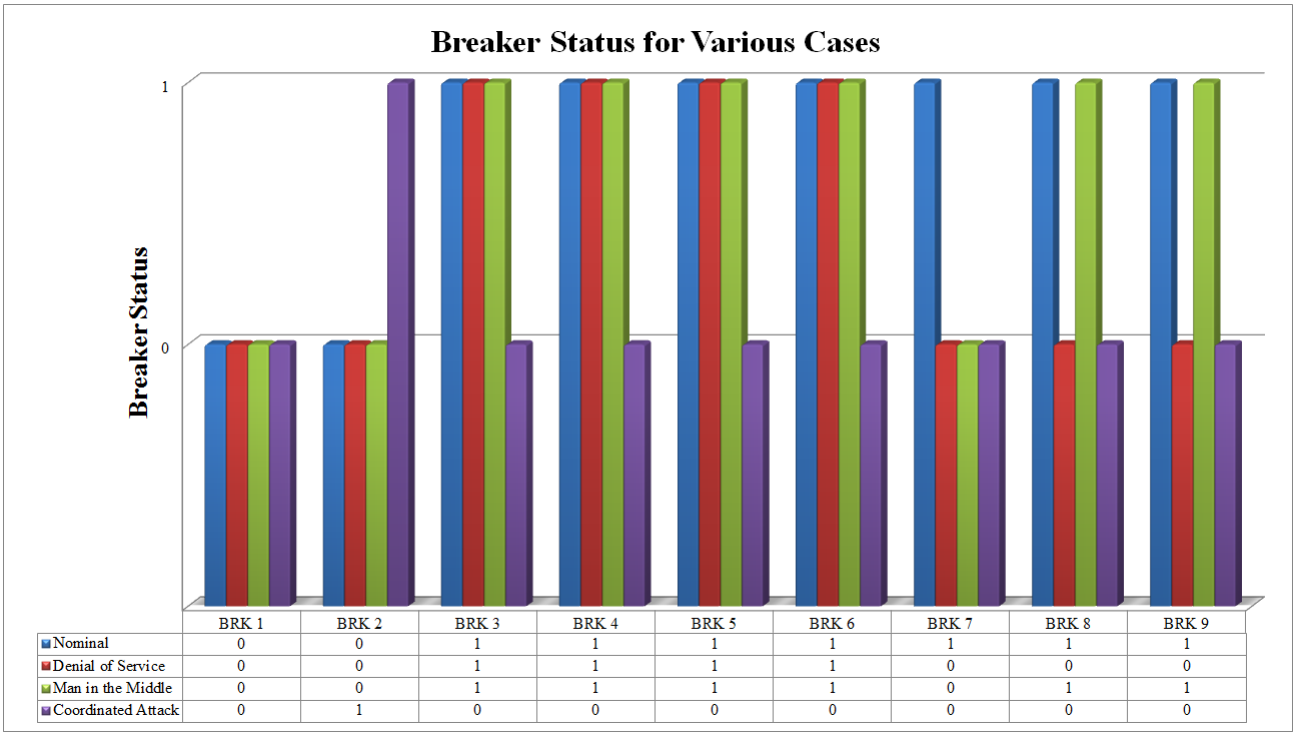

Fig. 6. Breaker Status for Various Cases

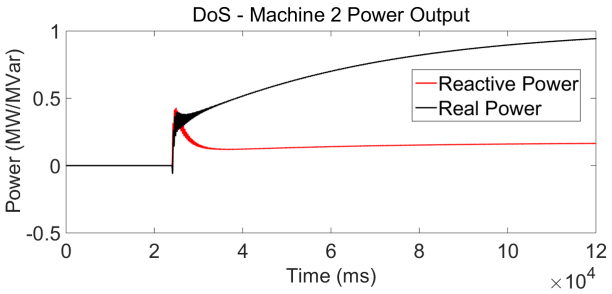

Fig. 7. Power Output of Gas Unit During DoS Attack

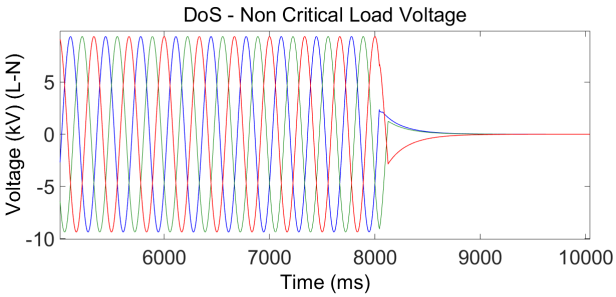

Fig. 8. Non Critical Load Shed During DoS Attack

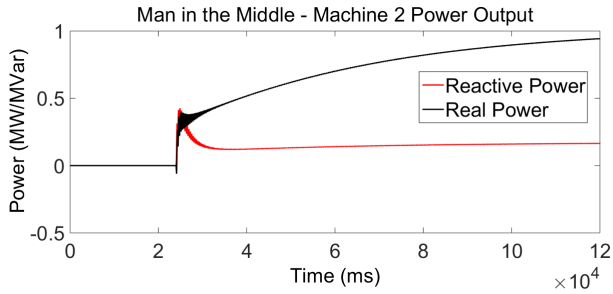

Fig. 9. Power of Auxiliary Generator Due to Man in the Middle Attack

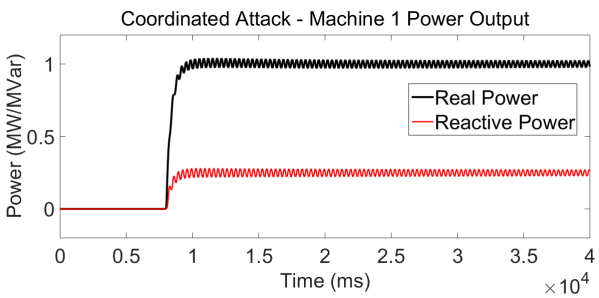

Fig. 10. Auxiliary Generator Power Output During Coordinated Attack

configuration (if necessary) adds more time to the process. Hence the testbed is not suitable for analysis of phenomena with short timeline, but for applications such as reconfiguration with a slower timeline, the performance of the testbed is acceptable.

V. Conclusions

The goal of this paper is to create a real-time, cyber-physical testbed for microgrid analysis. The power system model is developed in RTDS/RSCAD, the network model in

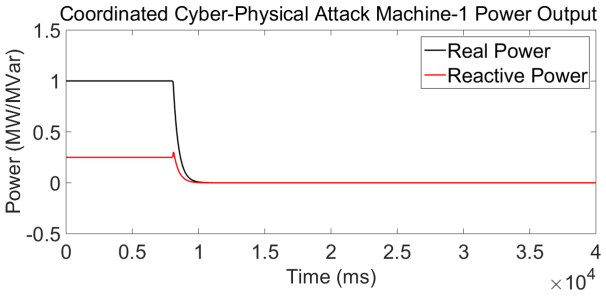

Fig. 11. Auxiliary Generator Power Output During Coordinated Cyber-Physical Attack

CORE, and an interface to connect the two modeling tools is implemented in Python. The interface is based on TCP/IP, and takes advantage of the RTDS/Runtime's ListenOnPort interface option. The data from the power system simulator is wrapped in OPC and delivered to the reconfiguration algorithm at control center. The impact of different cyber-physical attacks have been analyzed using the testbed. The proposed microgrid co-simulation testbed can be used to test a variety of future applications, with a focus on cyber-physical system security.

REFERENCES

[1] D. K. Nichols, J. Stevens, R. Lasseter, J. Eto, and H. Vollkommer, "Validation of the CERTS microgrid concept the CEC/CERTS microgrid testbed," in *IEEE Power Engineering Society General Meeting, 2006.*

[2] E. Kabalci, R. Bayindir, and E. Hossain, "Hybrid microgrid testbed involving wind/solar/fuel cell plants: A desing and analysis testbed," in *International Conference on Renewable Energy Research and Application (ICRERA), 2014.*

[3] M. Meiqin, D. Ming, S. Jianhui, L. Chang, S. Min, and Z. Guorong, "Testbed for microgrid with multi-energy generators," in *Canadian Conference on Electrical and Computer Engineering, (CCECE) 2008.*

[4] A. Khmais, M. Nasir, A. Mohamed, and H. Shareef, "Design and simulation of small scale microgrid testbed," in *Third International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM), 2011.*

[5] K. Sedghisigarchi, Y. Eslami, A. Davari, and S. Wilkerson, "A real-time testbed for coordinated control of inverters in LV microgrids," in *IEEE International Energy Conference (ENERGYCON), 2014.*

[6] A. Hahn, B. Kregel, M. Govindarasu, J. Fitzpatrick, R. Adnan, S. Sridhar, and M. Higdon, "Development of the powercyber SCADA security testbed," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, ser. CSIIRW '10.

[7] M. Stanovich, I. Leonard, K. Sanjeev, M. Steurer, T. Roth, S. Jackson, and M. Bruce, "Development of a smart-grid cyber-physical systems testbed," in *IEEE PES Innovative Smart Grid Technologies (ISGT), 2013.*

[8] G. Dondossola, G. Garrone, J. Szanto, G. Deconinck, T. Loix, and H. Beitollahi, "ICT resilience of power control systems: experimental results from the CRUTIAL testbeds," in *IEEE/IFIP International Conference on Dependable Systems Networks, DSN '09.*

[9] T. Yardley, R. Berthier, D. Nicol, and W. Sanders, "Smart grid protocol testing through cyber-physical testbeds," in *IEEE PES Innovative Smart Grid Technologies (ISGT), 2013.*

[10] M. Ekstedt and T. Sommestad, "Enterprise architecture models for cyber security analysis," in *IEEE/PES Power Systems Conference and Exposition, PSCE '09.*

[11] M. Pahlavan, M. Papatriantafilou, and E. M. Schiller, "Gulliver: a testbed for developing, demonstrating and prototyping vehicular systems," in *Proceedings of the 9th ACM international symposium on Mobility management and wireless access*. ACM, 2011.

[12] C. Siaterlis and B. Genge, "Cyber-physical testbeds: Scientific instruments for cyber security assessment of critical infrastructures," 2008.

[13] R. Liu and A. Srivastava, "Integrated simulation to analyze the impact of cyber-attacks on the power grid," in *Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2015.*

[14] R. Liu, C. Vellaithurai, S. Biswas, T. Gamage, and A. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *Smart Grid, IEEE Trans. on*, 2015.

[15] J. Hong, A. Stefanov, C.-C. Liu, and M. Govindarasu, "Cyber-physical security in a substation," in *IEEE Power and Energy Society General Meeting, 2012.*

[16] R. Kuffel, J. Giesbrecht, T. Maguire, R. Wierckx, and P. McLaren, "RTDS-A fully digital power system simulator operating in real time," in *IEEE Communications, Power, and Computing. Conference Proceedings, (WESCANEX), 1995.*

[17] J. Ahrenholz, "Comparison of CORE network emulation platforms," in *MILITARY COMMUNICATIONS CONFERENCE, MILCOM 2010.*

[18] Freeopcua, "FreeOPCUA - GitHub," 2015, [Online; accessed 10-August-2015]. [Online]. Available: http://freeopcua.github.io/

[19] S. Chanda, "Measuring and Enabling Resiliency in Distribution Systems with Multiple Microgrids," Master's thesis, Washington State University, Pullman, WA, 2015.

[20] "CORE Manual [Online]," http://downloads.pf.itd.nrl.navy.mil/docs /core/coremanual.pdf, Tech. Rep.

[21] A. Darby, "Explanation of protocols. I [Substation communication]," in *IEEE Colloquium on Substation Integration, Protection and Control, 1999.*

[22] M. Son and M.-J. Yi, "A study on OPC specifications: Perspective and challenges," in *International Forum on Strategic Technology (IFOST), 2010.*

[23] J. F. Kurose, *Computer Networking: A Top-Down Approach Featuring the Internet, 3/E.* Pearson Education India, 2005.

[24] M. Johnson and R. Ducey, "Overview of U.S. Army microgrid efforts at fixed installations," in *IEEE Power and Energy Society General Meeting, 2011.*

[25] Naval Facilities Engineering Command. (2014) SPIDERS phase 2 Fort Carson technology transition public report. [Online]. Available: http://energy.gov/sites/prod/files/2014/11/f19/spiders _phase2_publicreport_print_0.pdf

[26] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," in *IEEE/PES Power Systems Conference and Exposition, PSCE '09.*

[27] L. Qi, J. Langston, M. Steurer, and A. Sundaram, "Implementation and validation of a five-level STATCOM model in the RTDS small time-step environment," in *IEEE Power Energy Society General Meeting, PES '09.*