TU Delft

Delft University of Technology

Document Version
Final published version

Citation (APA)
Naglic, M., Joseph, A., Pan, K., Popov, M., Meijden, M. V. D., & Palensky, P. (2019). Grid Awareness Under Normal Conditions and Cyber-Threats. In P. Palensky, M. Cvetković, & T. Keviczky (Eds.), *Intelligent Integrated Energy Systems: The PowerWeb Program at TU Delft* (pp. 55-75). Springer. https://doi.org/10.1007/978-3-030-00057-8_3

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
In case the licence states “Dutch Copyright Act (Article 25fa)”, this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.

Green Open Access added to TU Delft Institutional Repository

'You share, we take care!' - Taverne project

https://www.openaccess.nl/en/you-share-we-take-care

Otherwise as indicated in the copyright section: the publisher is the copyright holder of this work and the author uses the Dutch legislation to make this work public.

Chapter 3
Grid Awareness Under Normal Conditions and Cyber-Threats



Matija Naglic, Arun Joseph, Kaikai Pan, Marjan Popov, Mart van der Meijden and Peter Palensky

Abstract The situational grid awareness is becoming increasingly important for power system operations due to smaller operational margins, wide range of uncertainties entailed by renewables and highly critical infrastructure failures due to potential cyber-attacks. In this chapter, we look at some of the state-of-the-art technologies to monitor events in a power system under normal operating condition, followed by detection algorithms for regular business risk events, such as faults and equipment failures, and finally, we look into methods for quantifying vulnerability of under the rare and men-orchestrated cyber-attacks. First, we outline an architecture of a central piece of today's grid awareness system, Wide Area Monitoring, Protection and Control technology. Next, we review an event detection method used to identify and record faults and failures in the grid. Finally, we present a method for vulnerability assessment of grids under cyber-attacks.

M. Naglic (✉) · A. Joseph · K. Pan · M. Popov · M. van der Meijden · P. Palensky
Faculty of Electrical Engineering, Mathematics and Computer Science,
Delft University of Technology, Delft, The Netherlands
e-mail: m.naglic@tudelft.nl

A. Joseph
e-mail: arun.joseph@tudelft.nl

K. Pan
e-mail: k.pan@tudelft.nl

M. Popov
e-mail: m.popov@tudelft.nl

M. van der Meijden
e-mail: m.a.m.m.vandermeijden@tudelft.nl

P. Palensky
e-mail: p.palensky@tudelft.nl

© Springer Nature Switzerland AG 2019

P. Palensky et al. (eds.), *Intelligent Integrated Energy Systems*,
https://doi.org/10.1007/978-3-030-00057-8_3

3.1 Wide Area Monitoring, Protection and Control

The design, control and operation of Electric Power System (EPS) are undergoing significant changes. The environmental policies [1] are driving the society towards the zero-carbon emission by 2050 with energy production based only on renewable energy sources. The future EPS are expected to be highly interconnected (AC and DC grids) with significantly changed dynamics and dominated by intermittent renewable energy sources, typically integrated using power electronic devices. Additionally, electric vehicles as a sustainable alternative to internal combustion engine bring new patterns and challenges in energy supply. The new dynamics in energy demand and supply, unexpected disturbances, protection maloperation, and inadequate control schemes can cause system instabilities, leading to cascading failures and potentially catastrophic blackouts. A common reason for the occurrence of blackouts is lack of immediate coordinated protection and control when the EPS becomes unstable [2–4]. The conventional protection and control schemes are not designed to cope with the new local and wide area fast dynamics and states (conditions), imposed by future EPS. In the recent years, the Smart Grid technological advances in terms of sophisticated Intelligent Electronic Devices (IED), fast and reliable telecommunication links, and increased computational capacities have created new opportunities for design of next-generation monitoring, protection, and control schemes. As a result, the research and industry are driving towards advanced Wide Area Monitoring, Protection, and Control (WAMPAC) system [5]. The WAMPAC system is favorable to ensure efficient, more resilient, and secure operation of EPS by sophisticated utilisation of Smart Grid components in means of intelligent sensors, actuators, and state-of-the-art Information and Communications Technology (ICT). Typically, the WAMPAC system utilizes the advanced Synchronized Measurement Technology (SMT) [5–7] as a key building block to deliver time synchronized measurements (synchro-measurements) of electrical quantities from system-wide dispersed locations. Supported by precise time synchronization, the SMT comprises of intelligent electronic devices (IED) or Phasor Measurement Units (PMU), and Phasor Data Concentrators (PDC), connected over ICT infrastructure into a hierarchically organized network [8], as illustrated in Fig. 3.1.

3.1.1 WAMPAC-Ready Platform for Online Validation of Corrective Control Algorithms

Performance of a WAMPAC system and implemented applications is often mission critical and can in worst case scenario lead to system-wide blackout. Since actual SMT provided measurements can dramatically differ from conventional measurements, obtained from software simulations, it is prudent to extensively validate all emerging grid-saving applications under realistic conditions in an isolated and

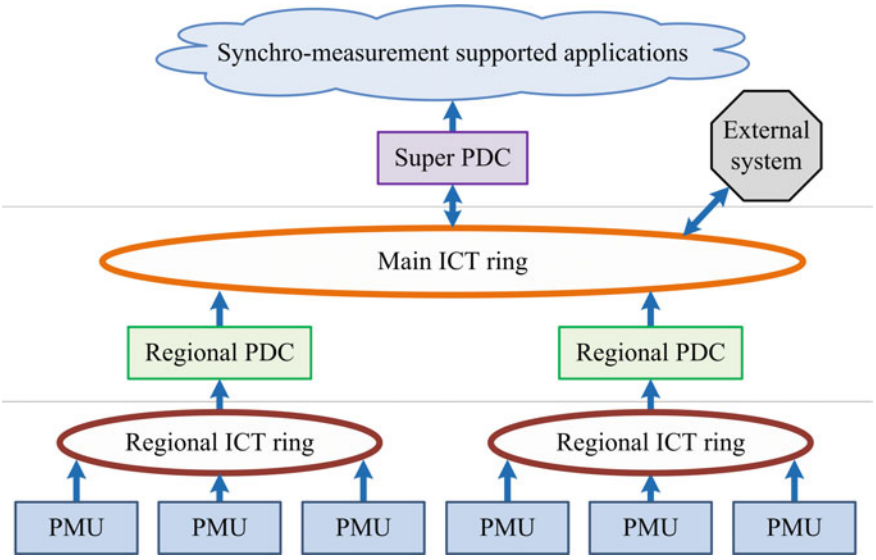

Fig. 3.1 Synchronized measurement technology infrastructure [8]

flexible simulation environment, before being implemented in an actual grid. Besides, communication delay, jitter, packet loss, available data throughput, and communication network reliability are the important factors that can significantly affect WAMPAC applications performance. To design a reliable and robust WAMPAC application, the abovementioned aspects need to be considered during WAMPAC application design and validation.

To serve this purpose, a simulation platform has been developed at the Delft University of Technology (TUD) [9], as a co simulation comprising of the SMT supported EPS model and the underlying ICT infrastructure. The presented WAMPAC-ready platform represents a cyber-physical simulator, due to the tight coupling between EPS and ICT, interacting with each other in a closed-loop manner, as illustrated in Fig. 3.2. The EPS component is represented by the RTDS real-time power system simulator with the integration of SMT components as HIL. In order to emulate the wide area ICT network, the open-source WANem network emulator and ns-3 network simulator are used as Software-in-the-Loop (SIL). To enable simplified design and online validation of WAMPAC applications, a MATLAB supported Synchro-measurement Application Development Framework (SADF) [8] has been in-house developed as SIL. In the following subsections we review the key parts of this simulation platform.

3.1.2 *Synchronized Measurement Technology Supported EPS Network with Hardware-in-the-Loop*

In order to simulate EPS phenomena, the RTDS real-time power system simulator, capable of performing electromagnetic transient simulations with a typical 50 μs time step, is used. The EPS network is built in a comprehensive RSCAD graphical user interface and simulated in the RTDS simulator in real-time. One of its main benefits is the possibility of HIL performance and compliance testing of control and measurement devices like PMUs, protective relays, circuit breakers, and control devices under realistic network conditions. Due to its modular design, it is suitable for fast prototyping and evaluation of diverse EPS applications. The simulated power system quantities (voltage and current waveforms, status signals and control commands) are exchanged between the RTDS and HIL devices in real time via numerous analog and digital input/output interfaces. In this way, feedback signals and control commands are used to change any set point or modify the EPS topology as typically performed by system operators in control centres. This functionality allows closed-loop control algorithms to be performed and evaluated under realistic conditions in a flexible simulation environment, before being implemented in the actual grids [8]. The presented platform in Fig. 3.2 consists of the SMT components needed to provide

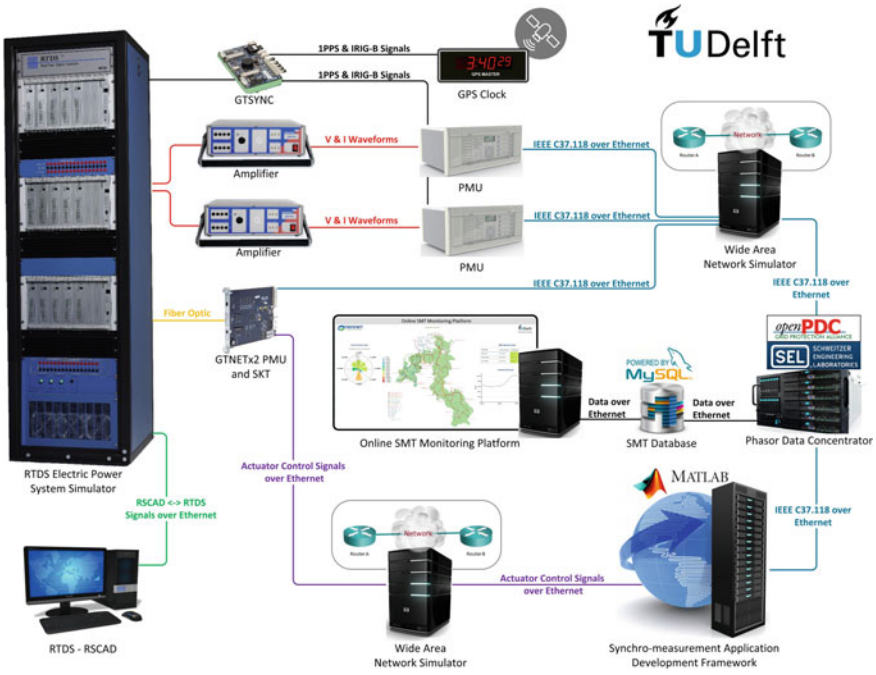

Fig. 3.2 WAMPAC-ready platform for online validation of corrective control algorithms [9]

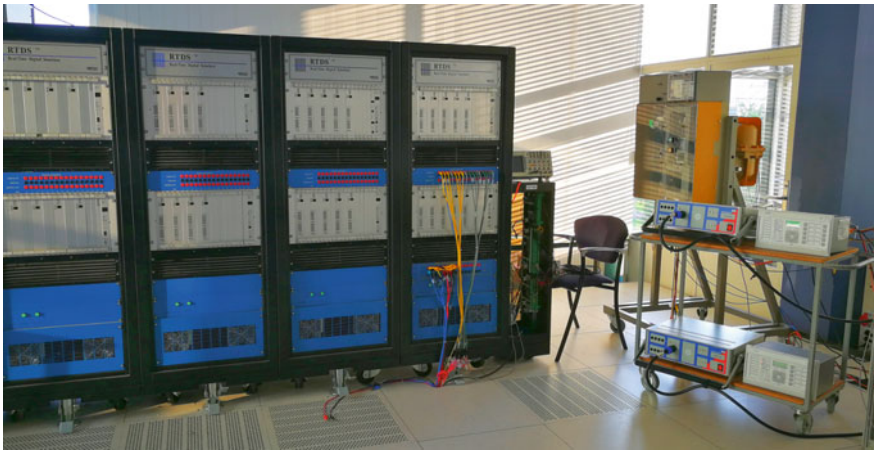

Fig. 3.3 RTDS with SMT components

real time observability of grid dynamics based on the IEEE C37.118 [10, 11] standard. Two Alstom P847 IEDs are used, each capable of measuring two current and voltage channels, in total providing four synchrophasor streams. Hereby, two high-precision Omicron CMS-156 amplifiers are used to provide suitable signal levels for direct feeding to the actual PMUs (see Fig. 3.3). In addition, up to 24 embedded PMUs provided by the GTNET2x card can be used simultaneously, which adds up to 26 PMUs available in total. Moreover, to provide accurate time synchronization a GPS grand master clock is used to provide Inter-Range Instrumentation Group code B (IRIG-B) protocol based timestamp and 1 Pulse Per Second (1PPS) time signal to a GTSYNC card and the PMUs. Additionally, the clock provides IEEE 1588 Precision Time Protocol (PTP) time synchronization to Phasor Data Concentrators (PDCs) and SADF. OpenPDC and SEL software PDCs are used to aggregate and store separate online PMU data streams. The PDCs receive synchrophasor streams from all of the PMUs in the simulation, aligns synchrophasor measurements with the identical time-tags and aggregates them into a single synchrophasor data stream, forwarded to the MATLAB based Synchro-measurement Application Development Framework [8], as presented in Fig. 3.2. Additionally, synchrophasor measurements are simultaneously stored in the MySQL database, mainly for the online monitoring purpose and off-line analyses.

To simulate telecommunication characteristics, WANem network emulator is used, which in real-time emulates communication delay, jitter, packet loss, and available data throughput for each communication channel. In addition, ns-3 network simulator is used as SIL in order to investigate different ICT network related phenomena (link and node data-congestion, jitter, delay, packet drop etc.) and to assess the cyber-security vulnerabilities (false data injection, buffer overflows, device misconfiguration). By using the aforementioned ICT network simulators, each PMU stream and send control commands can be characterised with its own unique ICT

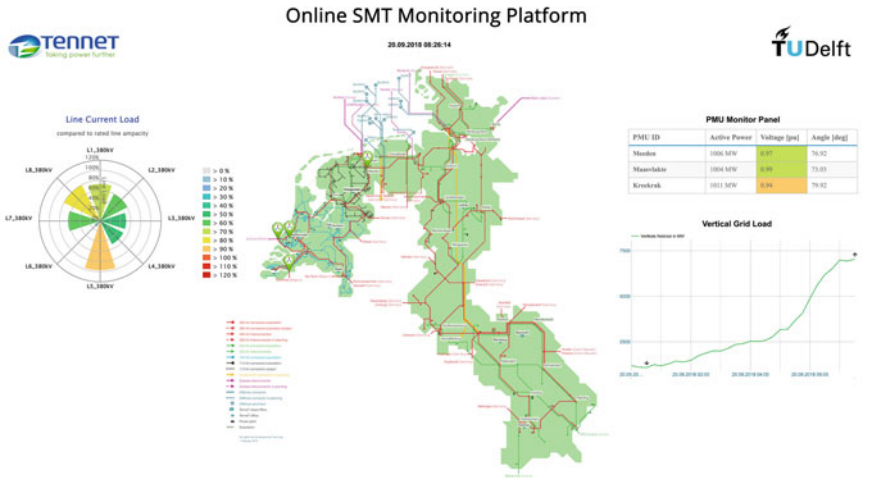

Fig. 3.4 Online SMT monitoring platform for real-time monitoring of EPS, viewed on tablet device [9]

performance characteristics that can imitate the actual ICT network conditions from the field. The presented platform can be utilized to analyse different cyber-attacks that could potentially endanger the safe operation of EPS. Different possible scenarios can be performed on the ICT components, data exchange, IEDs, and power hardware components.

3.1.3 Synchronized Measurement Technology Supported Monitoring Platform

As a part of the simulation platform [9], a web-based online SMT monitoring platform has been in-house developed (see Fig. 3.4) for the real-time monitoring of grid dynamics. The monitoring platform is mainly used for the online PMU measurements monitoring purposes, abnormal event detection and alarming, line load monitoring, offline analysis and data export. It connects to the online MySQL database, populated with the measurements from the OpenPDC. The web-platform is based on JavaScript and PHP programming languages and runs on top of the Linux operating system. Visualisation is based on HTML markup language with CCS and JQuery support. Due to the used protocols, it is cross-platform compatible (PC, tablet, smart phone) and intuitive to navigate (see Fig. 3.5).

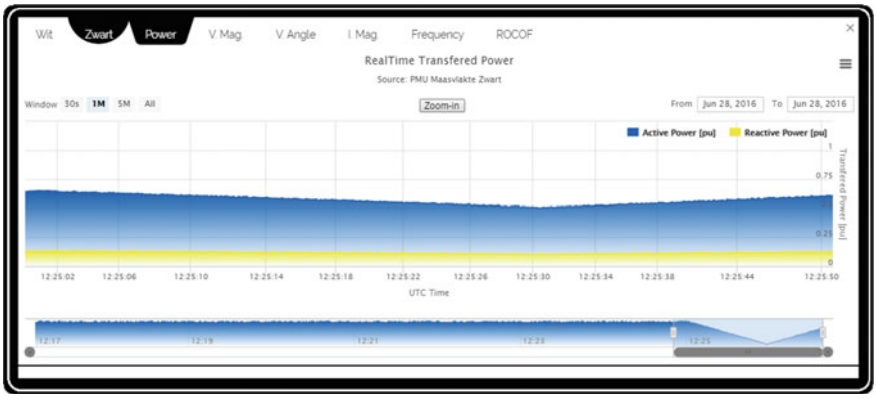

Fig. 3.5 Real-time monitoring of active and reactive power, measured by PMU device and viewed on tablet device [9]

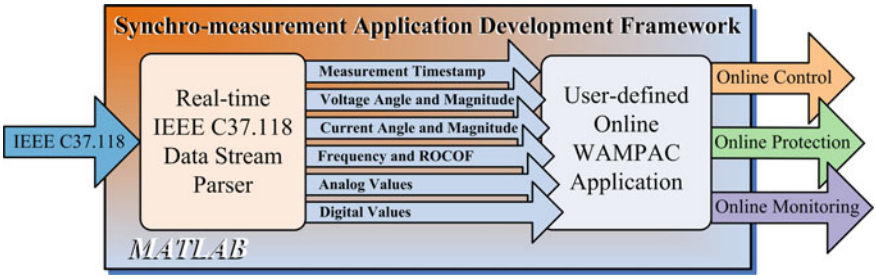

Fig. 3.6 MATLAB based Synchro-measurement Application Development Framework [8]

3.1.4 MATLAB Supported Synchro-measurement Application Development Framework

To enable a seamless integration between the SMT supported EPS and user-defined online applications, a MATLAB based Synchro-measurement Application Development Framework (SADF) has been developed (see Fig. 3.6) [8]. The SADF facilitates the real-time access and simplified use of the IEEE C37.118.2-2011 standard synchro-measurement data in the MATLAB programing environment. A MATLAB programing suite is a powerful software engineering toolbox supported the by numerous built-in mathematical, signal processing, and visualization functions. It is cross-platform compatible (Windows, Mac, Unix) and can be interfaced with C, C++, Java, Fortran, and Python programming languages. MATLAB has been a de facto programming language for research worldwide and has an extended online community support [12].

This concludes the presentation of the simulation platform. In the next section, we review a fast detection algorithm that can be used with such platform to detect and report faults to the system operator.

3.2 Fault Detection Using Synchro-measurements

The detection of a fault, its isolation and reconfiguration are important and challenging aspects power system operations and control. Components with complex dynamics interact in electrical power grids and the faults occur often. In extreme cases, they lead to cascading and highly undesirable events such as blackouts. Thus, quick fault detection is an imperative. The typical fault detection techniques are confined to the detection of a loss of a significant component (e.g., a transmission line, load, generation unit) using information from protection devices and SCADA (supervisory control and data acquisition) elements. The time scale of interest for detection is in the order of a few second up to several minutes. Modern systems, such as WAMPAC, offer high sampling rates (at the order of kHz) and potential for quicker detection and response. However, this potential for the quick response is not fully utilized due to lacking automation procedures, and thus far, WAMPAC relies on the control room operator knowledge to react after the fault has been detected. This section considers the problem of fault detection in a smart grid paradigm, where we expect the electricity grid to develop more towards a self-healing grid. Such a centralized control room based automated fault detection mechanism is proposed in this section.

The centralized control room should be equipped with tools to detect and react to undesired events, such as faults, in order to prevent cascading failures. The process starts with collecting synchro-measurements through the SMT system, as seen in Fig. 3.7. The measurements can be collected from the real system, or as in our case, from the EPS simulation, implemented in RTDS and interfaced through the GTNET cards. The second unit in Fig. 3.7 contains different fault detection algorithms that

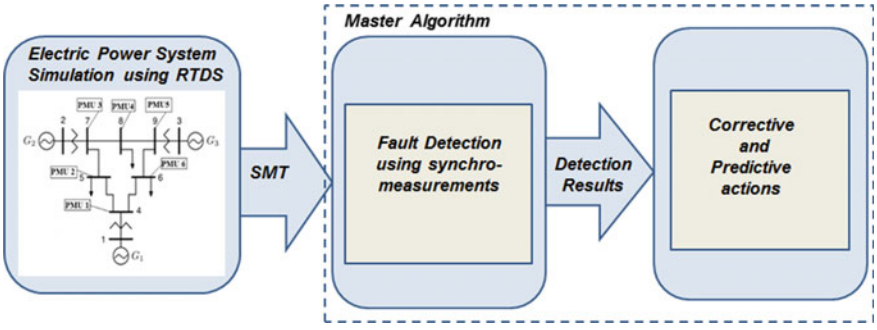

Fig. 3.7 Real-time platform

process the measurement data observing the faulty grid behavior. The third unit in the same figure consists of corrective and predictive measures. When working with synchro-measurements, if a fault is detected quickly, there often exists a sufficient time interval to predict the grid behavior before performing any action. To enable predictive actions, fast fault detection is of great importance. The further subsection illustrates the use of statistical methods as for fault detection.

3.2.1 Fault Detection Using Quickest Change Detection

In this method, the incremental changes in the net power injection at each bus are modeled as independent random variables, and the line outage is considered as a change event in the probability distribution of bus voltage phase-angle measurements obtained from SMT. As the real-time monitoring and operatability of the power systems is of great importance, extensive study has been made in line outage detection in the minimum possible time, particularly, Chen et. al in [13] proposed a method based on the theory of quickest change detection. In this subsection, a short description of the theory of QCD proposed in [13] and an application of this method for a 9 bus power system is depicted.

We consider a power system of N nodes denoted by a set $\chi = \{1, \ldots, N\}$, each of which correspond to a bus, and assume there are L edges. Let (m, n) denote the transmission line between buses m and n. Let $V_i(t)$ and $\theta_i(t)$ denote the voltage magnitude and phase angle respectively, at bus i. Also, let $P_i(t)$ and $Q_i(t)$ denote the net active and reactive power respectively, injected at bus i. In order to represent the quasi-steady-state behaviour of the power system, the real and reactive power balance components at each bus i can be written as:

$$P_i(t) = p_i\left(\theta_1(t), \ldots, \theta_N(t), V_1(t), \ldots, V_N(t)\right) \tag{3.1}$$

$$Q_i(t) = q_i\left(\theta_1(t), \ldots, \theta_N(t), V_1(t), \ldots, V_N(t)\right) \tag{3.2}$$

where $p_i(\cdot)$ and $q_i(\cdot)$ are functions used to represent the dependence on the network parameters. A linearized small signal power flow model is, however, considered and is used to perform the statistical test for change detection.

Considering the discretized version of the active and reactive power equations, we have

$$P_i[k] = p_i\left(\theta_1[k], \ldots, \theta_N[k], V_1[k], \ldots, V_N[k]\right) \tag{3.3}$$

$$Q_i[k] = q_i\left(\theta_1[k], \ldots, \theta_N[k], V_1[k], \ldots, V_N[k]\right) \tag{3.4}$$

where the time instant $t = k\Delta t$, $k = 1, 2, \ldots$ and $\Delta t > 0$. Defining $\Delta P_i[k] = P_i[k] - P_i[k-1]$, and $\Delta Q_i[k] = Q_i[k] - Q_i[k-1]$, and assuming that, for each bus i, $p_i(\cdot)$ and $q_i(\cdot)$ are continuously differentiable with respect to each θ_i and V_i at

$\theta_i[k]$ and $V_i[k]$, $\Delta P_i[k]$ and $\Delta Q_i[k]$ can be expressed using first order Taylor series expansion of (3.3) and (3.4) as

$$\Delta P_i[k] \approx \sum_{j=1}^{N} a_{ij}[2k]\Delta\theta_j[k] + \sum_{j=1}^{N} b_{ij}[2k]\Delta V_j[k] \tag{3.5}$$

$$\Delta Q_i[k] \approx \sum_{j=1}^{N} c_{ij}[2k]\Delta\theta_j[k] + \sum_{j=1}^{N} d_{ij}[2k]\Delta V_j[k] \tag{3.6}$$

where a_{ij} and b_{ij} are, respectively, the derivatives with respect to θ_j and V_j of p_i, and c_{ij} and d_{ij} are, respectively, the derivatives with respect to θ_j and V_j of q_i.

Based on the standard assumptions in the analysis of transmission systems, we have $a_{ij}[k] \gg b_{ij}[k]$, and $d_{ij}[k] \gg c_{ij}[k]$, and using the dc assumptions, $a_{ij}[k]$ becomes only the function of network alone, that is $a_{ij}[k] = a_{ij}$, and the analysis is presented only for $\Delta P_i[k]$, giving

$$\Delta P_i[k] \approx \sum_{j\in\chi, j\neq 1} a_{ij}\Delta\theta_j[k] \tag{3.7}$$

In matrix form, the above expression can be written as

$$\Delta P[k] \approx H_0\Delta\theta[k] \tag{3.8}$$

where $\Delta P[k] \in \mathbb{R}^{N-1}$ and $\Delta\theta[k] \in \mathbb{R}^{N-1}$, the entries of which are $\Delta P_i[k]$ and $\Delta\theta_i[k]$ for $i \in \chi, i \neq 1$.

The physical fluctuations in the real power injection vector $\Delta P[k]$ is modeled as independent and identically distributed Gaussian random vectors of covariance Σ, that is $\Delta P[k] \sim \mathcal{N}(0, \Sigma)$. In terms of observation $\Delta\theta[k]$, we have

$$\Delta\theta[k] \approx M_0\Delta P[k] \tag{3.9}$$

where $M_0 = H_0^{-1}$. Hence, under normal operation of the system, that is, prior to the line-outage event, $\Delta\theta[k] \sim f_0$, where

$$f_0 = \mathcal{N}(0, M_0\Sigma M_0^T). \tag{3.10}$$

Suppose a persistent outage occurs in line (m, n) at time $t = t_f$, where $(\gamma - 1)\Delta t \leq t_f < \gamma\Delta t$, for some $\gamma > 0$. In the event of outage, for $k \geq \gamma$, the matrix H_0 in (3.8) changes to $H_{(m,n)} = H_0 + \Delta H_{(m,n)}$, where $\Delta H_{(m,n)}$ is a perturbation matrix. Then the post-outage approximate power flow equation becomes

$$\Delta P[k] \approx H_{(m,n)}\Delta\theta[k] \tag{3.11}$$

and correspondingly

$$\Delta\theta[k] \approx M_{(m,n)}\Delta P[k] \tag{3.12}$$

where $M_{(m,n)} = H_{(m,n)}^{-1}$. Since H_0 has the same sparsity structure as the graph Laplacian of the network, the only non-zero terms in the matrix $\Delta H_{(m,n)}$ are $\Delta H_{(m,n)}[n,n] = -1/X_{(m,n)}$, $\Delta H_{(m,n)}[m,m] = -1/X_{(m,n)}$ and $\Delta H_{(m,n)}[m,n] = 1/X_{(m,n)}$. Thus, after the outage of the line (m,n), $\Delta\theta[k] \sim f^{\sigma}_{(m,n)}$, where

$$f^{\sigma}_{(m,n)} = \mathcal{N}(0, M_{(m,n)}\Sigma M^{T}_{(m,n)}). \tag{3.13}$$

for $k > \gamma$. It is assumed that the outaged line is not restored until a change is detected, that is, the change is persistent.

The goal of detecting line-outage has now became the problem of detecting the change in the probability distribution of the sequence $\{\Delta\theta[k]\}_{k\geq 1}$ as quickly as possible, while maintaining a certain level of detection accuracy, usually the probability of false alarm. Since it is assumed that the pre- and post-outage probability distribution functions f_0 and $f^{\sigma}_{(m,n)}$ are known, the popular Cumulative Sum (CuSum) algorithm can be used. In CuSum algorithm, a sequence of statistics is computed as

$$W_{(m,n)}[k+1] = \left(W_{(m,n)}[k] + \log \frac{f^{\sigma}_{(m,n)}(\Delta\theta[k])}{f_0(\Delta\theta[k])} \right)^{+} \tag{3.14}$$

where $W_{(m,n)}[0] = 0$ and the plus sign defined as $(x)^{+} = x$ if $x \geq 0$, otherwise $(x)^{+} = 0$. The CuSum algorithm hence declares a line outage in line (m,n) when the $W_{(m,n)}[k]$ computed for each line crosses a predetermined threshold A. The threshold A is adjusted according to the false alarm rate.
Denoting τ_C as the time at which the CuSum algorithm declares the line outage, we have

$$\tau_C = \inf\{k \geq 1 : W_{(m,n)}[k] > A\} \tag{3.15}$$

Since there are $L = 6$ buses, the line outage time is decided by choosing a time τ_{max}, at which the maximum of the L values of $W_{(m,n)}[k]$ crosses the threshold A. The relationship between A and the false alarm rate β is already established as $A = \log(L\beta)$ in [13]. Algorithms involving hypothesis testing rely on keeping the false alarm rate constant, which, in this case, is equivalent to keeping the quantity A constant. However, fixing the exact values of β is a matter of experience which falls in the hands of design engineers.

3.2.2 Other Statistical Algorithms for Change Detection

In the following section, two other statistical algorithms for change detection are described. They are explained as follows:

1. Meanshift test: Meanshift test is also known as one shot detection test wherein the distribution of the observations at a change point and before the change point is compared to detect the outage of line. Thus the algorithm detects a meanshift that occurs during the outage of a line ℓ between bus m and n using the test statistic:

$$W_{\ell}^{\mu}[k] = \log \frac{f_{\ell}^{CP}(\Delta\hat{\theta}[k])}{f_0(\Delta\hat{\theta}[k])} \tag{3.16}$$

   where $f_{\ell}^{CP}(\cdot)$ denote the distribution at the change point. The decision maker declares an outage when the test statistic of any of the L lines crosses their corresponding threshold A_{ℓ}. Thus the stopping time can be formally described as

$$\tau^{\mu} = \min_{\ell \in L} \left\{ \inf\{k \geq 1 : W_{\ell}^{\mu}[k] > A_{\ell}\} \right\}. \tag{3.17}$$

2. Shewhart test: In QCD theory, Shewhart test is popularly used to perform change detection due to the easiness of implementation. A mild extension of Shewhart test for QCD in line outage system is proposed in [14], where the mean-shift and transient phenomenon is incorporated to the classical log-likelihood ratio between persistent post outage an pre-outage distributions. The statistic for outage of line ℓ is

$$W_{\ell}^{Sh}[k] = \max_{i \in \{0,1,\ldots,T\}} \left\{ \log \frac{f_{\ell}^{i}(\Delta\hat{\theta}[k])}{f_0(\Delta\hat{\theta}[k])} \right\} \tag{3.18}$$

   where i indexes each of the T transient response periods. The stopping time for Shewhart's test is defined as

$$\tau^{sh} = \min_{\ell \in L} \left\{ \inf\{k \geq 1 : W_{\ell}^{sh}[k] > A_{\ell}\} \right\}. \tag{3.19}$$

3.2.3 QCD Implementation in WECC Three-Machine Nine Bus System

The PMU placement for a WECC three-machine nine-bus system is shown in Fig. 3.8, with the PMUs placed in Buses 4, 5, 6, 7, 8 and 9. For the topology shown here, H_0 matrix is of order 6×6. By construction, H_0 matrix is a sparse matrix whose non-zero entries are calculated from reactance values of the line between buses. Figure 3.9 shows results of the case study. A 3-phase line to ground fault is simulated on the

line between Bus 4 and Bus 5. The event starts at 0.4 s, with a fault duration chosen as 0.45 s and the Fig. 3.9 shows 1 s of system operation. The sequence of statistics $W_{(m,n)}$ from (3.14) is calculated using the real-time in-feed measurement data from SMT system. For the present study we have only considered the use of phase angle measurement values for calculation of sequence of the statistics. It can be noticed from Fig. 3.9 that with the chosen $A = 5000$ value the fault can be detected in a few milliseconds. This method was implemented as an algorithm and tested for different types of faults between the buses and scenarios of line outages, it was observed that by the proper selection of the threshold value A each fault can be differentiated and detected in very short time scales.

The algorithms, such as the one presented in this section, can be used to process synchro-measurements quickly, improving grid awareness to common equipment failures and faults, and enabling predictive response actions. In the next section, we look at the methodology for improving grid preparedness to cyber-attacks.

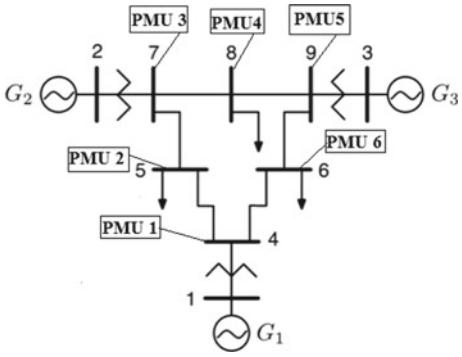

Fig. 3.8 PMU placement in WECC three-machine 9 bus system

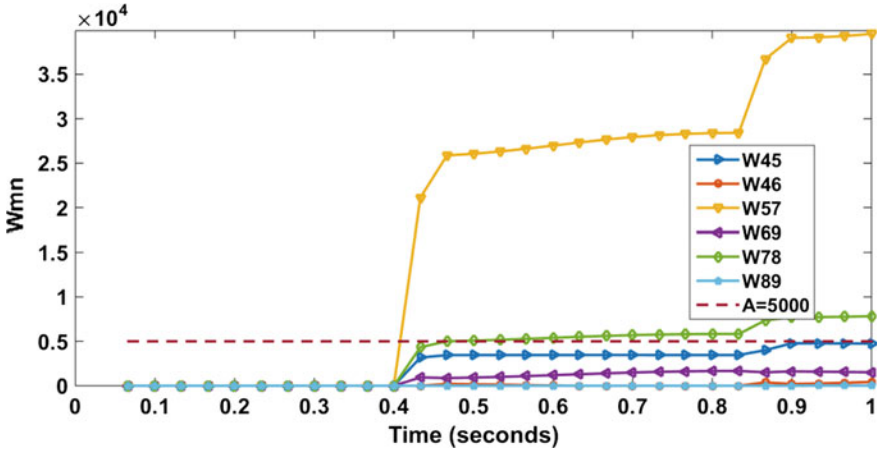

Fig. 3.9 Sequence of statistics calculation for the outage of line 57

3.3 Vulnerability Assessment in Smart Grids Under Cyber-Attacks

The monitoring systems in power grids, e.g. SCADA and WAMPAC, depend heavily on proper operation of ICT infrastructure as the measurement data gets transported through the communication network to utility control center. However, cyber security vulnerabilities within the ICT infrastructures may allow attackers to manipulate SCADA and WAMPAC systems [15, 16]. Attackers can perform data integrity attacks by exploiting software vulnerabilities to inject false data on cyber components. System resources can also be rendered unavailable through denial of service (DoS) attacks by congesting the network. What makes things worse is that attackers can perform data integrity attacks and availability attacks in a coordinated way, i.e., combined data attacks. Combined data attacks expand the attack scenarios against power grids and even can bypass mitigation schemes for pure integrity or availability attacks [17].

Cyber-attacks on wide area monitoring systems would have great impact on power system reliability. Table 3.1, based on [18], lists typical data attacks and their impacts on several important applications like State Estimation (SE), Automatic Generation Control (AGC) and Special Protection Schemes (SPS). For instance, data attacks on SE could be achieved by compromising SCADA status and power flow measurements. Such attacks can result in a poor situation awareness of the power system and also lead to incorrect system operation leading in line overloads and market impacts in terms of uneconomical generation. Similarly, combined data attacks on AGC and SPS would impact the operational reliability and even cause cascading outages.

In order to increase the security of these systems, one needs analytic methods to first understand the vulnerabilities and then to validate or explore them with appropriate tools. However, analytic methods may have to ignore some details when modeling the heterogeneous intelligent power system, but could be used to create attack scenarios and guide the cyber security experiments on testbeds/tools. Thus, tools that integrate different cyber and physical components are needed to support the design and evaluation of cyber security issues of intelligent power system, from vulnerability analysis to attack impact assessment with empirical results. It should be noted that vulnerability and impact of attacks can be combined together in the notion of *risk*. Risk analysis methods and tools combining vulnerability and impact assessment for data attacks are needed to implement risk assessment methodologies [19]. In addition, the combination of analytic methods and numerical simulation could also contribute to develop mitigation schemes, e.g., a more robust algorithms/methods that combine system-theoretic and ICT-specific measures can be proposed to protect SCADA and WAMPAC against data attacks [20].

Table 3.1 Data attacks targeting electricity grid monitoring system (based on [18])

Attacks	Specific types	Access	Attack targets	Affected applications	Coordination	Possible impact
Integrity attack, availability attack, combined attack	Man-in-the-middle attack, buffer overflow attack, DDoS flooding attack	Via SCADA network, RTU	SCADA status and power flow measurements	State estimation	Space, same time	Line overloads, poor situation awareness, economic loss
		Via SCADA network, RTU	Frequency, tie-line flow measurements	Automatic generation control	Space, same time	Frequency imbalance, operational reliability
		Via WAMPAC network, PMU	PMU measurements	Special protection schemes	Space, staggered time	Operational reliability, blackout or even cascading outages

3.3.1 Analytic Vulnerability Assessment

3.3.1.1 Data Attacks and Vulnerability Assessment Problem

Vulnerability of intelligent power system to data attacks is usually quantified by computing attack resources needed by the attacker to corrupt the system and keep undetectability. The vulnerability assessment is presented through the notion of *security index*. This metric can quantify the attack resources and consequently the vulnerabilities of the system to attacks. The intelligent power grid is more vulnerable to attacks with small security metric since such attacks need less resources to be executed.

We take data attacks on SE as an example. The data collected from substations includes line power flow and bus power injection measurements. These m measurements are denoted by $z = [z_1, \ldots, z_m]^T$. We assume that a power system has $n + 1$ buses, and that there are n phase angles to be estimated excluding the reference angle under the DC power flow model, i.e., the system state $z = [x_1, \ldots, x_n]^T$. We can write $z = Hx + e$, where $H \in \mathbb{R}^{m \times n}$ is the constant Jacobian matrix and $e \in \mathbb{R}^m$ is the measurement noise vector. With the goal of perturbing the SE and further corrupting the applications in EMS, the attacker would gain access to the measurement data. The measurements under different attack scenarios from the view of SE can be presented as follows:

- Data integrity attack - also known as false data injection (FDI) attack, is able to change measurement values from z to $z + a$ where a is the *FDI attack vector*.

- Data availability attack - includes DoS or jamming attack which would make specific measurements unavailable to SE, i.e., $z_0 = (I - \text{diag}(d))z$ where $d \in \{0, 1\}^m$ is the *availability attack vector* and I is an identity matrix.
- Combined attack - combines the FDI and availability attack that makes the measurements from z to $(I - \text{diag}(d))z + a$ corrupted by a and d.

To formulate the security index, optimization problems with the objective specified as security index and constraints corresponding to the undetectability or impact conditions are proposed to characterize attacks with different attack vectors. Looking at the attack scenarios above, if the attacker corrupts certain measurements using FDI attack vector $a = Hc$, it can remain hidden from being detected by some built-in bad data detection schemes but perturb the current state to a degree of c. It's also shown in our recent work [17] that combined attacks can achieve the same target with the attack vector $a = (I - \text{diag}(d))Hc$. An illustrative security index can be introduced as the minimum number of measurements that need to be corrupted by the attacker, with the objective $\alpha_j := \min_{a,d} \quad \|a\|_0 + \|d\|_0$ and constraints corresponding to the undetectability conditions for attack vectors.

3.3.1.2 Analytic Vulnerability Assessment Incorporating Communication Network Properties

The vulnerability assessment problem above shows the measurements/sensors that need to be manipulated by the attacker. This security metric suits for the cases that attacks arise from the level of sensors. A more interesting scenario is to look into the attacks from the level of communication networks since usually the attacker would explore vulnerabilities in the networks, e.g., compromising remote access points, obtaining access to corporate networks. The vulnerability assessment should consider the communication network. However, modeling the communication network in an analytic framework is challenging due to its complexity and heterogeneity. Here, the communication network properties of interest for security analysis are as follows:

- Communication topology;
- Routing schemes - the routing paths of packets / data;
- Communication latency - how the packets / data would be delayed in each communication infrastructure;
- Packet loss / missing data - the possibility of packet drop in each communication infrastructure.

In [17, 21] we introduced a method to deal with the first two properties that can be employed in the analytic vulnerability assessment. We introduced a binary vector called *routing vector* which denotes the communication nodes/links that each measurement traverses. Using the graph of the communication network and routing schemes for all the measurements, we can build a *routing matrix* stacked by the routing vectors. The routing matrix contains the information of communication topology and routing schemes. The network-aware security index can be introduced

as the minimum number of communication nodes/links that need to be attacked and the constraints use the *routing vectors* to map the data attacks on measurements to attacks on the communication network. Thus the security index can illustrate the vulnerability of SE to data attacks on the communication network.

It should be noted that some ICT-specific security measures can be modeled in such security index problem. For instance, multi-path routing schemes can be described using *routing vectors*. Data authentication can be implemented by adding constraints to indicate measurements that originate from the node protected by authentication. More cyber properties of communication networks, latency and packet loss, can also be considered as the factors that impact the construction of the security index problem.

These security indexes from the analytic vulnerability assessment specify the measurements/communication infrastructures to be attacked, thus could be used to create attack scenarios for simulation. However, such security index do not consider the attack impact on the physical system operation. In fact, data attacks with the same security metrics could have considerable different impact. Co-simulation could offer the capabilities to look into the attack impact and provide empirical results to validate and contribute in developing mitigation measures.

3.3.2 Co-simulation Supporting Vulnerability and Impact Analysis

3.3.2.1 Co-simulation Framework for Risk Assessment

In our papers [22, 23], we discussed co-simulation of intelligent power grids and its potential applications for cyber security analysis. A co-simulation framework is an integrated environment including simulators of power system, communication network and EMS applications. Under the co-simulation, the communication model can be implemented as a hierarchical one that is close to reality. From co-simulation, the attack scenarios from the analytic vulnerability assessment can be validated and the attack impact can be explored from simulation results. The risk of system to data attacks can be assessed incorporating both vulnerability and attack impact.

The co-simulation framework is shown in Fig. 3.10 and is implemented on top of the integration of power system, communication network and control/application simulators. This platform should: (1) be modular, extensible and flexible to simulate communication networks; (2) allow implementation of attacks and mitigation schemes.

3.3.2.2 Co-simulation Setup: Tools, Integration and Attacks Modeling

Here we present our co-simulation platform as shown in Fig. 3.11 and further details are referred to [21]. This co-simulation platform is implemented with three tools: DIgSILENT PowerFactory for the power system, OMNeT++ for the communication network, and Matlab/Matpower for the EMS algorithms. OMNeT++ is selected because it is a generic simulation engine, open source and it allows plug-n-play through NED editor and integration to external devices. The *scheduler* of OMNeT++ is customized as the master algorithm and external interface for integration with PowerFactory and Matlab/Matpower (Fig. 3.11).

1. Power system simulator: DIgSILENT PowerFactory is used to conduct a quasi-static power flow simulation. PowerFactory's Python API is used to create a script that controls the execution of the simulation. The same script implements the interface with OMNeT++. Real time execution is achieved by synchronizing the power flow calculations with the system clock. The script sends measurements to OMNeT++ every time period (set to be 5 s), but it can expect generator set points at any time.
2. Communication network simulator: OMNeT++ is used for discrete-event based communication network simulation. A custom OMNeT++ *scheduler* is built to enable data exchange with PowerFactory and Matlab over TCP/IP sockets and run the OMNeT++ in real-time. The communication nodes such as RTUs, modems and routers are built using the modules in OMNeT++ represent the LAN (local area network) of a substation. Besides, there are two kinds of communication links/channels: (1) channel of the LAN between RTUs and modems; (2) channel of the WAN (wide area network) between routers.

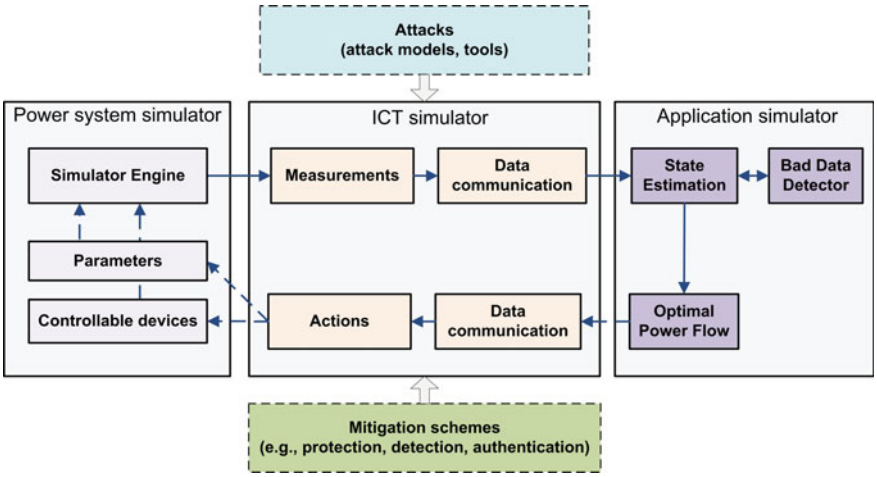

Fig. 3.10 Co-simulation based cyber security risk assessment framework

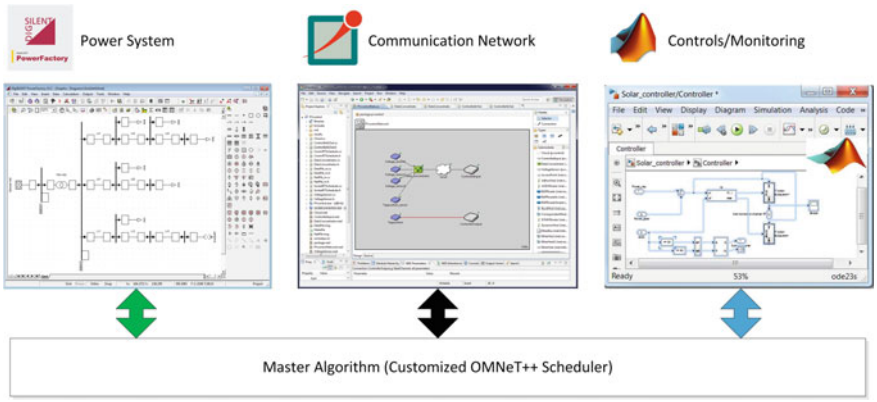

Fig. 3.11 A co-simulation platform setup

3. EMS algorithm: Matpower has been used to simulate the EMS applications in Matlab, including state estimation (with bad data detection) and optimal power flow algorithms. A script is implemented to exchange data with OMNeT++ scheduler over TCP/IP sockets and store measurements into a data pool. The State Estimation module uses the latest measurements from data pool to create a snapshot of estimated power flow. The Optimal Power Flow module uses load estimates from State Estimation to perform optimal power flow calculation and sends commands of generator set points to PowerFactory through OMNeT++.

The integration of simulators is implemented as follows: data is exchanged between PowerFactory, OMNeT++ and Matlab via TCP/IP sockets using the ASN.1 protocol. On the PowerFactory side, data exchange is implemented in the Python script that controls the simulator execution, while on the OMNeT++ side, data exchange is implemented through a custom scheduler. This scheduler acts as the "master" to coordinate the co-simulation, handle the data exchanges with PowerFactory and Matlab, and also run the OMNeT++ in a real-time mode.

As discussed in the previous section, an attacker can manipulate the measurements by injecting false data, making it unavailable or both. After accessing a router, the attacker can launch data integrity and availability attacks on all the data traveling through it by executing a *man-in-the-middle attack*. By jamming, DoS or physical attack, the attacker can block measurements in communication links. The attack scenarios from the analytic vulnerability assessment can be conducted. The results from network-aware security index problem is used to choose the routers to be attacked. This attack is implemented in OMNeT++ by changing the behavior of the router in case it is accessed by the attacker.

It should be noted that these types of attacks can be modeled based on some attack "libraries". For instance, the NETA framework [24] can be used and further developed to add attack modules in the simulation model. Moreover, attacks like Man-in-the-middle attack, DDoS flooding attack, can be implemented by using

available tools (e.g., Ettercap suite, Tribe Flood Network tool) and integrating them into the co-simulation. Besides, the mitigation schemes for attacks, e.g., protection and authentication, can also be implemented by adding the configurations to the modules in OMNeT++.

References

1. Long Term Global Goals for 2050, Climate Action Network International, http://www.climatenetwork.org/sites/default/files/can_position-long_term_global_goals_for_2050.pdf. Accessed 4 June 2018
2. Final report of the investigation committee on the 28 September 2003 blackout in Italy, TUCE (2004)
3. U.S.-Canada Power System Outage Task Force, in *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* (Natural Resources Canada, 2004)
4. International Conference on Large High Voltage Electric Systems and Conférence Internationale des Grands Réseaux Electriques à Haute Tension. *Wide Area Monitoring and Control for Transmission Capability Enhancement* (Cigré, 2007)
5. V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M.M. Begovic, A. Phadke, Wide-area monitoring, protection, and control of future electric power networks. Proc. IEEE **99**(1), 80–93 (2011)
6. F. Aminifar, M. Fotuhi-Firuzabad, A. Safdarian, A. Davoudi, M. Shahidehpour, Synchrophasor measurement technology in power systems: Panorama and state-of-the-art. IEEE Access **2**, 1607–1628 (2014)
7. G.A. Phadke, J.S. Thorp, Synchronized Phasor Measurements and Their Applications (Springer International Publishing, Berlin, 2017)
8. M. Naglic, M. Popov, M.A.M.M. Meijden, V. Terzija, Synchro-measurement application development framework: an IEEE standard C37.118.2-2011 supported MATLAB library. IEEE Trans. Instrum. Meas. 1–11 (2018)
9. M. Naglic, I. Tyuryukanov, M. Popov, M. van der Meijden, V. Terzija, WAMPAC-ready platform for online evaluation of corrective control algorithms, in *Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion (MedPower 2016)* (Institution of Engineering and Technology, 2016)
10. IEEE, *Std C37.118.1-2011 (Revision of IEEE Std. C37.118-2005): IEEE Standard for Synchrophasor Measurements for Power Systems* (IEEE, 2011)
11. IEEE, *Std. C37.118.1a, IEEE Standard for Synchrophasor Measurements for Power Systems - Amendment 1: Modification of Selected Performance Requirements* (IEEE, 2014)
12. Matlab Central
13. Y.C. Chen, T. Banerjee, A.D. Domínguez-García, V.V. Veeravalli, Quickest line outage detection and identification. IEEE Trans. Power Syst. **31**(1), 749–758 (2016)
14. G. Rovatsos, X. Jiang, A.D. Domínguez-García, V.V. Veeravalli, Comparison of statistical algorithms for power system line outage detection in 2016, in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (2016), pp. 2946–2950
15. T.M. Thomas, S. Abu-Nimeh, Lessons from stuxnet. Computer **44**(4), 91–93 (2011)
16. A. Hahn, A. Ashok, S. Sridhar, M. Govindarasu, Cyber-physical security testbeds: architecture, application, and evaluation for smart grid. IEEE Trans. Smart Grid **4**(2), 847–855 (2013)
17. K. Pan, A.M.H. Teixeira, M. Cvetkovic, P. Palensky, Combined data integrity and availability attacks on state estimation in cyber-physical power grids, in *Proceedings of the IEEE International Conference on Smart Grid, Communications (SmartGridComm)* (2016), pp. 271–277
18. A. Ashok, A. Hahn, M. Govindarasu, Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. J. Adv. Res. **5**(4), 481–489 (2014)

19. K. Pan, A. Teixeira, M. Cvetkovic, P. Palensky, Cyber risk analysis of combined data attacks against power system state estimation. IEEE Trans. Smart Grid. https://doi.org/10.1109/TSG.2018.2817387
20. M. Findrik, P. Smith, J.H. Kazmi, M. Faschang, F. Kupzog, Towards secure and resilient networked power distribution grids: process and tool adoption, in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 435–440, 2016
21. K. Pan, A. Teixeira, C.D. López, P. Palensky, Co-simulation for cyber security analysis: data attacks against energy management system, in *Accepted in 8th IEEE International Conference on Smart Grid Communications (SmartGridComm)* (2017)
22. P. Palensky, A.A. Van Der Meer, C.D. López, A. Joseph, K. Pan, Cosimulation of intelligent power systems: fundamentals, software architecture, numerics, and coupling. IEEE Indust. Electron. Mag. **11**(1), 34–50 (2017)
23. P. Palensky, A. van der Meer, C. Lopez, A. Joseph, K. Pan, Applied cosimulation of intelligent power systems: implementing hybrid simulators for complex power systems. IEEE Indust. Electron. Mag. **11**(2), 6–21 (2017)
24. L. Sánchez-Casado, R.A. Rodríguez-Gómez, R. Magán-Carrión, G. Maciá-Fernández, Neta: evaluating the effects of network attacks. Manets as a case study, in *Advances in Security of Information and Communication Networks* (Springer, 2013), pp. 1–10