INL/CON-20-58606-Revision-0

Scalable, Physical Effects Measurable Microgrid for Cyber Resilience Analysis (SPEMMCRA)

Jacob J Ulrich, Timothy R McJunkin, Craig G Rieger

October 2020

INL/CON-20-58606-Revision-0

Scalable, Physical Effects Measurable Microgrid for Cyber Resilience Analysis (SPEMMCRA)

Jacob J Ulrich, Timothy R McJunkin, Craig G Rieger

October 2020

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy, Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517, DE-AC07-05ID14517

Scalable, Physical Effects Measurable Microgrid for Cyber Resilience Analysis (SPEMMCRA)

Jacob Ulrich
dept. of National & Homeland Security
Idaho National Laboratory
Idaho Falls, Idaho USA
jacob.ulrich@inl.gov

Timothy McJunkin
dept. of National & Homeland Security
Idaho National Laboratory
Idaho Falls, ID USA
timothy.mcjunkin@inl.gov

Craig Rieger
dept. of National & Homeland Security
Idaho National Laboratory
Idaho Falls, ID USA
craig.rieger@inl.gov

Michael Runyon
Quality Engineering
Kollmorgen Corporation
Radford, VA
michael.runyon@kollmorgen.com

***Abstract*—The ability to advance the state of the art in automated cybersecurity protections for industrial control systems (ICS) has as a prerequisite of understanding the trade-off space. That is, to enable a cyber feedback loop in a control system environment you must first consider both the security mitigation available, the benefits and the impacts to the control system functionality when the mitigation is used. More damaging impacts could be precipitated that the mitigation was intended to rectify. This paper details networked ICS that controls a simulation of the frequency response represented with the swing equation. The microgrid loads and base generation can be balanced through the control of an emulated battery and power inverter. The simulated plant, which is implemented in Raspberry Pi computers, provides an inexpensive platform to realize the physical effects of cyber attacks to show the trade-offs of available mitigating actions. This network design can include a commercial ICS controller and simple plant or emulated plant to introduce real world implementation of feedback controls, and provides a scalable, physical effects measurable microgrid for cyber resilience analysis (SPEMMCRA).**

***Index Terms*—industrial control system, automated security, scalable Microgrid, cyber-physical system**

I. Introduction

Industrial control systems (ICS), or operational technologies (OT), are a central part of physical operations of infrastructures, such as power systems. OT may be connected to traditional information technologies (IT) networks for administering the production, consumption and transmission of data and other messaging. The OT systems include feedback control loops, both autonomous and human in the loop, which have different time scales of operation. Latency or dropped messages could cause performance and possibly stability issues in the controlled infrastructure system. Future cyber technologies need to be designed to mitigate recognized faults through isolation or other active defenses while minimizing disruptions in deterministic communications, due to false positives from intrusion detection sensors. However, to further engender resilience to cyber attack within these environments, the future lies in active defenses that can mitigate attacks in a timely fashion.

The path forward to evaluate this trade-off space, therefore, is to understand the impacts in planning, design and implementation that will allow an informed understanding of cyber mitigation benefit versus physical impact to enable human and automated decision making. To achieve this goal, a framework for evaluation can be developed within an emulated cyber-physical systems connected to a hardware based controller and supervisory system. An example of a hardware controller in the loop, which integrates normal set point and data exchange interactions seen in a networked ICS environment, is described in this paper. This platform allows for a deeper understanding that can be further refined in future higher fidelity implementations. To illustrate that cyber attacks can impact the physcial world, a simple swing-equation model, which is the basis for the real power dynamics of frequency response of a lumped electrical system with at least some synchronous machines, was used. An emulated battery system provides the actuator available to control injection or consumption of power to compensate for frequency errors. The emulated system is implemented on Raspberry Pi (RPi) computers. The controller is a commercial ICS controller connected to a supervisory computer containing a human machine interface. This implementation will be referred to as the scalable, physical effects measurable Microgrid for cyber resilience analysis (SPEMMCRA).

While a number of different hardware in the loop systems could be envisioned and used [1] [2], these systems are heavily dependent upon large number of virtual machines (VMs) or personal computer based software system emulations that require even more hardware to connect controller hardware in the loop. The benefit of the RPi based design is to provide a cost-effective means to scale systems, with multiple emulated microgrids and controllable elements. This platform allows multiple segments response elements like software defined networks (SDN) and other security protections to be tested with a demonstrable physical effects.

The organization of this paper includes a brief background on the power physics used in Section II. Section III provides an overview of the network implementation of the microgrid devices. Section IV provides the background on the purpose and implementation of relevant scenarios, with the cyber resilient results provided in Section V. Section VI provides a summary and conclusion of the cyber resilience benefits of SPEMMCRA.

II. Swing equation Implementation

To provide a simple system to evaluate the physical effects of cyber attack and defense, is provided by emulating a microgrid as a simple uncontrolled base load synchronous machine generator, variable loads, and a controllable storage source to demonstrate frequency variations and stabilizing control of the frequency. The swing equation provides the physical representation of the electric grid with traditional generators that help maintain frequency stability through the kinetic energy stored in the flywheel effects of the rotation of the turbine, shaft, and generator core [3]. The real power balancing of a power grid, in this case built of smaller scale generation as could be recognized in a microgrid, can be expressed through a simple electro-mechanical relationship between electric load and the power put into the turbine of a generator. The dynamics represented by the governing differential equation can be expressed as follows:

If mechanical power applied to the generator is greater than the electric load: the frequency goes up because energy is added to the spinning machines. If the load becomes larger or a generator goes off line, the frequency goes down, because some of the kinetic energy is removed from the spinning machines to supply the deficit.

The differential equation expressing this relationship is non-linear and possibly time-variant with the moment of inertia that changes with connection or removal of additional generation and synchronous machine-based loads. The differential equation for calculating the frequency of a microgrid that has at least one synchronous machine is known as the swing Equation 1. The equation is give as:

$$P_g - \; P_e = J\omega_m \frac{d^2\delta}{dt^2} \tag{1}$$

where P_g is the power generated by the heat or other mechanical forces connected to the turbine and generator, $P_e$is the electric load or power being consumed, J is the moment of inertia of the spinning machine, ω_m is the angular velocity of the reference spinning machine which is proportional to the grid frequency and δ is the angular position of the generators rotor relative to the reference frequency (i.e. the rate machines angular velocity is changing due to the imbalance). The second derivative of the rotor position is proportional to the rate of change of the rotational grid frequency. For this emulation we will use a two pole generator so the mechanical rotational velocity will be equivalent to the grid frequency. We also assume the rate of change of frequency is slow enough that the generator does not trip based on being out of synchronicity with grid system to which it is attached. The microgrid is considered as multiple nodes, so the reference frequency will increase or decrease based on the power generation and load imbalances of the distribution grid. To arrive at sufficient fidelity to provide physical realism and yet allow real time computation the equation is implemented as the simplified difference equation:

$$\Delta\omega_m = \frac{(P_g - \; P_e)\,\Delta\mathrm{t}}{J\omega_m} \tag{2}$$

with $\Delta\mathrm{t} = 0.0167\mathrm{s}$, chosen to be small enough to provide a reasonable degree of accuracy in the calculation of the change in frequency in real time. The load and generation are driven by recorded system data, which has been made available through a previous education outreach effort by a municipal electrical utility [4]. The data set contains hydro-electric generation, wind generation, load and meteorological data. One year of historical data has been collected and repeats as necessary. The data set contains periods of power outages as well as seasonal and diurnal cycles. The net power imbalance is calculated as:

$$\begin{aligned} P_a\left(t\right) &= P_g - P_e \\ &= P_a\left(t\right) U_h G_h\left(t\right) + U_w W\left(t\right) + S\left(t\right) \\ &\quad + C\left(t\right) - U_c L_r\left(t\right) - \sum_i L_i D_r(t) \end{aligned} \tag{3}$$

where U_h, U_w, and U_c are the number of hydro generation units, wind generation units, and residential customer units that are multiplied by the hydro generation, $G_h\left(t\right)$, wind speed, $W\left(t\right)$, and residential load, $L_r\left(t\right)$, from the municipal utility data. The net power added from the controllable storage source, $S\left(t\right)$, adds to the generation or absorbs power from grid to enable the player to have a feedback control input to regulate the frequency as illustrated in 1. Additionally, C is the net power into the distribution grid of contracts bought and sold. The industrial loads, L_i, are summed to find the total amount of power being consumed by constant loads, when not curtailed through a demand response action by the balancing authority (BA). The state of demand response is given as $D_r = 0$ for curtailed load and 1 otherwise. For the purpose of this paper a municipal city or a portion of one that has generation and control sufficient to support itself is a microgrid. The purpose of having a emulated plant is to provide for a reason for the controller to exist and connect the cyber attack and cyber response to a dynamic system where communication latency or time to detect and resolve the attack are important.

III. Microgrid Network

The microgrid network parses the grid frequency control among devices as shown in Fig. 2. In this design, individual RPi computers represent commercial and residential loads, commercial, bulk and distributed generation, and energy storage. Frequency control can occur in one of the individual generation RPis or separately in the environment, as shown

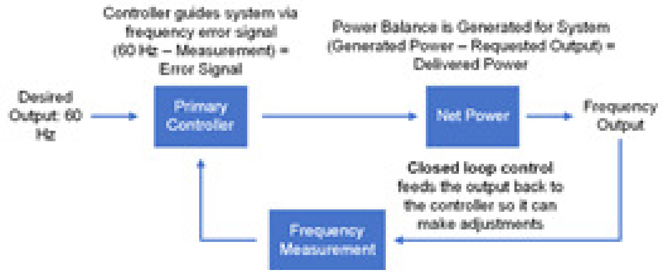

Controller guides system via frequency error signal (60 Hz – Measurement) = Error Signal
Power Balance is Generated for System (Generated Power – Requested Output) = Delivered Power
Desired Output: 60 Hz
Primary Controller
Net Power
Frequency Output
Closed loop control feeds the output back to the controller so it can make adjustments
Frequency Measurement

Fig. 1. BA Feedback Control

in Fig. 2. In this way, one of the devices can act as the controlled response evaluating the frequency error and applying an actuator based on the control system gains. In this case, the feedback control, illustrated in Fig. 1, is separate individual generation or storage, but could be specifically aligned with an individual resource such as energy storage where load support is provided. Pseudocode for this latter implementation is provided in Fig. 2, where the RPi interacts with an Allen Bradley controller over an analog signal representing the output of a a frequency sensor and the control signal to drive the response of the battery. The control law was a standard Proportional-Integral Derivative control. Alternatives include interfacing using a digital network sharing, as compared to analog.

With the swing equation as the physics behind the communications network, the evaluation of effects is dependent upon the types of deterministic interactions that are performed to support the control system interactions. As an example, Fig. 3 provides for several different operations. These include the following:

1) Setpoints from the operator human machine interface (HMI) to the individual frequency controller
2) Power data shared between the frequency controller and the individual generator
3) Condition data shared back to the HMI

The ability to include multiple RPi instances of loads, generators, or storage assets, which may be controllable or not controllable allows this platform to easily scale.

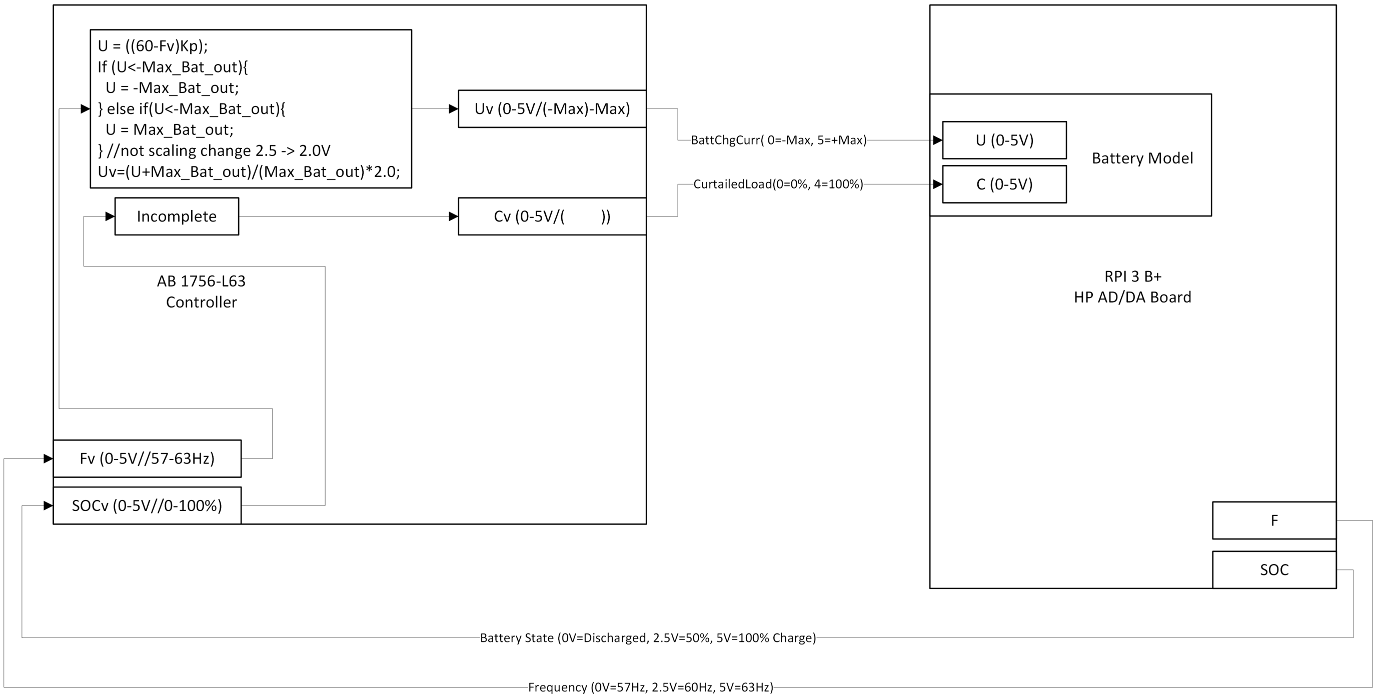
The impact to any of these from a data integrity or denial of service (DOS) attack on the communications network is dependent on the importance of the individual data and its use in the overall control of the microgrid operation, whether automated with a feedback loop or manually controlled by an operator. Examples of mitigating nonspecific attacks on the network that might be attempting change local controller gains or set points would be to disconnect the controller from the network and confirm the set points and gains are nominal or default. For example, set frequency set point to 60 Hz and gains to a nominal value even if there are potentially optimal values from the supervisory control. In this way the asset may still nominally contribute to frequency stability without the central controller input. If there are multiple assets contributing to frequency stabilization, one asset could be shutdown and taken out of service, should a compromise or misbehavior of the device be detected. Other devises may adequately maintain frequency stability while the suspect one is repaired, reconfigured or replace.

Implementation of the network includes standard hardware-based network interface using transmission control protocol -internet protocol (TCPIP) within the RPi's, but this can also be enhanced using Mininet network emulations for additional complexity of the network design. The complexity of the network is designed to distribute the network assets, i.e., generation, loads and frequency controls, through segmentation using SDN. The SDN are utilized as the response that achieves the mitigation, and depending on the type of attack and how SDN is implemented, a physical effect is noted. This trade-off space, as previously discussed, is then achieve through experimentation that informs the desired mitigation within a level of acceptable impact to the function. As different network designs are tested against different attacks, this understanding generates the resilience of the overall system and ultimately the cyber resilience of the design. For denial of service, these can include packet loss, throughput and round trip time (RTT) to determine the availability of a link.

IV. Cyber Example Setup

A. *Notional Scenario Narative*

A narrative of the scenario follows: A prominent university has a microgrid that contains several photovoltaic systems, energy storage devices and controls that supplements power to the university. In addition, the microgrid provides a test range for advanced energy storage and microgrid controls concepts for researchers at the engineering college. An autonomic intelligent cyber-physical sensor (AICPS) [5] has been installed on the network for performance testing by the computer science and electrical engineering department as part of a collaboration. In this collaboration, the computer scientists are integrating a cyber-only detection with a physics-based approach from the electrical engineers. The continued running of experiments provides a diverse data set to vet their AICPS. The network communications and security for the microgrid devices are maintained by the university's information technology (IT) communications group. This network is normally isolated from all university traffic through a private enclave, and has no internet activity. However, during a weekend of testing, one of the researchers desired to update the firmware/software on a few microgrid smart devices to accompany testing. To do these updates, he connects his laptop, which is connected to a personal hotspot, to the private enclave, and bridges the microgrid network to allow internet downloads and microgrid device updates. Unbeknownst to the researcher, his laptop has a virus that has placed a remote access Trojan (RAT). The RAT allows for a malicious actor to use this laptop as a platform for launching compromises. The threat actor has already performed reconnaissance of the private research network; however, the threat actor has prior knowledge of the microgrid. Later forensics and investigation will discover the threat actor was a former graduate student who was barred



```
U = ((60-Fv)Kp);
If (U<-Max_Bat_out){
  U = -Max_Bat_out;
} else if(U<-Max_Bat_out){
  U = Max_Bat_out;
} //not scaling change 2.5 -> 2.0V
Uv=(U+Max_Bat_out)/(Max_Bat_out)*2.0;
```

Fig. 2. Pseudocode for Frequency Control using Energy Storage

from accessing the microgrid any further from research due to inappropriate use of the equipment. His intentions were to disrupt other researchers' experiments, and the investigation from the scenarios that follow.

B. *Physical and Cyber Metrics*

The ability to recognize the impact of cyber attack, and more specifically, mitigating benefit are the primary basis for applying this microgrid network. Within the design of this system, frequency is controlled by the modulation of generation and energy sources. Responses to disturbances in latency effect the communications of the data that are obvious in trending information from Equations 2 and 3. These, as well as data integrity attacks that effect set point transmission to the frequency controller, power data from individual generators, or data to the operator, would result in anomalies that would also be obvious in trending.

To measure the overall effectiveness of the cyber mitigation, an evaluation of the cyber effects to the ICS operation should also be understood. This is specifically in light of denial of service attacks, that may or may not impact the resulting physical system depending on the amount of latency and the ICS and physical function effected. Packet loss, throughput and round trip time (RTT) are critical metrics to determine the availability of a link. Equation 4, the Mathis equation, allows us to estimate these values.The maximum segment size for this environment is 1480 bytes. The metrics for responses for the attack testing that follows is provided in table II.

$$M = \frac{MSS}{RTT} * \frac{1}{\sqrt{(p)}} \tag{4}$$

where MSS = Maximum Segment Size, RTT = Round Trip Time, p = Packet Loss. The systems physical adaptive capacity with an asset removed or reconfigured may also need to be evaluated prior to taking a mitigating action that might have excessive risk of causing an instability to the system. Metrics such as those described in [6] could be considered to evaluate the impact of disabling or adjusting the gains in a way that change the response of the asset.

C. *Scenario Cyber Attacks*

Two types of attacks will be considered for demonstration of the SPEMMCRA toward the notional university system that exploits the RAT in the scenario, a DOS and data integrity attack. Table I provides a taxonomy for these attacks. The table also includes a set of potential cyber resilient responses to the attack and the resulting physical effects. Where there are multiple options, the particular cyber resilient response that is relevant for this demonstration is highlighted within the table. Bearing in mind our prior discussion on the exchange of information and effects, the table provides more detailed consideration on the tradeoff space action versus physical effects.

V. Scenario results

The SPEMMCRA is designed for scalable application of cyber responses that result in physical effects for a trade-off analysis. The purpose of this test bed is to avoid costly high fidelity physical real-time simulation, using a emulation that provides sufficient fidelity to understand time dependent effects. If a detailed analysis of a real system is required, high fidelity real-time simulators, such as RTDS or Opal-RT, should

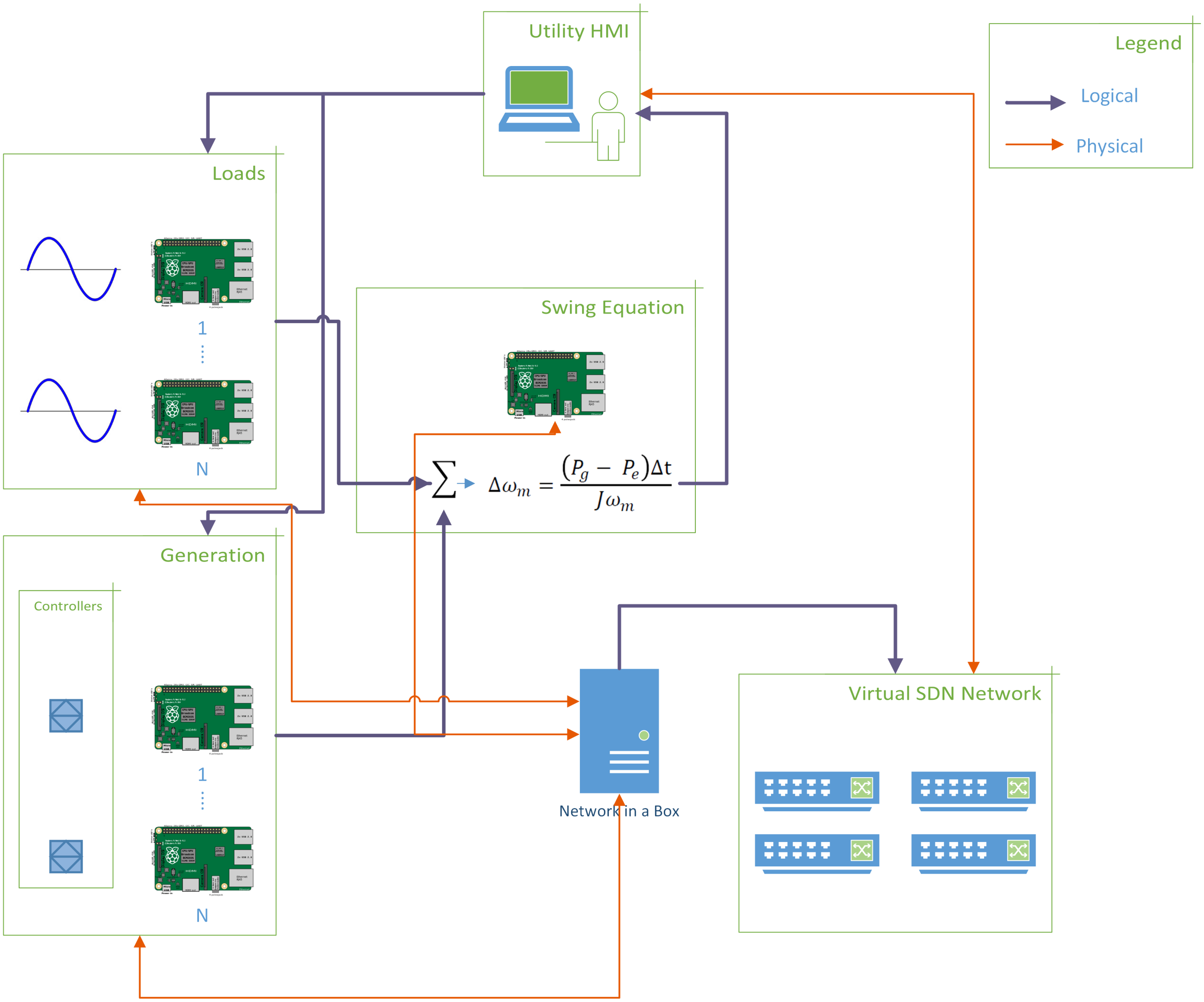


Fig. 3. SPEMMCRA Network Example

be used in place of the RPis. The scenarios that follow, which include both a denial of service and data integrity, provide a perspective on the type of results that can be expected.

For the AICPS application, a number of the students were running experiments on the microgrid. The former graduate student desired to interfere with these experiments, and did this through denial of service and data integrity attacks. The impacts of these attacks is analyzed through SPEMMCRA, which included analysis of how these attacks could have been mitigated using software defined network (SDN) switches.

A. Denial of Service

A denial of service (DOS) attack eliminates or delays communication to one or multiple assets in a cyber-physical system. DOS may be caused accidentally from a poor system configuration or it may be caused deliberately by overwhelming a systems resources. A DOS may be cyber or physical in nature. A cyber DOS occurs when an end device such as a controller, or a network device like a router is unable to communicate due to their TCP/IP stack being overwhelmed. A DOS attack attempts to eliminate communications between legitimate devices by generating a large amount of traffic to the point the legitimate devices can no longer serve traffic to one another. A physical DOS which may be caused by disconnecting a physical device is out of the scope of this case study.

A DOS attack can target either the sensing or command portion of a cyber-physical control loop. In our case study, Fig. 4 shows the results of a DOS against the battery. This attack prevents the controller from receiving sensing measurements from the battery. The effect is a noticeable drop in frequency from 60 HZ to 59.9 HZ. The SOC is hardly effected and closely mirrors the normal SOC. Fig. 5 shows a DOS attack

TABLE I
CYBER ATTACK TAXONOMY AND RESILIENT RESPONSE

Attack Taxonomy	**Denial of Service**	**Data Integrity**
Vector	HMI, Controller, Routers, Servers, Switches	Header Based
Possible Target	Breaks control feedback loop	HMI, Controller
Network Effect	Halts routing and switching to multiple devices	Control loop is compromised; false control values resent
Cyber Resilient Response	Moving Target Defense (MTD) Block incoming packets by source address using SDN Redirect traffic to virtual network Disable system processes if coming from known host	Place controller and HMI on new network segment using SDN Detect and block physical port of attacker using SDN MTD
Mitigative Benefit	Prevents targeting of end devices Blocks attackers' access to send packets on network Allows attack to continue on a non-critical network Stops attack from insider threat or compromised device	Restore the control loop Removes man in the middle Prevents attacker from Targeting control loop
Physical Effect	Mitigation may generally save the system, but the rerouting the traffic will cause potential loss of monitoring or response, i.e., inability to send new set points or controller responses out of date due to bad data.	Mitigation removes compromised data, which could be acted upon, but may have ancillary effects and would require an assurance that any controller or logic that uses it is placed in a good state. This good state is still a degraded state.

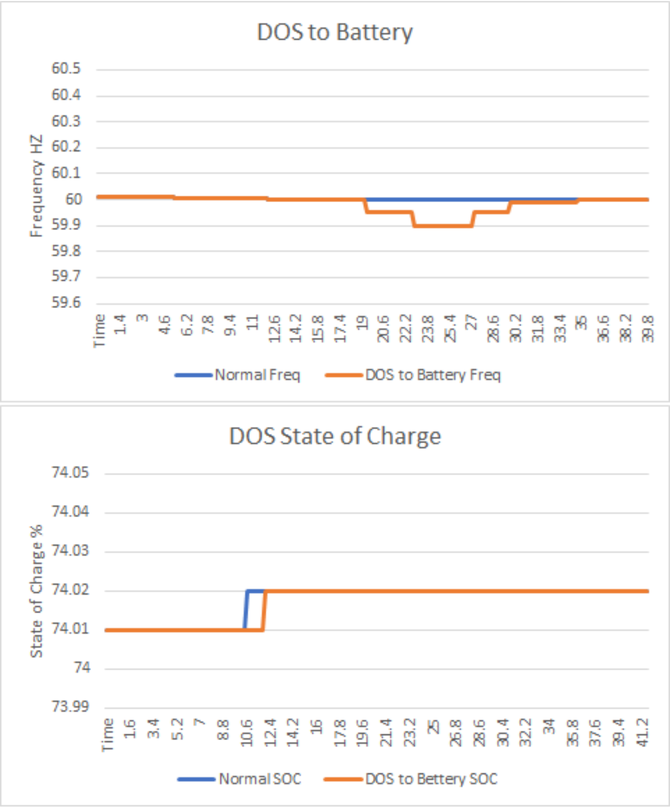


Fig. 4. Physical Effects of a DOS Against the Battery

against the controller. This attack prevents the battery from receiving control commands and causes an increase to frequency from 60 HZ to 60.04 HZ.

The ability of SPEMMCRA to support both virtual and physical connections allows for the collection of necessary results on all virtual and physical links. This data includes full packet captures and link speed measurements at every node in the network. The combination of calculated and empirical values shows the impacts of both the DOS attack and the selected response actions.

Table II illustrates the network statistics both calculated using equation 4 and measured from the testbed. Average throughput is the average amount of total traffic per second during an attack or normal operation. The maximum throughput refers to the calculated theoretical throughput available to legitimate traffic during an event. In the case of the DOS the average throughput jumps from 176 B/s to 9.77 gb/s which leaves only 9.22 B/s of bandwidth available to legitimate traffic. Approximately 5.2% of normal control traffic is maintained which results in severe physical anomalies.

The automated response is the same for both attack scenarios. The flow rules allowing incoming traffic to each device is removed and replaced by the ARE to establish a secondary physical link between the battery and state of charge controller. This effectively resolves the attack in the DOS to the battery in 7.8 seconds and the DOS attack to the controller in 10.6 seconds.

B. Data Integrity

An integrity based attack against a control system attempts to modify packets in the control loop. The attack can change the commands being written to a physical device. Changes can also be made to the measurements being sent from a sensor to the controller. This could result in commands that would cause a physical device to take inappropriate actions that could drive the values of the system out of bounds.

In this case study, the attacker intercepts the control packets from the controller and flips the sign of the control value. This causes the opposite intended change to the physical system. Fig. 6 show the effects on frequency and SOC in the battery. The attack commences at 23.2 seconds and immediately causes the battery to increase charge which lowers the frequency to 58.2 hz.

TABLE II
NETWORK STATISTICS

	RTT (ms)	Packet Loss (%)	Average Thoughput	Maximum Thoughput
SDN Out of Band	0.038	0	285 B/s	9.85 gb/s
In-Band Normal	0.038	0	176 B/s	9.85 gb/s
Network Scanning	0.043	0	308 B/s	8.71 gb/s
Denial of Service	183	77	9.77 gb/s	9.22 B/s
DNP3 Integrity Attack	0.039	0	203 B/s	9.6 gb/s

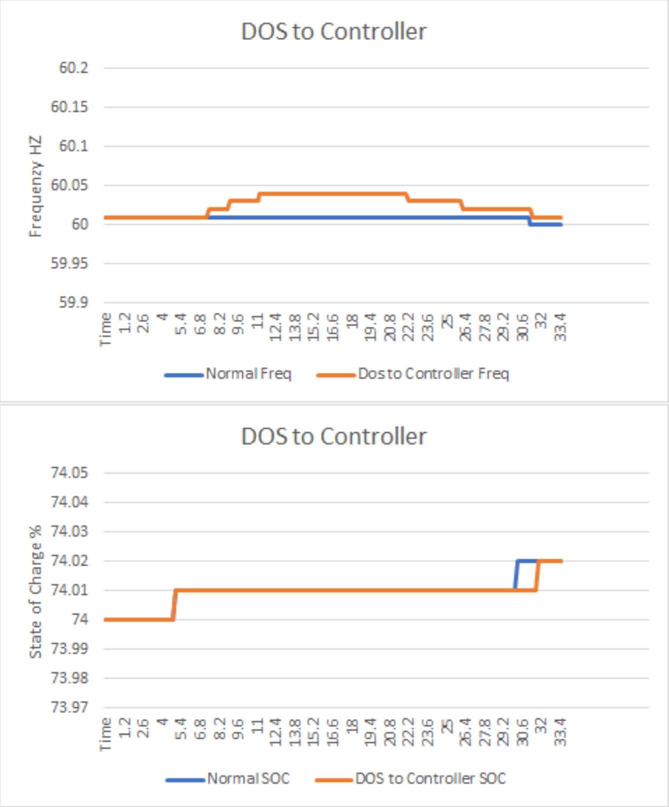


Fig. 5. Physical Effects of a DOS Against the Controller

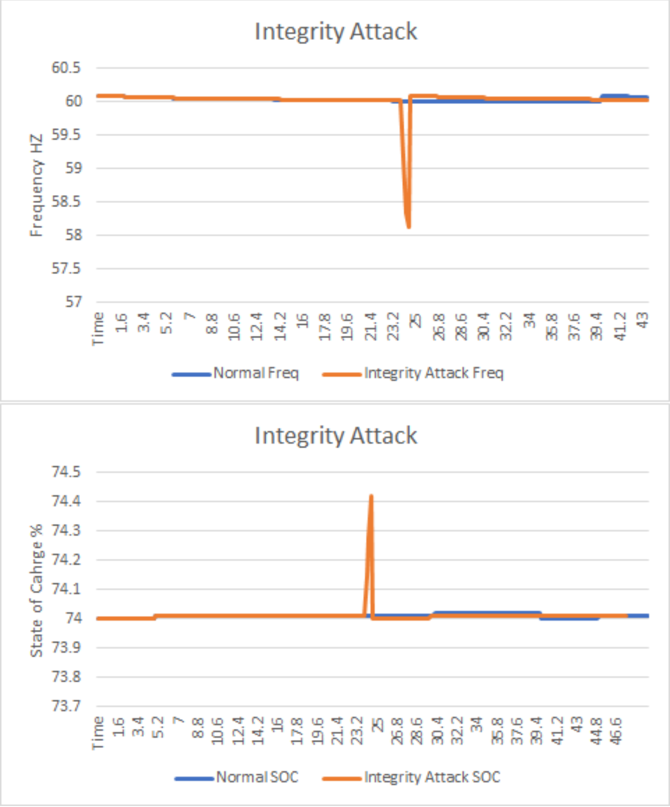


Fig. 6. Physical Effects of an Integrity Attack Against DNP3 Communication

SPEMMCRA enabled the programmatic control of the automated responses. The cyber response to this attack is implemented in a single script that integrates with all nodes in the test. The response works by blocking the physical port of the attacker. This action eliminates their ability to conduct a man in the middle attack and returns control to the SOC controller which immediately corrects the physical anomaly and returns the frequency to 60 HZ by quickly discharging the battery.

VI. SUMMARY AND CONCLUSIONS

This paper detailed SPEMMCRA, a networked ICS that controls a simulation of the frequency response represented by the swing equation. SPEMMCRA suports multiple loads and base generation which are balanced through the control of an emulated battery and power inverter. The simulated plant, which is implemented in Raspberry Pi computers, provides an inexpensive platform to realize the physical effects of cyber attacks to show the trade-offs of available mitigations. The simulated plant also included a commercial Allen-Bradley ICS controller to introduce real world implementation of feedback controls.The system can be scaled by incorporating many RPis representing various assets that may be connected to more controllers. The scalability is limited to the number of RPis and controllers available. Note a RPi could also be coded with the controller function.

SPEMMCRA was shown to enable the novel configuration of virtual and physical ICS and network devices. Two cyber attack case studies were presented to include a DOS and an integrity attack against the control of the emulated battery. SPEMMCRA provided the emulation of control loops and SDN capabilities necessary to asses ICS device security and test effect of automated responses. The case studies showed SPEMMCRA is a useful research tool, which provides the capabilities of collecting emperical network data used to address the effects of cyber attacks and responses in ICS environments.

VII. ACKNOWLEDGEMENTS

This work was supported by the Office of Naval Research under grant number N000141812395. We thank our colleagues Professor Masood Parvania, PhD and Jairo Trujillo, PhD. from the University of Utah who provided insight and expertise that assisted this research. Effort performed through Department of Energy under U.S. DOE Idaho Operations Office Contract DE-AC07-05ID14517, as part of the Resilient Control and Instrumentation Systems (ReCIS) program of Idaho National Laboratory.

REFERENCES

[1] A. S. V. Venkataramanan and A. Hahn, "Real-time co-simulation testbed for microgrid cyber-physical analysis," in *2016 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Vienna, Austria, 2016, pp. 1–6.

[2] T. R. McJunkin, C. G. Rieger, B. K. Johnson, D. S. Naidu, L. H. Beaty, J. F. Gardner, I. Ray, K. L. Le Blanc, and M. Guryan, "Interdisciplinary Education through "Edu-tainment" Electric Grid Resilient Control Systems Course," in *2015 ASEE Annual Conference &amp; Exposition*. Seattle, Washington: ASEE Conferences, Jun. 2015. [Online]. Available: https://peer.asee.org/24349

[3] J. J. Grainger, *Power System Analysis*, 1st ed. New York: McGraw-Hill Education, Jan. 1994.

[4] Center for Advanced Energy Studies. Idaho falls power: Hydro energy production and load. [Online]. Available: http://http://wind-for-schools.caesenergy.org/wind-for-schools/IF˙Power.html

[5] T. Vollmer and M. Manic, "Cyber-physical system security with deceptive virtual hosts for industrial control networks," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1337–1347, 2014.

[6] T. R. McJunkin and C. G. Rieger, "Electricity distribution system resilient control system metrics," in *2017 Resilience Week (RWS)*, Sep. 2017, pp. 103–112. [Online]. Available: https://ieeexplore.ieee.org/document/8088656