energies

MDPI

Article

Transmission and Distribution Real-Time Analysis Software for Monitoring and Control: Design and Simulation Testing

Dan Zhu [1], Murat Dilek [1], Max Zhong [1], Abhineet Parchure [2,*], Robert Broadwater [2], Nicholas Cincotti [3], Timothy Kutchen [3], Scott Placide [3] and Luan Watson [3]

[1] National Information Solutions Cooperative, Blacksburg, VA 24060, USA
[2] Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24061, USA
[3] Pepco Holdings Inc., Washington, DC 20068, USA
* Correspondence: abhineet@vt.edu

Abstract: The US electric grid is facing operational, stability, and security challenges. Transmission system operators need some measure of visibility into distribution system renewable generation. Distribution system generation needs to support transmission system voltage. The grid is experiencing an expansion in measurement systems. How to take full advantage of this expansion and defend against attacks, both cyber and physical, poses additional challenges. This paper introduces software designed to meet these challenges. At the center of the software is an Integrated System Model (ISM) that spans from transmission to secondary distribution. The ISM is employed in real-time abnormality detection, voltage stability forecasting, and multi-mode control. The software architecture along with selected analysis modules is presented. Testing results are presented for: 1—attacks on utility infrastructure; 2—energy savings from optimal control; 3—distribution system control response during a low voltage transmission system event; 4—cyber-attacks on PV inverters, where physical inverters are used in hardware-in-the-simulation-loop studies. Contributions of this work include real-time analysis that spans from three-phase transmission through secondary distribution; an approach for detecting abnormalities that employs measurements from three independent measurement systems; and a multi-mode distribution system control that responds to cyber-attacks, physical attacks, equipment failures, and transmission system needs.

Keywords: Integrated System Model (ISM); Graph Trace Analysis (GTA); Advanced Metering Infrastructure (AMI); Supervisory Control And Data Acquisition (SCADA); coordinated control; cyber-attack; smart inverter

Citation: Zhu, D.; Dilek, M.; Zhong, M.; Parchure, A.; Broadwater, R.; Cincotti, N.; Kutchen, T.; Placide, S.; Watson, L. Transmission and Distribution Real-Time Analysis Software for Monitoring and Control: Design and Simulation Testing. *Energies* **2023**, *16*, 4113. https://doi.org/10.3390/en16104113

Academic Editor: Yun Liu

Received: 27 February 2023
Revised: 22 April 2023
Accepted: 6 May 2023
Published: 16 May 2023

1. Introduction

The US is transitioning to a renewable-based electric grid [1]. The growth of renewable generation is posing problems. Transmission system operators need some measure of visibility into distribution system generation and operations. Distribution system generation must support transmission system voltage. This paper introduces real-time analysis software designed to address emerging grid operational, stability, and security challenges. At the center of the software is an Integrated System Model (ISM). An ISM integrates distinct transmission, substation, primary distribution, and secondary distribution models from different utility organizational silos into a memory-efficient, one-source-of-truth model. The ISM maintains topology and offers the topology to generic algorithms that run on the ISM. Graph Trace Analysis (GTA) is used by the algorithms to implement matrix-free calculations [2].

In addition to the growth in renewable generation, utilities are experiencing a tsunami of grid data from diverse systems. How to take full advantage of this expansion and defend against attacks, both cyber and physical, poses challenges. A voltage regulator can fail on its lowest tap, or a substation measurement can be set with a gain that is off by 50%,

and today such problems are often not discovered until a customer's refrigerator motor becomes noisy. The ISM software includes algorithms that via power flow analysis correlate data from diverse measurement systems, discovering abnormalities at the time they occur. When multiple abnormalities are discovered, GTA traces are used to discover a common source of the abnormalities.

The ISM-based, real-time analysis software includes a multi-mode, coordinated control that employs an optimal power flow. Operational problems resulting from abnormalities can be mitigated with multi-mode control [3–5], where different control strategies are used for different abnormalities and/or objectives. Maximizing energy savings while controlling voltage can be achieved by using different modes of control for different conditions, for example, one control mode for blue-sky day (no solar fluctuations) conditions, and one for high solar PhotoVoltaic (PV) variability conditions. This allows utilities to choose condition-appropriate, time-series voltage profiles for the control system to target. In the multi-mode control, the setpoints of control devices, including smart inverters, are coordinated along a feeder according to an optimal, time-series, power flow solution. This coordination increases voltage stability margins, helps to avoid oscillations among inverters, and improves energy savings.

In the ISM software, the same GTA power flow algorithm is used for transmission, radial distribution, lightly meshed distribution, and heavily meshed distribution [6–9]. The GTA power flow has been demonstrated to be faster than traditional power flow algorithms. In some time-series analysis cases, the GTA power flow has run as much as 24 times faster than traditional power flow analysis [10]. In comparing with traditional power flow practice, two enhancements in fidelity employed here are:

- Transmission is modeled as three-phase [11];
- Distribution secondary circuit conductors are modeled [12].

The GTA power flow can compute maximum loading limits for lines and busses [2,13]. This ability, together with forecasted load and renewable generation, is used by the ISM software to forecast voltage stability.

The work presented here makes three contributions. First, the ISM used in real-time analysis, monitoring, and control, models transmission as three-phase, and the model spans from transmission through secondary distribution. Previous works have used balanced transmission system models and have not modeled secondary distribution conductors [14–19]. Second, the abnormality detection presented uses statistical analysis of the ISM together with measurements from three independent measurement systems to detect cyber-attacks, physical attacks, equipment failures, and instrument failures. Previous works have not used three independent measurement systems, nor have they addressed detecting such a broad range of attacks [14–19]. It may be noted that the abnormality detection presented here was inspired by utilities using the GTA power flow with SCADA and customer load measurements, where the correlation of the two independent measurement sets through the power flow analysis led to the discovery of failed substation instrumentation, large kWhr meters that were connected backwards, and voltage regulators that had failed on the low tap [7,20–22]. Third, the multi-mode distribution system control presented controls the voltage profile to realize maximum economic benefits while responding to cyber-attacks, physical attacks, equipment failures, instrumentation failures, and transmission system voltage support needs. Previous works have not addressed this broad range of control modes for mitigating detected abnormalities [14–19].

Section 2 introduces the architecture of the ISM software system. Section 3 describes three of the analysis modules. Results from selected studies are presented in Section 4, where studies considered include attacks on the utility system, energy savings, and a transmission system low voltage event with concurrent attacks on PV inverters. Physical inverters in a hardware-in-the-simulation-loop are employed. Section 5 presents conclusions.

2. ISM Real-Time Software

The ISM real-time software takes in weather forecasts, PV generation forecasts, Supervisory Control And Data Acquisition (SCADA) measurements, bellwether Advanced Metering Infrastructure (AMI) voltage measurements, and PV inverter measurements, and time synchronizes the measurement sets. An overview of the software architecture is shown in Figure 1. There are four core analysis modules:

1. Faster-Than-Real-Time Simulator (FTRT): Performs time-series, power flow analysis employing the following four forecasts, where the load forecast is generated in the Data Engine of Figure 1 [23].
    a. One-minute step-size, 30 min native load forecast;
    b. One-minute step-size, 30 min PV generation forecast;
    c. One-hour step-size, 24 h native load forecast;
    d. One-hour step-size, 24 h PV generation forecast.
2. Abnormality Detection: Detects abnormalities that are affecting the operation of the power system. Abnormalities include cyber-attacks, physical attacks, failed instrumentation, failed controllers, and unknown system operations.
3. Voltage Stability Analysis: Forecasts voltage stability of lines and busses, alarming on low voltage stability margins or events that could lead to voltage collapse, such as loss of renewable generation below a load bus that creates an instability.
4. Coordinated Control: For each controllable device, provides time-series, voltage setpoints based on a multi-mode, coordinated control strategy, where control considers voltage control, energy savings, voltage stability, and abnormal operations. For each control mode, a desired feeder voltage profile range (i.e., lower and upper bounding curves) is specified.

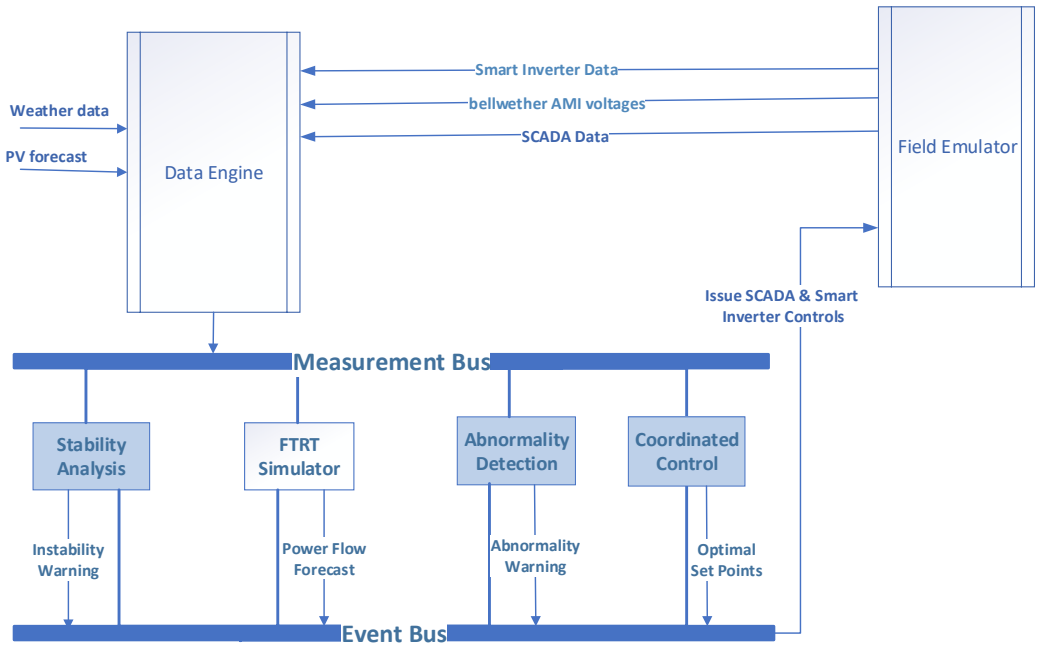

Figure 1. ISM Real-Time Software Architecture Overview.

Three features to be noted about the ISM real-time software architecture of Figure 1 are:

1. Event-driven microservices implement each analysis module (e.g., Stability Analysis of Figure 1) as a self-hosting service. That is, the execution of each analysis module is triggered by events that are generated from other services in the software system (e.g., forecast ready, anomalies detected, etc.). The data bus (represented by the Measurement and Event busses of Figure 1) provides a consistent interface across all analysis modules. The data bus processes all the inter-module communications,

including synchronous and asynchronous requests. Using predefined interfaces exposed by the data bus, all the modules obtain measurements and forecasts as data service clients and exchange analysis results. This flexible design allows adding or removing software modules without impacting the rest of the system. Multiple modules of the same type can be added to scale to larger systems.

2. Data Engine provides a single-entry point for input data. The data engine encapsulates data gathering, filtering, and time synchronization into one self-hosting unit. This insulates the analysis modules from impacts of data interface updates. Embedded in the Data Engine is a weather-dependent, native load forecast. There are two native load forecasts, a 30 min load forecast with a one-minute step size and a 24 h forecast with a one-hour step size. The load forecast is based on stochastic, weather-dependent load models derived from customer AMI load and/or SCADA data [23]. Using the input PV forecasts, the Data Engine contains a statistical analysis of the PV variability of each PV generator. PV variability statistics for aggregates of generators being controlled together (i.e., generators grouped into an aggregate receive the same control strategy) are derived and used to determine if there is a level of PV variability at which the inverters under ISM software control cannot control the system voltage within desired limits. The desired voltage limits are by default set to the voltage control deadbands on nearby voltage regulators or switched capacitor banks. That is, the inverters should control the voltage variations during high PV variability such that utility control devices do not move.
3. Field Emulator is used for use case testing. The emulator applies the control settings from the multi-mode, Coordinated Control to the control devices simulated in the emulator ISM (note, the control settings can also be applied to physical control devices if hardware-in-the-simulation-loop is being employed, as discussed below). That is, the emulator performs power flow analysis, where the analysis results are used to emulate real-time measurements. The emulator also simulates threat scenarios by reading in a script that specifies changes to the power flow results being passed to the Data Engine, thus simulating measurements being corrupted or failed. A threat scenario script can also change the control commands from the Coordinated Control, simulating cyber-attacks, control equipment failures, or unknown operations.

3. Overview of Core Analysis Modules

As illustrated in Figure 1, four analysis modules in the ISM software are: Stability Analysis, Faster-Than-Real-Time (FTRT) simulator, Abnormality Detection (AD), and Coordinated Control (CC). GTA is used in all modules. The FTRT module is a time-series, GTA power flow analysis employing the load and PV generation forecasts. This section focuses on the other three analysis modules.

3.1. Stability Analysis

The voltage Stability Analysis employs the GTA power flow. The GTA power flow can solve loading conditions up to and beyond the tip of the steady-state voltage stability curve [2,13]. The Stability Analysis uses this capability to determine the additional load that can be added to each bus or line beyond which voltage instability arises. Lines or busses approaching their unstable load condition are alarmed. Using the forecasted loading and renewable generation for the day, a voltage stability forecast with one-hour step sizes is performed. The total amount of renewable generation below each load bus is also forecasted. Voltage stability margins at each bus are then evaluated for the contingency of losing all PV generation below the bus. When the Stability Analysis raises a voltage stability event, the CC switches to the stability mode, providing support to the transmission system. This will be illustrated with a low voltage event in Study 3 below.

3.2. Abnormality Detection

Error statistics between time-series, power flow analysis, and field measurements can provide intelligence for detecting abnormalities, where error statistics for SCADA measurements, AMI voltage measurements, and smart inverter voltage measurements are employed. Having error statistics based on historical measurements, the results of the FTRT simulator can be compared against field measurements and statistically unexpected errors that exist for a few measurement samples can be flagged as abnormalities. Abnormalities can be due to cyber-attacks, failed controllers, failed instruments, physical attacks, unknown operations of field devices, and others.

The Abnormality Detection (AD) runs periodically, adapting to the measurement interval of the field data. Figure 2 illustrates the AD program flow. Once a new set of measurements are available from the Data Engine, AD starts by first screening the measurement set, looking for measurements that fall outside of the historically expected statistical range. First consider the path in Figure 2 where there are no out-of-range measurements. In this case, AD compares the real-time simulation results to the voltage measurements at bellwether AMI meter locations. If one or more outliers are found, then feeder path circuit traces [1] are performed from the outlier locations to try to find a common source of the anomaly, such as a malfunctioned voltage control device.

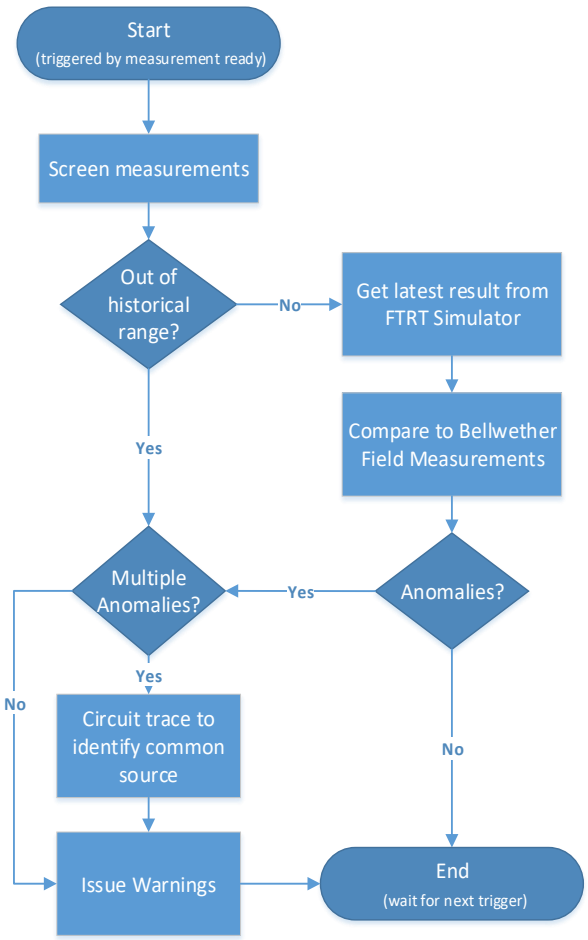

Figure 2. Abnormality Detection Program Flow.

Now consider the path in Figure 2 where one or more measurement comparisons falls outside of the expected statistical range. Again, in this case feeder path traces are used to try to identify a common source for the anomalies.

3.3. Coordinated Control

The multi-mode, Coordinated Control (CC) algorithm determines two voltage control schedules, a 30 min schedule for smart inverters, and a 24 h, hourly schedule for utility control devices. The 30 min schedule is updated approximately every 30 min, whereas the 24 h schedule runs at midnight and is only updated when forecasts change and/or when certain events occur, such as switching operations. The objective of CC is to achieve a desired feeder voltage profile range as measured at AMI bellwether meter locations, where the desired voltage profile consists of voltage ranges for each hour. For instance, at 10:00 the desired voltage range may be [118 V, 119 V]. The desired feeder voltage profile is a function of [24]:

- Amount of renewable generation variability;
- Voltage stability event;
- Abnormality event.

Thus, in determining the 24 h control schedule, CC seeks to minimize

$$\sum_{t=1}^{n} \sum_{m=1}^{N} |vbm(t) - vpm(t)| \quad (1)$$

where

t = hour index
n = 24
m = bellwether meter index
$vb_m(t)$ = power flow voltage at bellwether meter m for hour t
v_L = lower limit for desired voltage profile for hour t
v_H = upper limit for desired voltage profile for hour t
$vp_m(t)$ = desired voltage for hour t, where

$$vp_m(t) = vb_m(t) \text{ if } v_L < vb_m(t) < v_H, \text{ else} \quad (2)$$

$$vp_m(t) = v_L \text{ if } vb_m(t) < v_L, \text{ else} \quad (3)$$

$$vp_m(t) = v_H \text{ if } vb_m(t) > v_H. \quad (4)$$

Thus, Equation (1) minimizes over time the absolute values of the difference between bellwether meter voltages and desired values for bellwether meter voltages. If a power flow bellwether voltage falls within the desired range for an hour, it does not add to the cost.

All existing voltage control devices, such as Substation Load Tap Changers (LTCs), voltage regulators, switched capacitor banks, and inverters that are available for control, are used by CC to achieve the desired voltage profile. This gives CC the highest possible controllability, constrained by the size and location of these assets. Ideally, each distribution feeder would have optimally placed and sized control assets that CC uses, but the control algorithm is designed to work with whatever control assets are made available to it. An optimal power flow employing a Discrete Ascent Optimal Programming search [25] is used to determine the voltage setpoints for the control devices. Each control device receives a voltage setpoint corresponding to the voltage from the optimal power flow solution. The voltage setpoints vary across control devices throughout the feeder, and for each control device the voltage setpoints vary throughout the day.

CC runs when

- A new 24 h native load and/or renewable generation forecast becomes available;
- A new 30 min native load and renewable generation forecast becomes available;
- There is a change in circuit configuration;
- There is a voltage stability event;

- There is an abnormality event.

For the 24 h forecast, if utility control device motion is deemed too high, then the control device moves in the planned 24 h control schedule are reduced such that the loss in energy savings is minimized. That is, limiting the motion of the utility control devices can increase energy usage. In performing the reduction in control device motion, a Discrete Ascent Optimal Programming search is used for selected control device types. That is, LTC motion may be limited while not limiting motion of voltage regulators or switched capacitor banks. Conversely, LTC and voltage regulator motion may be limited while not limiting motion of switched capacitor banks. Or, motion of all utility control devices may be limited, where the maximum number of moves of an LTC may be different than the maximum number of moves of a voltage regulator, and likewise for switched capacitor banks.

For the 30 min forecast, CC updates control modes and voltage settings for inverters, where the intent is to have the inverters control voltage variations due to significant renewable generation variations. When high renewable generation variations are anticipated, CC changes the control modes of inverters from maximum real power generation (unity power factor) to voltage control (volt-var curve), where the voltage control setpoints of inverters located at different locations along the circuit take on different values.

In the absence of voltage stability and abnormality events, and for low levels of renewable generation variability (e.g., less than 5% variability), CC seeks to maximize energy savings. The desired voltage profile range is configurable, where the default desired voltage range is the same at all points along the feeder. With PV generation present, the voltage profile used to maximize energy savings varies from daytime to nighttime and may vary throughout the day. Along with implementing CVR savings, this control maximizes power production from inverters while controlling voltage. Furthermore, controlling to a lower voltage profile will allow greater levels of PV generation to operate on the feeder.

If CC forecasts that high generation variations will result in utility control device deadbands being exceeded, CC widens the utility device control deadbands during the period of high variations. This widening of the deadbands reduces the motion of the utility control devices.

For a transmission system voltage stability event, CC seeks to maximize reactive power support for the transmission system by raising the voltage profile across the feeder to a high voltage level. For an abnormality event where the cause of the abnormality is not known, CC seeks to keep the voltage midway between high and low voltage limit violations. If the cause of the abnormality is predicted and confirmed by the operator, then CC can act to offset the cause. For instance, if a voltage regulator is identified as being failed on its low voltage tap, then the power flow analysis sets the voltage regulator to failed on the low voltage tap, and CC neglects the voltage regulator in control calculations. In this case, CC can run in the maximum energy savings mode while the abnormality exists.

4. Abnormality Detection (AD) and Coordinated Control (CC) Studies

Three studies are presented in this section. The first study focuses on testing the ability of AD to detect attacks on utility system infrastructure and PV inverters. The second study evaluates the energy savings of CC over the existing control. The third study evaluates the response of CC to a transmission system low voltage event while simultaneous cyber-attacks are occurring on PV inverters. The third study incorporates two physical inverters in hardware-in-the-simulation-loop experiments, and three types of cyber-attacks are considered.

Figure 3 illustrates the ISM used in the studies here, consisting of a transmission system and two distribution feeders. The transmission model has three voltage levels: 69 kV, 138 kV, and 230 kV. The total transmission load is approximately 1500 MW. There are 37 three-phase loops in the transmission system model. Figure 4 shows one of the feeder secondary circuits, along with a plot comparing AMI voltage measurements with time-series, power flow results at a customer meter on that distribution secondary. The

voltage plot shows a close match between actual, measured, time-series voltages, and those calculated using power flow on a detailed grid model.

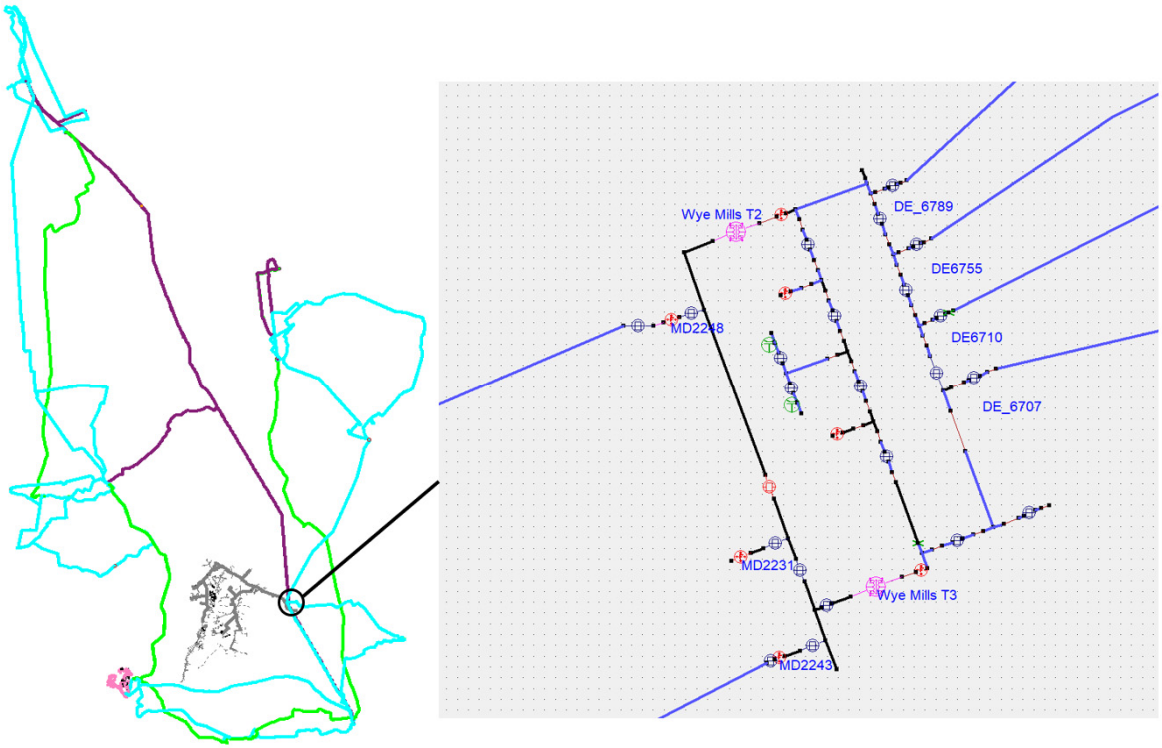

Figure 3. On the left is ISM, where transmission system is blue (69 kV), purple (138 kV), and green (230 kV), and distribution is shown in light gray and pink. On the right is a blowup of a substation showing two transformers, one of which serves the gray distribution feeder.

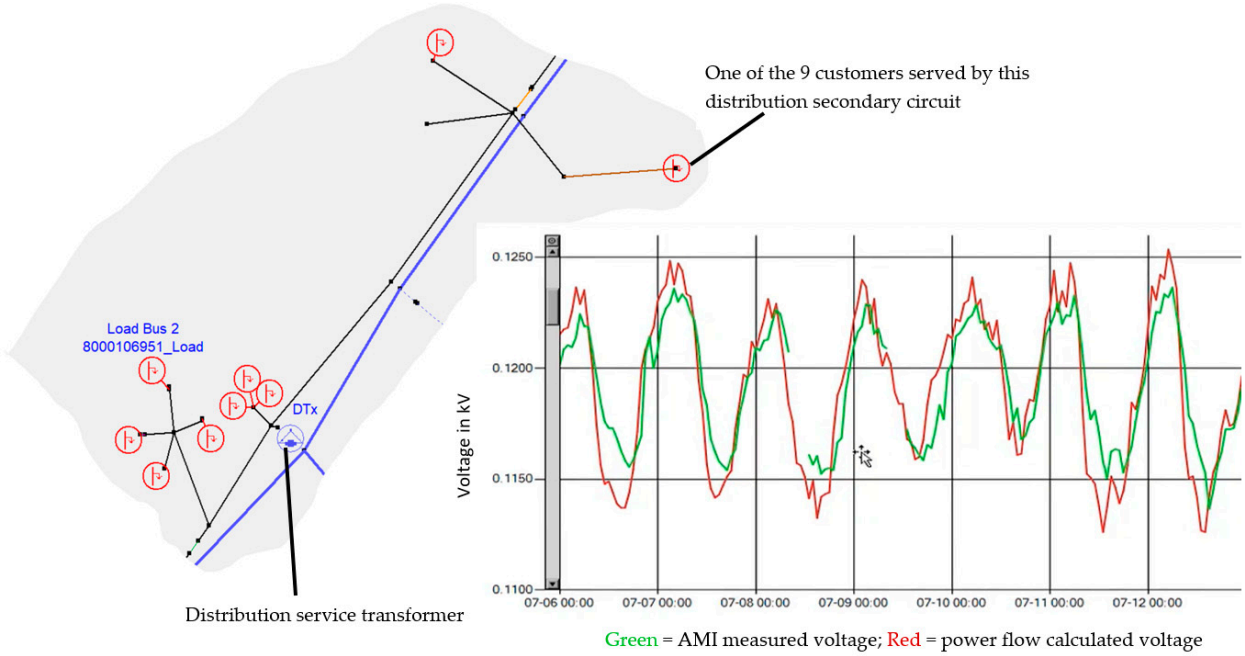

Figure 4. On the left is a blowup of a secondary circuit on the gray distribution feeder of Figure 3. On the right is a plot showing the comparison of AMI voltage measurements (green) with corresponding time-series power flow results (red) for a distribution secondary connected load.

The gray and pink distribution feeders shown in Figure 3 were selected based on the following criteria:

- Multiple PV customers including at least one large PV generator (over 1 MW);
- Multiple voltage control devices;
- AMI meter measurements available on more than 95% of the customers;
- Information about the feeders is provided in Table 1.

Table 1. Information on distribution feeders shown in Figure 3.

Description Item	Feeder 1 (Gray)	Feeder 2 (Pink)
Substation Configuration	2 XFMR Open Bus Single Feeder	3 XFMR Bus Tie
Feeder Type	Mixed	Residential
Number of Customers	2040	1627
Primary Voltage	24.94 kV, Y-G	13.2 kV, Y-G
Feeder Length	143 miles	16.52 miles
Distance from Sub to Farthest Load	15.5 miles	3.79 miles
Peak Load	17.39 MVA	6.7 MVA
Minimum Daytime Load (SCADA)	2.85 MVA	1.4 MVA
Number of Distribution Transformers	1009	194
Connected KVA	54,780	16,836
Number of Capacitor Banks	5	1
Number of Voltage Regulator Banks	1	1
Total Active PV Generation (kW)	1908	3106

4.1. Study 1. Detection of Cyber-Attacks on Utility Equipment and Inverters

In evaluating the ability of AD to detect cyber-attacks on utility equipment and inverters, 25 scenarios were selected based on a risk and impact analysis [26]. Scenarios investigated attacks on DER and inverter controls, SCADA controls (e.g., switches, reclosers, breakers), and meters (e.g., smart meters). These attack scenarios were injected into the Field Emulator of Figure 1 by third-party attackers who could change any set of measurement and/or control signals. The cyber-attack scenarios are grouped into three categories: modify, block, and delay. Table 2 presents a sample of AD detection results covering the three categories of cyber-attacks. Of the 25 scenarios, AD detected 22 attacks and partially detected three attacks, giving a success rate of 88%, where partially detected cases are not considered a success. In the partially detected cases, AD caught the major events, such as customer loss of power, but failed to recognize subtleties, such as measurements being delayed. For instance, the partially detected case shown in Table 2 resulted in all customers on the feeder losing power. In this attack, the feeder MW flow from SCADA showed a zero reading which reflected the event, so the AD program deemed the measurement valid but did not recognize that the sample rate of the meter had been reduced.

Unlike missing measurements, manipulation of the measurement sampling rate was difficult to detect. However, if changing the measurement sampling rate impacts control decisions that cause the performance of the system to deteriorate from the expected performance, then AD can detect the presence of the abnormality.

In addition to the software simulations of cyber-attacks, two physical inverters were connected in a hardware-in-the-simulation-loop (HIL) and used in cyber-attack testing. The grid-tied Primo 3.8-1 Fronius and SB3.8-US SMA inverters were chosen for the lab experiments. The HIL interconnection is illustrated in Figure 5. The two physical inverters, driven by PV simulators, replaced two secondary circuit interfaced inverters on a secondary circuit in the ISM.

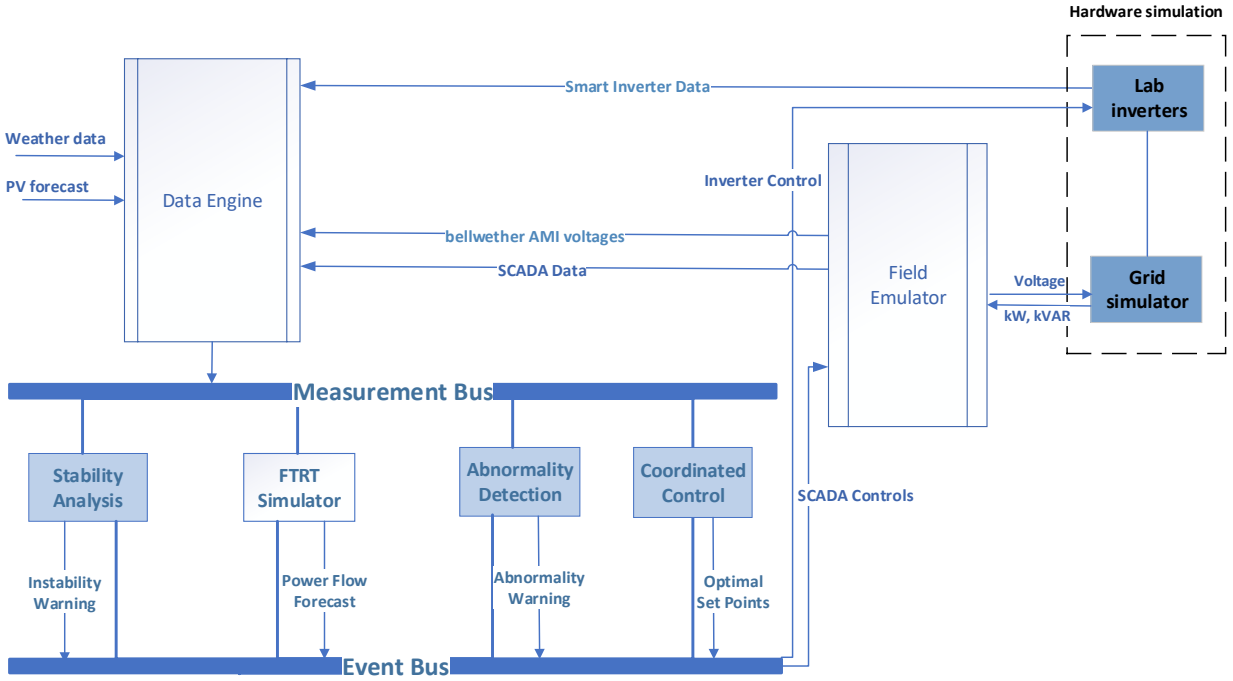

Figure 5. HIL testing employing two physical inverters.

Table 2. Sample of Abnormality Detection Results.

Category	Start Time	End Time	Device Type/UID	Manipulation	Detected?	Warning Messages	Detection Time
blocking	1 September 2020 15:30	1 September 2020 18:30	switch/recloser A	Status, open recloser	Yes	inverter INV1 in feeder 1 offline (invert rating: 1584.0 kW)	1 September 2020 16:00
	2 September 2020 17:30	2 September 2020 18:30	switch/recloser B	Status, open recloser	Yes	Loss of power detected on feeder 1, all customers downstream of recloser B	2 September 2020 18:00
delay	12 September 2020 12:00	12 September 2020 13:00	meter/M1, switch/breaker A	Status, sampling rate, delay block amount, coordinated attack between a breaker and its SACDA meter	Yes	Loss of power detected on feeder 2, NO POWER ON ENTIRE FEEDER!! Y feeder flow SCADA measurement invalid!	12 September 2020 12:00
	15 September 2020 13:00	15 September 2020 15:00	meter/M2, switch/breaker B	Status, SCADA meter sampling rate	Partial	Loss of power detected on feeder 2, NO POWER ON ENTIRE FEEDER!! Zero MW flow measurement on feeder Y	15 September 2020 13:00
modify	17 September 2020 13:00	17 September 2020 15:00	inverter/INV1	Status, power factor	Yes	inverter INV1 in feeder 1 offline (invert rating: 1584.0 kW)	17 September 2020 13:00
	18 September 2020 13:00	18 September 2020 15:00	inverter/INV2	Status, power factor	Yes	inverter INV2 in feeder 1 offline (invert rating: 69.8 kW)	18 September 2020 13:00

Twenty-three HIL attack cases, attacking either both or one of the physical inverters, were performed. These cases ranged from denial of service to intermittent power attacks to modification of the inverter controller. The AD program successfully detected 21 of the attacks. In the two undetected cases, one had a very small impact on the kW flow. The other case was an intermittent attack where the inverter output cycled between 100% and 5%. At the time when the inverter flow measurements were sampled, the inverter

output happened to be near 100%, so the attack went undetected. When all 48 attacks are considered, 25 attacks analyzed with simulation and 23 HIL attack experiments, AD had a success rate of 89.6% in detecting attacks.

4.2. Study 2. Energy Savings with Coordinated Control

For the energy savings study, Feeder 1 of Table 1 was analyzed for each of the four seasons. Using AMI load measurements and PV generation estimates, time-series power flow analysis was run twice, first using the existing control strategy, and second with CC. Table 3 presents results of the comparison.

Table 3. Seasonal and annual energy savings, carbon reduction, feeder savings, and per-customer annual dollar savings comparisons of existing control with Coordinated Control for Feeder 1.

Time Period	Energy Savings with CC (%)	Energy Savings with CC (GWh)	Carbon Reduction with CC (US Tons)	Feeder Savings with CC (USD)	Savings per Customer (USD)
Winter	3.09	0.39	166	$41,228	20.21
Spring	4.63	0.57	242	$60,155	29.49
Summer	2.60	0.37	157	$39,051	19.14
Fall	3.42	0.425	181	$44,982	22.02
Annual	3.43	1.76	746	$185,416	90.86

For calculating carbon reduction, an average carbon emission of 0.85 pounds per kWh was assumed. For calculating the per-customer dollar savings shown in Table 3, an average retail cost of electricity of 10.46 cents per kWh was used [27].

From Table 3, the economic benefits of coordinated control are seen to have the highest percentage of energy savings during Spring and Fall, 4.63% and 3.42%, respectively. Relatively lighter loading, leading to higher bellwether voltages and subsequently greater room to lower feeder voltages, can explain this observation. Summer and winter, with heavier feeder loading, are observed to have lower percentage energy savings, 2.6% and 3.1%, respectively. Table 3 shows that the total annual savings predicted for Feeder 1 is $185,416, where the annual savings for each customer is $90.86. It should be noted that there are other value streams not considered here, such as savings to the utility at peak due to high generation costs.

CC was also compared with the existing control for high PV variability and storm scenarios. To simulate high PV variability and storm conditions, clear sky, summer day, PV generation conditions were altered. For 'high PV variability', twenty dips in PV generation, going from 100% of measured generation to 10% and back to 100%, were created uniformly across two hours from 3 to 5 pm. For the storm simulation, clear sky PV generation was used for the first hour from noon to 1 pm, followed by PV generation being lowered to 20% of the rating of each PV generator for the next two hours. Table 4 summarizes the energy savings comparison between the existing control and CC. As seen from Table 4, CC still yields energy savings.

Table 4. Energy savings comparison of existing control with Coordinated Control for high PV variability and storm scenarios for Feeder 1.

Test Case	Existing Control kWh	CC kWh	Energy Savings (%)
High PV Variability (3–5 p.m.)	24,447.38	23,990.38	1.87
Storm (Noon–3 p.m.)	44,225.36	42,859.45	3.09

In the energy savings analysis presented here, the number of controllers, the size of the controllers, and the locations of the controllers were not designed for optimum operations over the time-varying load and generation. Thus, the improvements shown with CC here

are suboptimal [24,28]. Previous work has indicated that energy savings may be doubled by redesigning the feeder control devices for optimal performance [28].

4.3. Study 3. CC Response to Transmission System Low Voltage with Cyber Attacks on PV Inverters Employing Hardware-in-the-Simulation-Loop

In this study, a transmission system low voltage event is evaluated while simultaneously cyber-attacks are occurring on PV inverters, where two physical inverters are used in hardware-in-the-simulation-loop experiments. First, the performance of CC is considered without cyber-attacks, and then the performance of AD is considered for three different cyber-attacks.

Between the hours of 13:00 and 15:00 in the afternoon, the transmission system voltage falls by approximately 10% of its nominal level. In response to the low voltage, CC switches to stability mode, controlling for a desired high feeder voltage profile of 123.5 volts, and the control mode of all PV inverters is switched from unity power factor to volt-var control for supporting the feeder and transmission system voltage. An example volt-var control curve used for the inverter control is shown in Figure 6. Note that for the given inverter of Figure 6, the volt-var control center point voltage is in per unit (i.e., 1.07 per unit for voltage event in Figure 6), being determined from an optimal power flow solution. The volt-var control curve used for a specific inverter depends upon where the inverter is located along the feeder. In comparing the performance of CC with the existing control, CC caused 3.4 times more reactive power to be injected into the transmission system than the existing control, providing support to the transmission system voltage.

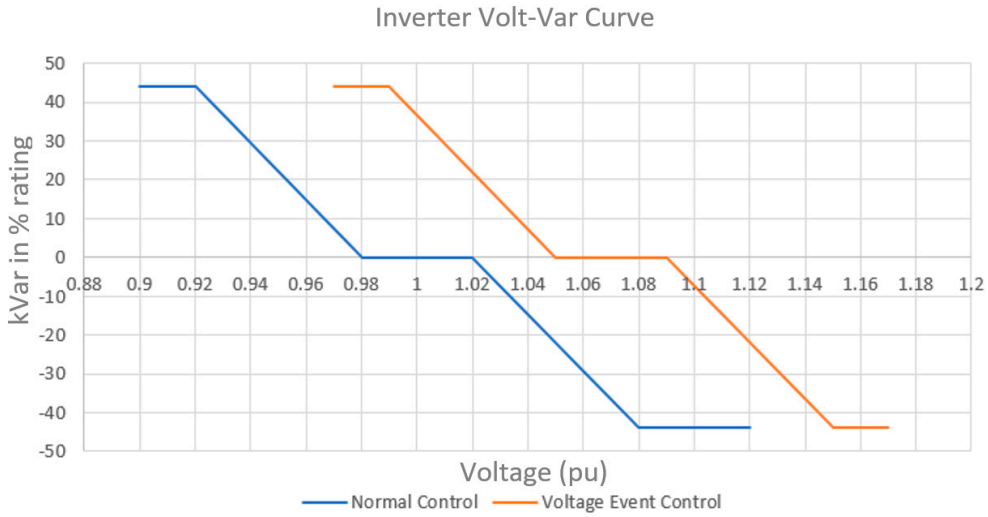

Figure 6. Example inverter control curve used during transmission system voltage event.

Employing the same transmission low voltage event (i.e., 11.6% voltage drop from 13:00 to 15:00), three types of cyber-attacks on the inverters were evaluated, where each attack targeted different inverter control variables—a real power attack, a reactive power (power factor) attack, and a standby mode attack. Details of the three cyber-attacks are provided in Table 5.

The intermittent real power attack was launched at the beginning of the transmission system voltage event. Due to the transmission system voltage event, at the start of the attack, the inverters are set to volt-var control. From Figure 7, it may be seen that the real power measurement generally trailed the expected inverter output, except at the time of attack (13:00). However, the reactive power measurements were exactly as expected; thus, the inverter was still able to provide voltage support during this attack.

Table 5. Low Voltage Grid Cyber-Attack Case Descriptions.

Case Name	Description	Start Time	End Time
Intermittent real power attack	Change the maximum power output from 100–5–100% with 1-s interval (60 cycles, 1 min)	25 August 2020 13:00	25 August 2020 13:59
Intermittent reactive attack	Change power factor excitation from under-over-under excited with 3-s interval (30 cycles, 1.5 min)	26 August 2020 13:00	26 August 2020 13:59
Standby mode attack	Disconnect inverter from the grid	27 August 2020 14:00	27 August 2020 14:59

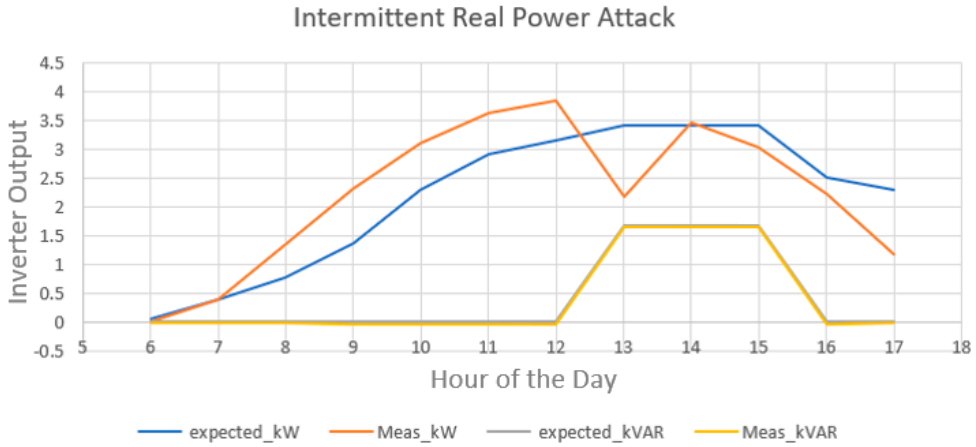

Figure 7. With low voltage grid from 13:00 to 15:00, inverter expected kW (blue), measured kW (orange), expected kVAR (grey), and measured kVAR (yellow) flows for intermittent real power attack on inverters, where expected and measured kVAR values are the same.

As explained in Section 3.2, the expected inverter real power output (used by AD as a comparison reference) is from the PV generation forecast. The kW flow measurement is read from the inverters. The physical inverters are powered by a PV simulation instead of actual PV panels, and the PV simulator output is driven by a set of predefined PV measurements. To create more realistic variations in the PV outputs, some noise was masked onto the predefined PV measurements, and the noise-modified PV measurement fed to AD as the expected PV generation. This kind of measurement masking was used in all cyber-attack cases to train AD to recognize cyber-attack signatures among noise. Therefore, the expected and measured kW flows shown in Figure 7 and in Figures 8 and 9 (to be considered below) do not match, even at the time points when there is no attack.

The intermittent reactive power factor attack resulted in the inverter acting against the expected control (i.e., absorbing vars instead of injecting vars) during the time of attack. Figure 8 shows that the attack only affected the reactive power and did not change the real power significantly. The absorbing of reactive power by the inverters drew the feeder voltage further down when the feeder voltage was already low.

Via the inverter modbus control, a hacker can remotely switch a smart inverter into standby mode. This would be a cyber-attack where a hacker breaches the modbus communications. If the PV inverter is operating under CC, the attack can be detected from the abnormal inverter measurements. Figure 9 shows that both the measured real and reactive power flows dropped to zero when the attack happened, and that they are drastically different than the expected real and reactive power outputs.

In summary, the AD program was able to detect all three cyber-attacks during the low voltage grid condition. Except for the attack on real power output, CC lost inverter voltage control capability. During the low voltage event, the attack on the reactive power control may be argued to be the worst, since the attack resulted in the feeder absorbing vars from the transmission system.

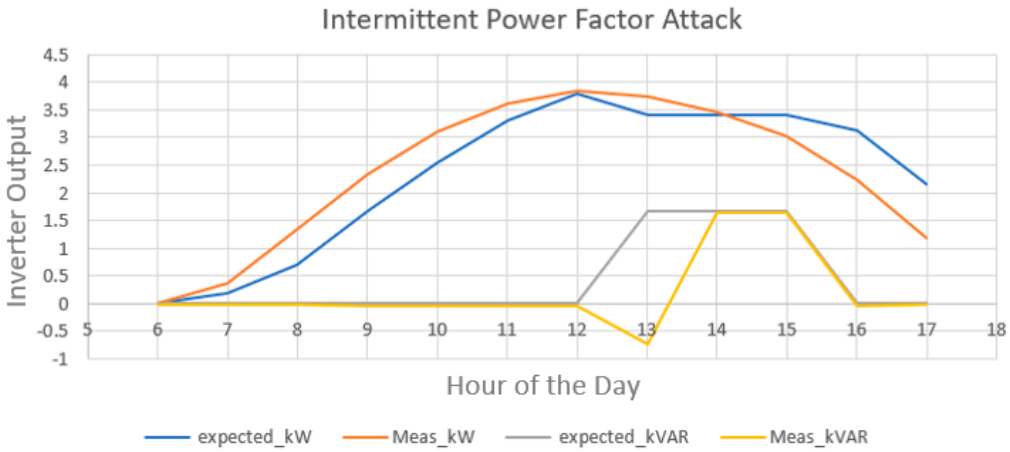

Figure 8. With low voltage grid from 13:00 to 15:00, inverter expected kW (blue), measured kW (orange), expected kVar (grey), and measured kVar (yellow) flows for intermittent power factor attack on inverters.

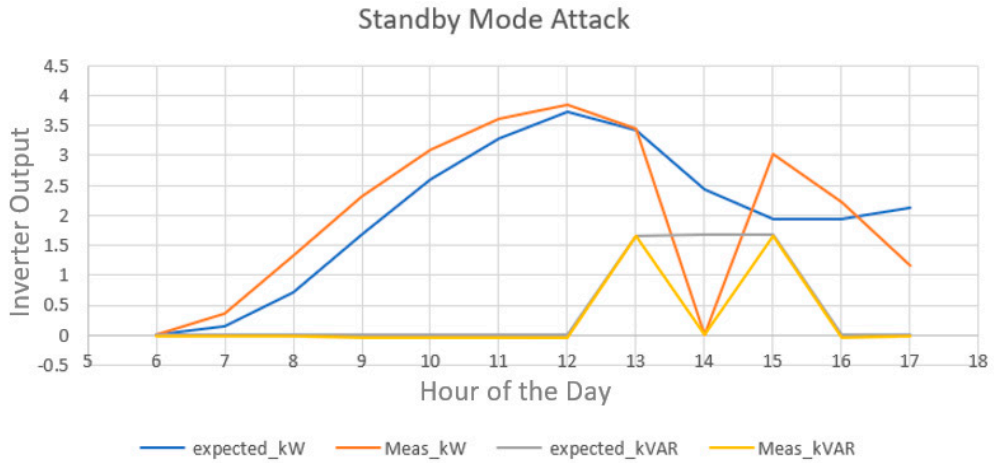

Figure 9. With low voltage grid from 13:00 to 15:00, inverter expected kW (blue), measured kW (orange), expected kVAR (grey), and measured kVAR (yellow) flows for standby mode attack on inverters.

5. Conclusions

In reaching for more clean and distributed energy, the electric grid is becoming more complex. Complexity is managed with models, especially in situations never experienced before. In an energy-independent grid, the number of generators and storage devices is going to be orders of magnitude larger than today. The models used to manage the increased complexity will also be orders of magnitude larger than the models used today. The ISM-based work presented here is a step toward this future.

The real-time ISM software architecture, based on event-driven microservices and time synchronization of diverse measurement streams, provides extensibility. With this architecture, new abnormality detection modules can be added without touching existing code. Likewise, new control modules for mitigating abnormalities can be added while maintaining the existing control modules, such as coordinated control.

The Abnormality Detection is a last-ditch effort in defending against cyber-attacks, physical attacks, failed infrastructure, and unknown system operations that significantly affect operations. For the 51 cases considered, AD had an overall success rate of 90.2%.

To mitigate equipment failures and attacks, to coordinate transmission and distribution system control, to optimize energy usage, and to provide for the highest levels of renewable penetration that can be achieved, a multi-mode control strategy is needed. With Coordinated Control, voltages are controlled to agree with the results of an optimum power flow solution. Comparisons of Coordinated Control with an existing control have been

presented for seasonal energy savings, storm energy savings, high PV variability energy savings, and distribution system support of transmission system voltage. Other control modes described include abnormalities and confirmed abnormalities.

The test results presented here predict that the ISM-centric, real-time software can improve grid situational awareness, help discover and mitigate abnormal operations, reduce costs, and improve voltage stability margins. The ISM real-time software is to be field tested at a U.S. utility. One area of improvement identified by the authors includes using cloud technology to run grid simulations at scale, in a performant and cost-effective manner. Another area of further improvement includes using data to automate the build and near-real-time tuning of grid models to enhance model accuracy.

Author Contributions: Conceptualization, A.P. and R.B.; methodology, D.Z., A.P. and R.B.; software, D.Z., M.D., M.Z. and A.P.; validation, A.P.; formal analysis, D.Z., R.B., M.D., M.Z. and A.P.; investigation, D.Z., R.B., M.D., M.Z. and A.P.; resources, N.C., T.K., S.P. and L.W.; data curation, D.Z., M.Z., N.C. and L.W.; writing—original draft preparation, D.Z., R.B. and A.P.; writing—review and editing, M.D., M.Z., A.P., R.B., N.C., T.K., S.P. and L.W.; visualization, M.Z.; supervision, D.Z., R.B. and N.C.; project administration, D.Z., R.B. and N.C.; funding acquisition, R.B. All authors have read and agreed to the published version of the manuscript.

Funding: This material is based on work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office Award Number DE-EE0008768.

Data Availability Statement: Publicly available reports and data are available from U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy under Award Number DE-EE0008768.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kroposki, B.; Johnson, B.; Zhang, Y.; Gevorgian, V.; Denholm, P.; Hodge, B.-M.; Hannegan, B. Achieving a 100% Renewable Grid: Operating Electric Power Systems with Extremely High Levels of Variable Renewable Energy. *IEEE Power Energy Mag.* **2017**, *15*, 61–73. [CrossRef]
2. Tbaileh, A.; Jain, H.; Broadwater, R.; Cordova, J.; Arghandeh, R.; Dilek, M. Graph Trace Analysis: An Object-Oriented Power Flow, Verifications and Comparisons. *Electr. Power Syst. Res.* **2017**, *147*, 145–153. [CrossRef]
3. Broadwater, R. A design approach for a power plant feedwater control system. *IEEE Control Syst. Mag.* **1983**, *3*, 4–11. [CrossRef]
4. Hambrick, J.; Broadwater, R.P. Configurable, Hierarchical, Model-Based Control of Electrical Distribution Circuits. *IEEE Trans. Power Syst.* **2011**, *26*, 1072–1079. [CrossRef]
5. Jung, J.; Onen, A.; Arghandeh, R.; Broadwater, R.P. Coordinated control of automated devices and photovoltaic generators for voltage rise mitigation in power distribution circuits. *Renew. Energy* **2014**, *66*, 532–540. [CrossRef]
6. Dilek, M.; de Leon, F.; Broadwater, R.; Lee, S. A Robust Multiphase Power Flow for General Distribution Networks. *IEEE Trans. Power Syst.* **2010**, *25*, 760–768. [CrossRef]
7. Cheng, D.; Zhu, D.; Broadwater, R.; Lee, S. A Graph Trace Based Reliability Analysis of Electric Power Systems with Time Varying Loads and Dependent Failures. *Electr. Power Syst. Res.* **2009**, *79*, 1321–1328. [CrossRef]
8. Jain, H.; Parchure, A.; Broadwater, R.P.; Dilek, M.; Woyak, J. Three-Phase Dynamic Simulation of Power Systems Using Combined Transmission and Distribution System Models. *IEEE Trans. Power Syst.* **2016**, *31*, 4517–4524. [CrossRef]
9. Jain, H.; Bhatti, B.A.; Wu, T.; Mather, B.; Broadwater, R. Integrated Transmission-and-Distribution System Modeling of Power Systems: State-of-the-Art and Future Research Directions. *Energies* **2021**, *14*, 12. [CrossRef]
10. Bhatti, B.; Broadwater, R.; Dilek, M. Integrated T&D Modeling vs. Co-Simulation—Comparing Two Approaches to Study the Smart Grid. In Proceedings of the 2019 IEEE Power & Energy Society General Meeting (PESGM), Atlanta, GA, USA, 4–8 August 2019.
11. Omran, S.; Broadwater, R.; Hambrick, J.; Dilek, M.; Thomas, C.; Kreikebaum, F. Load Growth and Power Flow Control with DSRs: Balanced vs Unbalanced Transmission Networks. *Electr. Power Syst. Res.* **2017**, *145*, 207–213. [CrossRef]
12. Parchure, A.; Tyler, S.J.; Peskin, M.A.; Rahimi, K.; Broadwater, R.; Dilek, M. Investigating PV Generation Induced Voltage Volatility for Customers Sharing a Distribution Service Transformer. *IEEE Trans. Ind. Appl.* **2017**, *53*, 71–79. [CrossRef]
13. Bhatti, B.; Broadwater, R.; Dilek, M. Analyzing Impact of Distributed PV Generation on Integrated Transmission & Distribution System Voltage Stability—A Graph Trace Analysis Based Approach. *Energies* **2020**, *13*, 4526.
14. Zhang, Y.; Wang, J.; Chen, B. Detecting false data injection attacks in smart grids: A semisupervised deep learning approach. *IEEE Trans. Smart Grid* **2021**, *12*, 623–634. [CrossRef]

15. Duan, N.; Yee, N.; Otis, A.; Joo, J.Y.; Stewart, E.; Bayles, A.; Spiers, N.; Cortez, E. Mitigation strategies against cyberattacks on distributed energy resources. In Proceedings of the 2021 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2021, Washington, DC, USA, 16–18 February 2021; pp. 1–5. [CrossRef]
16. Sridhar, S.; Govindarasu, M. Model-based attack detection and mitigation for automatic generation control. *IEEE Trans. Smart Grid* **2014**, *5*, 580–591. [CrossRef]
17. Olowu, T.O.; Dharmasena, S.; Jafari, H.; Sarwat, A. Investigation of false data injection attacks on smart inverter settings. In Proceedings of the 2020 IEEE CyberPELS, Miami, FL, USA, 14–16 April 2020; pp. 1–6. [CrossRef]
18. Liu, Z.; Wang, Q.; Tang, Y. Design of a cosimulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems. *IEEE Access* **2020**, *8*, 95997–96005. [CrossRef]
19. Majumdar, A.; Agalgaonkar, Y.P.; Pal, B.C.; Gottschalg, R. Centralized volt-var optimization strategy considering malicious attack on distributed energy resources control. *IEEE Trans. Sustain. Energy* **2018**, *9*, 148–156. [CrossRef]
20. Cheng, D.; Onen, A.; Zhu, D.; Kleppinger, D.; Arghandeh, R.; Broadwater, R.P.; Scirbona, C. Automation Effects on Reliability and Operation Costs in Storm Restoration. *Electr. Power Compon. Syst.* **2015**, *43*, 656–664. [CrossRef]
21. Onen, A.; Cheng, D.; Broadwater, R.P.; Scirbona, C.; Cocks, G.; Hamilton, S.; Wang, X.; Roark, J. Economic Evaluation of Distribution System Smart Grid Investments. *Electr. Power Compon. Syst.* **2014**, *43*, 224–233. [CrossRef]
22. Onen, A.; Jung, J.; Dilek, M.; Cheng, D.; Broadwater, R.P.; Scirbona, C.; Cocks, G.; Hamilton, S.; Wang, X. Model-Centric Distribution Automation: Capacity, Reliability, and Efficiency. *Electr. Power Compon. Syst.* **2016**, *44*, 495–505. [CrossRef]
23. Zhong, S.; Broadwater, R.; Steffel, S. Medium Term Stochastic Load Model for Transformer and Feeder from AMI Load Data Spectral Analysis. *Int. J. Electr. Power Energy Syst.* **2017**, *91*, 1–9. [CrossRef]
24. Zhu, D.; Jain, A.K.; Broadwater, R.; Brunac, F. Feeder Voltage Profile Design for Energy Conservation and PV Hosting Capacity Enhancement. *Electr. Power Syst. Res.* **2018**, *164*, 263–271. [CrossRef]
25. Broadwater, R.; Dolloff, P.; Herdman, T.; Karamikhova, R.; Sargent, A. Minimum Loss Optimization in Distribution Systems: Discrete Ascent Optimal Programming. *Electr. Power Syst. Res.* **1996**, *36*, 113–121. [CrossRef]
26. Zografopoulos, I.; Konstantinou, C.; Tsoutsos, N.G.; Zhu, D.; Broadwater, R. Security Assessment and Impact Analysis of Cyberattacks in Integrated T&D Power Systems. In Proceedings of the MSCPES '21: Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, Virtual Event, 19–21 May 2021.
27. U.S. Energy Information Administration. Available online: https://www.eia.gov/tools/faqs/faq.php?id=74&t=11 (accessed on 3 March 2022).
28. Rahimi, K.; Jain, H.; Parchure, A.; Rousan, T.; Broadwater, R. Selecting and Redesigning Distribution Feeders for CVR Benefits. *Glob. J. Res. Eng.* **2016**, *16*, 9–16.