1

Introduction: The Role of Wide Area Monitoring Systems in Dynamic Vulnerability Assessment

Jaime C. Cepeda¹ and José Luis Rueda-Torres²

¹ Head of Research and Development and University Professor, Technical Development Department and Electrical Energy Department, Operador Nacional de Electricidad CENACE, and Escuela Politécnica Nacional EPN, Quito Ecuador
² Assistant professor of Intelligent Electrical Power Systems, Department of Electrical Sustainable Energy, Delft University of Technology, The Netherlands

1.1 Introduction

Currently, most social, political, and economic activities depend on the reliability of several energy infrastructures. This fact has established the necessity of improving the security and robustness of Electric Power Systems [1]. In addition, the lack of investment, the use of congested transmission lines, and other technical reasons, such as environmental constraints, have been pushing Bulk Power Systems dangerously close to their physical limits [2]. Under these conditions, certain sudden perturbations can cause cascading events that may lead to system blackouts [1, 3]. It is crucial to ensure that these perturbations do not affect security, so the development of protection systems that guarantee service continuity is required. In this regard, Special Protection Schemes (SPS) are designed in order to detect abnormal conditions and carry out corrective actions that mitigate possible consequences and allow an acceptable system performance [4].

However, the conditions that lead the system to a blackout are not easy to identify because the process of system collapse depends on multiple interactions [5, 6]. Vulnerability assessment (VA) is carried out by checking the system performance under the severest contingencies with the purpose of detecting the conditions that might initiate cascading failures and may provoke system collapse [7]. A vulnerable system is a system that operates with a “reduced level of security that renders it vulnerable to the cumulative effects of a series of moderate disturbances” [7]. The concept of vulnerability involves a system’s security level (static and dynamic security) and the tendency of its conditions changing to a critical state [8] that is called the “Verge of Collapse State” [5]. In this context, vulnerability assessment assumes the function of detecting the necessity of performing global control actions (e.g., triggering of SPSs).

In recent years, emerging technologies such as Phasor Measurement Units (PMUs), which provide voltage and current phasor measurements with updating periods of a few milliseconds, have allowed the development of modern approaches that come closer to the target of real time vulnerability assessment [6, 7]. Most of these real time applications have been focused on identifying signals that suggest a possibly insecure steady state.
This kind of VA is capable of alerting the operator to take appropriate countermeasures, with the goal of bringing the system to a more secure operating condition (i.e., preventive control) [9]. Nevertheless, the use of PMUs has great potential to allow the performance of post-contingency Dynamic Vulnerability Assessment (DVA) that could be used to trigger SPSs in order to implement corrective control actions. In this connection, a Wide Area Monitoring System (WAMS), based on synchrophasor technology, constitutes the basic infrastructure for implementing a comprehensive scheme for carrying out real time DVA and afterwards executing real time protection and control actions. This comprehensive scheme is called a Wide Area Monitoring, Protection, and Control system (WAMPAC) [10]. This chapter presents a general overview of concepts related to power system vulnerability assessment and phasor measurement technology and subsequently highlights the fundamental relationship between these in modern control centers.

1.2 Power System Vulnerability

A vulnerable system is a system that operates with a “reduced level of security that renders it vulnerable to the cumulative effects of a series of moderate disturbances.” Vulnerability is a measure of system weakness regarding the occurrence of cascading events [7].

The concept of vulnerability involves a system’s security level (i.e., static and dynamic security) and its tendency to change its conditions to a critical state [8] that is called the “Verge of Collapse State” [5].

A vulnerable area is a specific section of the system where vulnerability begins to develop. The occurrence of an abnormal contingency in vulnerable areas and a highly stressed operating condition define a system in the verge of collapse state [5].

In this chapter, vulnerability is defined as “the risk level presented by a power system during a specific static or dynamic operating condition regarding the occurrence of cascading events.” This concept makes vulnerability an essential indicator of system collapse proximity.

Although there are a lot of vulnerability causes, which vary from natural disasters to human failures, system vulnerability is characterized by four different symptoms of system stress: angle instability, voltage instability, frequency instability, and overloads [5]. So, vulnerability assessment should be performed through analyzing the system status as regards these symptoms of system stress.

1.2.1 Vulnerability Assessment

Vulnerability assessment has the objective of preventing the occurrence of collapses due to catastrophic perturbations [11]. Performing VA requires specific mathematical models capable of analyzing the multiple interactions taking place between the different power system components [11]. These models have to consider the varied phenomena involved in the vulnerability condition and also the diverse timeframes in which the corresponding phenomena occur.

Many methods have been proposed for vulnerability assessment, which have been classified based on various criteria [6, 7]. However, in terms of their potential implementation in control centers, the techniques to assess vulnerability can be classified into
off-line, on-line, and real time methods. Figure 1.1 depicts the proposed classification of vulnerability assessment methods.

- **Off-line assessment:** Off-line assessment is done using conventional methods that are based on different complex model simulations; these usually involve time-consuming tasks, which restricts on-line applications. The high complexity is provoked by the huge number and diversity of the components that constitute an electric power system and their particular performance during dynamic phenomena. Among this class of methods are those that assess vulnerability via power flow computations. These approaches are based on the hypothesis that a typical contingency provokes minor changes in the Bulk Power Systems, so they migrate from one quasi-steady state to another. The simulations do not include any dynamic response analysis [7]. This type of evaluation is commonly called Static Security Assessment (SSA). As a complement of SSA, dynamic simulation is commonly used in order to consider all the static and dynamic power system components, simulating any type of contingency and any type of instability [9, 12]. In this case, the complexity of the modeling and mathematical computations demands high processing time [7, 9]. This evaluation is usually called Dynamic Security Assessment (DSA). Usually, both in SSA and DSA, several “what-if” contingencies are simulated in order to determine the most critical disturbances (i.e., N-x contingency analysis) [9].

- **On-line assessment:** In an on-line assessment, the information must be available in the SCADA/EMS (Supervisory Control and Data Acquisition/Energy Management System). The input data are updated using adequate tools and equipment (e.g., IEDs, PMUs, WAMS), but the output is not necessarily obtained as quickly as the real time events occur [12].

- **Real time assessment:** The input data reflect the most recent picture of the system conditions in a real time analysis, and the entire process is performed within very short time, typically not exceeding a couple of seconds [12]. Emerging technologies, such
as Phasor Measurement Units (PMUs), have allowed the development of modern approaches to vulnerability assessment [7, 12] capable of being updated practically in real time. Additionally, some novel mathematical methods permit processing the data obtained in real time through identification of indicators or patterns that show system vulnerability, using artificial intelligence (AI) or modern data mining techniques [7]. Tools based on AI allow the analysis of power system dynamic performance patterns in real time, using the knowledge obtained from off-line learning [7]. On the other hand, data mining techniques permit uncovering valuable hidden information immersed in the electric signals [7], which can exhibit certain regularities (patterns) signaling a possibly vulnerable condition [10, 13]. VA methods based on AI and data mining are oriented to evaluate both pre-contingency quasi-steady state data (i.e., real time DSA for coordinate preventive control actions) as well as post-contingency dynamic data (i.e., post-contingency Dynamic Vulnerability Assessment—DVA—for triggering corrective control actions). In the particular case of post-contingency DVA, it is noteworthy that PMUs are able to provide time-synchronized phasor data, which contain valuable dynamic information that could indicate system vulnerability status and potential collapses [7]. These post-contingency data offer a new framework for system vulnerability assessment that is known as Dynamic Vulnerability Assessment (DVA), which is oriented to coordinating corrective control actions. In this connection, post-contingency DVA requires even a quicker response than pre-contingency DSA, so that AI and data mining techniques are, possibly, the most prominent mathematical tools to be applied for accomplishing this type of real time assessment.

1.2.2 Timescale of Power System Actions and Operations

As mentioned, an important aspect to be considered in vulnerability assessment is the duration of the events involved in the VA timeframe of interest. Due to the complex tasks related to power system operation, which comprise modeling, analysis, simulation, and control actions, the timescale varies from microseconds to several hours [1]. Table 1.1 presents some power system actions and operations and their corresponding timeframes. Most of this book tackles the Dynamic Vulnerability

<table>
<thead>
<tr>
<th>Action or operation</th>
<th>Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electromagnetic transients</td>
<td>μs – ms</td>
</tr>
<tr>
<td>Switching overvoltage</td>
<td>Ms</td>
</tr>
<tr>
<td>Fault protection</td>
<td>100 ms</td>
</tr>
<tr>
<td>Electromagnetic effects in machine windings</td>
<td>ms – s</td>
</tr>
<tr>
<td>Electromechanical transients – stability</td>
<td>ms – s</td>
</tr>
<tr>
<td>Electromechanical oscillations</td>
<td>ms – min</td>
</tr>
<tr>
<td>Frequency control</td>
<td>1 s – 10 s</td>
</tr>
<tr>
<td>Overloads</td>
<td>5 s – h</td>
</tr>
<tr>
<td>Economic load dispatch</td>
<td>10 s – 1 h</td>
</tr>
<tr>
<td>Thermodynamic effects</td>
<td>s – h</td>
</tr>
<tr>
<td>Energy Management System applications</td>
<td>Steady state; ongoing</td>
</tr>
</tbody>
</table>

Table 1.1 Actions and operations within the power system [1].
Assessment (DVA) problem, focusing on post-contingency short-term phenomena, which develop in a timeframe of 15 to 20 seconds after a contingency occurs. This time window includes so-called short-term stability phenomena, which comprise transient stability, short-term voltage stability, oscillatory stability, and short-term frequency stability; and also, the possible overloads provoked by a change of system topology (these are the power system symptoms of stress).

Cascading events are the mechanism whereby failures propagate within a power system, thus leading the system to a possible collapse [14]. These events are usually caused by the conventional system protection schemes triggering in response to one or more symptoms of stress. These phenomena typically occur within timeframes between some milliseconds and several seconds, which means that a complete cascading event usually takes place in timescales from seconds up to hours. Therefore, the DVA timeframe definition specified in most of this book (i.e., 15 s to 20 s) matches the period in which an N-1 critical contingency might drive the system to further undesirable events (i.e., N-2 contingencies), which could be considered as the beginning of a cascading event.

A summary of some of the major blackouts registered in the last years is presented in Table 1.2. Several of the vulnerability assessment methodologies that will be presented in this book take a supervisory role whose response should be in the order of a few milliseconds to a few seconds. The use of monitoring methods such as the ones presented in this book, being capable of predicting the risk of initiating cascading events and whose response is in the order of seconds, might prevent the future occurrence of collapses such as those depicted in Table 1.2, whose total evolution is in the order of seconds to minutes.

### 1.3 Power System Vulnerability Symptoms

System vulnerability is characterized by four different symptoms of system stress, namely angle instability, voltage instability, frequency instability, and overloads [5].

Thus, most of the phenomena tackled throughout this book, based on the previously defined VA timeframe, comprise four short-term stability phenomena and post-contingency overloads. These phenomena include: transient stability, oscillatory stability, short-term voltage stability, short-term frequency stability, and post-contingency overloads initiated by topological modifications and power injection changes that follow an N-1 contingency.
1.3.1 Rotor Angle Stability

Rotor angle stability refers to the ability of synchronous machines of an interconnected power system to remain in synchronism after being subjected to a disturbance [17].

This type of stability depends on the ability to maintain or restore equilibrium between electromagnetic torque and mechanical torque of each synchronous machine in the system [17]. The electromagnetic torque of a synchronous machine, after a perturbation, can be resolved into two components: the “synchronizing torque” (in phase with rotor angle deviation—$\Delta \delta$), and the “damping torque” (in phase with the speed deviation—$\Delta \omega$), as shown by (1.1) [18].

$$\Delta T_e = T_S \Delta \delta + T_D \Delta \omega \quad (1.1)$$

where $T_S \Delta \delta$ is the synchronizing torque, $T_S$ being the synchronizing torque coefficient, and $T_D \Delta \omega$ is the damping torque, $T_D$ being the damping torque coefficient.

Instability in power systems is the result of a lack of one or both torque components: lack of sufficient synchronizing torque results in aperiodic or non-oscillatory instability (which characterizes transient stability phenomenon), whereas lack of damping torque results in oscillatory instability [17].

1.3.1.1 Transient Stability

Transient stability (TS) is a type of rotor angle stability that occurs when the system is subjected to a severe disturbance (e.g., a short circuit on a transmission line). The time-frame of interest in this phenomenon is usually 3–5 seconds following the disturbance [17]. This type of instability is usually characterized by a lack of synchronizing torque.

1.3.1.2 Oscillatory Stability

The rotor angle stability problem involves the study of the electromechanical oscillations inherent in power systems. Oscillatory instability occurs when there is lack of damping torque [17].

Oscillation problems may be either local or global in nature [18]. Local problems (local mode oscillations) are associated with oscillations among the rotors of a few generators close to each other. These oscillations have frequencies in the range of 0.7 to 2.0 Hz. Global problems (inter-area mode oscillations) are caused by interactions among large groups of generators. These oscillations have frequencies in the range of 0.1 to 0.7 Hz [18].

There are other two types of oscillatory problems caused by controllers of different system components (control modes), or by the turbine-generator shaft system rotational components (torsional modes) [18]. These types of oscillations present a large associated range of frequencies.

Modal analysis [18] is the most commonly used tool to analyze oscillations in a power system. It consists on the determination of the oscillatory modes and the analysis of their corresponding complex modal frequencies (i.e., the mode eigenvalues: $\sigma_i \pm j\omega_i$). Oscillatory stability is satisfied when all the modes present a positive damping. The frequency and damping of the oscillation can be determined from the eigenvalue as follows:

$$f_i = \frac{\omega_i}{2\pi} \quad (1.2)$$
\[ \zeta_i = \frac{-\sigma_i}{\sqrt{\sigma_i^2 + \omega_i^2}} \]  

where \( f_i \) and \( \zeta_i \) are the oscillation frequency and the damping ratio of i-th mode, respectively.

### 1.3.2 Short-Term Voltage Stability

Voltage stability (VS) refers to the ability of a power system to maintain steady voltages at all buses in the system after being subjected to a disturbance. Short-term voltage stability involves the dynamics of fast acting load components such as induction motors, controlled loads, and HVDC converters. The timeframe of interest is in the order of several seconds. Load dynamic modeling is often essential. Short circuits near loads could cause relevant effects in this type of stability [17].

### 1.3.3 Short-Term Frequency Stability

Frequency stability (FS) refers to the ability of a power system to maintain a steady frequency following a severe system upset resulting in a significant imbalance between generation and load.

Short-term frequency instability is characterized by the formation of an under-generated area with insufficient under-frequency load shedding such that frequency decays rapidly causing the area blackout within a few seconds [17]. On the other hand, when a large amount of load is disconnected, an over-generated area might be formed. In these cases, over-frequency issues might provoke the uncontrolled outage of generation units.

### 1.3.4 Post-Contingency Overloads

Power flows through system branches can vary after a contingency because a disturbance modifies the grid topology. High electric currents can provoke overloads, and this could trigger protection systems that may separate elements from the system and increase the system vulnerability problem [9]. So, a system may be stable following a contingency, yet insecure due to post-fault system conditions resulting in equipment overloads [17].

In this book, the possible overloads that should be controlled within few seconds are tackled. This type of overload commonly corresponds to special series equipment which presents fast overload control requirements (e.g., electronic devices). On the other hand, equipment that presents slow overload control requirements (i.e., minutes or hours) would permit an on-line assessment via contingency analysis as part of SCADA/EMS applications. In these cases, a quick vulnerability assessment might not be required.

Power system series equipment presents different overload timeframes due to the variety of particular features such as physical limits, thermal capability, and stability constraints, among others. For instance, AC transmission line overload is usually specified by three types of limits: thermal, angle stability, and voltage, from which the temperature commonly does not rise so fast to reach the maximum designed limit. However, angle stability and voltage limits might be quickly reached after a contingency [19].
The physical limits present particular interest in some series electronic equipment because of the special care required for the semiconductor devices of the power converters of HVDCs, FACTS devices, and photovoltaic or wind facilities. In these types of equipment, a quick assessment of possible overloads has relevant importance [19].

1.4 Synchronized Phasor Measurement Technology

1.4.1 Phasor Representation of Sinusoids

A phasor or phase vector constitutes the most commonly applied analytic representation of steady state sinusoidal waveforms of fundamental power frequency. Phasors are used as the basic mathematical tool of AC circuit analysis [20].

A pure sinusoidal equation given by:

\[
x(t) = X_m \cos(\omega t + \phi)
\]

where \( \omega \) is the signal angular frequency in radians per second, \( \phi \) is the phase angle in radians, and \( X_m \) is the peak amplitude of the signal; this can also be written as (1.5) based on Euler’s formula [21].

\[
x(t) = \text{Re} \{ X_m e^{j(\omega t + \phi)} \} = \text{Re} \{ X_m e^{j\phi} [e^{j\omega t}] \}
\]

The factor \( e^{j\omega t} \) of (1.5) can be suppressed from this equation when considering that the frequency \( \omega \) is a constant parameter in steady state. Under this assumption, (1.5) can be simply represented by a complex number \( \vec{X} \) rotating at the angular speed \( \omega \), known as its phasor representation or simply phasor, as shown by (1.6) [21].

\[
x(t) \Leftrightarrow \vec{X} = \left( \frac{X_m}{\sqrt{2}} \right) e^{j\phi} = \left( \frac{X_m}{\sqrt{2}} \right) (\cos \phi + j \sin \phi)
\]

where \( X_m/\sqrt{2} \) is the RMS (root mean square) signal value. Figure 1.2 illustrates the phasor representation of a pure sinusoidal equation given by (1.4).

\[\text{(a)}\]

\[\text{(b)}\]
1.4.2 Synchronized Phasors

A *synchronized phasor* or *synchrophasor* is defined by [22] as “a phasor calculated from data samples using a standard time signal as the reference for the measurement.”

The synchronized phasors are angularly referenced to a cosine wave at nominal system frequency synchronized to Coordinated Universal Time (UTC, according to the French language). The phase angle $\phi$ is defined to be $0^\circ$ when the maximum of the function $x(t)$ (1.4) occurs at the UTC second rollover (1 pulse per second (PPS) time signal), and $-90^\circ$ when the positive zero crossing occurs at the UTC second rollover [22, 23]. This fact means that synchronized phasors from remote sites have a defined common phase relationship [22].

The synchronizing signal must have uninterrupted and continuous availability and it has to offer easy access to every place where the electrical variables are measured. Additionally, enough accuracy has to be guaranteed in order to accomplish the maximum error requirements (Total Vector Error (TVE)). Thus, the most used synchronizing source is the Global Positioning System (GPS) based on the 1-PPS synchronizing signal, with a maximum error of $1 \mu s$ [22].

The concept of TVE and related compliance tests are expanded in [23]. In addition, the definition of frequency and the rate of change of frequency error limits, for both steady state and dynamic conditions, is also considered in [23].

1.4.3 Phasor Measurement Units (PMUs)

*Phasor Measurement Units* are devices that allow estimation of the synchrophasors of AC voltage and current sinusoidal waves. In order to calculate a synchrophasor, a PMU needs to read the electrical wave $x(t)$ as well as a reference cosine wave synchronized to UTC.

For calculating a synchrophasor, a PMU uses a phasor estimation algorithm. These algorithms employ $N$ samples in a specific time period for carrying out the phasor estimation. The most commonly applied algorithm is the Discrete Fourier Transform (DFT) [21].

Their high accuracy and response speed and their time synchronization ability make PMUs appropriate for wide area monitoring in steady and dynamic states, as well as for control and protection applications [2]. Figure 1.3 schematizes the basic structure of a PMU.

![PMU basic structure](image.png)

**Figure 1.3** PMU basic structure [21].
1.4.4 Discrete Fourier Transform and Phasor Calculation

The DFT is a method for computing the Fourier transform $X(f)$ of a few samples belonging to a specific signal $x(t)$. In this case, the Fourier transform is calculated in discrete intervals in the frequency domain when the signal is sampled in discrete points in the time domain.

Consider a periodic function $x(t)$ with period $T_0$, and $N$ samples: $x(k\Delta T)$, $k = 0, 1, 2, \ldots, N-1$, where $\Delta T$ is the sampling interval; then $T_0 = N\Delta T$. Under these considerations, the Fourier transform $X(f)$ has only $N$ different values corresponding to the frequencies $f = n/T_0$, where $n$ is between 0 and $N/2$ (if $N$ is an even number). The following equation represents the DFT definition considering $N$ samples and $\Delta T$ sampling intervals [21].

$$X\left(\frac{n}{T_0}\right) = \sum_{k=0}^{N-1} x(k\Delta T)e^{-j\frac{2\pi kn}{N}}, \ n = 0, \pm 1, \pm 2, \ldots, \pm \frac{N}{2} \quad (1.7)$$

The DFT is a useful tool for Fourier series spectral analysis. The Fourier series coefficients of a periodic function can be computed from the DFT of the sampled data by dividing the DFT corresponding to the frequency of interest by $N$. Since each frequency always appears in two positions ($\pm n$), the coefficients of the Fourier series are:

$$c_n = \frac{2}{N} X\left(\frac{n}{T_0}\right) = \frac{2}{N} \sum_{k=0}^{N-1} x(k\Delta T)e^{-j\frac{2\pi kn}{N}}, \ n = 0, 1, 2, \ldots, \frac{N}{2} \quad (1.8)$$

Considering that a phasor represents a pure sinusoidal function, it is necessary to extract the fundamental frequency component $f_0$ (coefficient $c_1$ of the Fourier series) of the sampled signal [21]. Thus, the phasor representation is:

$$\overline{X} = \frac{c_1}{\sqrt{2}} = \frac{2}{N\sqrt{2}} X\left(\frac{1}{T_0}\right) = \frac{\sqrt{2}}{N} X(f_0) \quad (1.9)$$

$$\overline{X} = \frac{\sqrt{2}}{N} \sum_{k=0}^{N-1} x(k\Delta T)e^{-j\frac{2\pi k}{N}} \quad (1.10)$$

1.4.5 Wide Area Monitoring Systems

Wide area monitoring systems (WAMS) permit access to distributed phasor measurements throughout the network by means of adequately located PMUs. For this purpose, in addition to PMUs, advanced signal processing algorithms, specialized communication systems, and a real time dynamic infrastructure are required. This technology includes applications related to the real time supervision and control of electric power systems. WAMS are mainly composed of PMUs, Phasor Data Concentrators (PDCs), and communication systems [10, 24].

WAMS provide direct voltage and current phasor measurements with updating periods of few milliseconds, ideally avoiding the necessity for state estimators. The fast updating intervals also allow the monitoring of power system dynamic behavior and offer the possibility of detecting potential insecure conditions that might lead the systems to blackouts [12].
It is possible to distinguish three different applications for wide area measurement systems:

- Wide area monitoring systems (WAMS)
- Wide area control systems (WACS)
- Wide area protection systems (WAPS)

Several monitoring, control, and protection applications are depicted in Figure 1.4. These applications are ranked depending on different operational levels. It is possible to note that synchronized phasor measurement technology corresponds to the fourth operational level, which is established by the so-called *Wide area monitoring, protection, and control systems (WAMPAC)* [2].

The overall WAMPAC scheme comprises several interrelated stages, each one having embedded applications to perform different relevant tasks in order to achieve the objective of allowing a “self-healing grid,” as illustrated in Figure 1.5.

Measurements of the actual system condition from PMU/SCADA-EMS are used to perform the following applications:

i) Update of system behavior knowledge database (i.e., operational statistics) and execution of pattern recognition routines, which supports the Dynamic Security Assessment (DSA) and real time Dynamic Vulnerability Assessment (DVA) tasks.

ii) DSA in normal operating states to determine whether or not the system security level is to be degraded in future time when considering a selected set of credible contingencies.

iii) Real time DVA to determine the actual system security level as well as its tendency to change its conditions to a critical state in post-disturbance immediate time.

The information obtained from DSA and DVA is passed to the control center (for real time monitoring and decision making) and potentially directly to the control systems as well.

*Figure 1.4 Wide area monitoring, protection and control systems [2].*
Several chapters of this book focus on presenting methodologies capable of performing post-contingency real time DVA based on the development and application of pattern recognition expert systems in combination with the evaluation of various performance indices.

1.4.6 WAMPAC Communication Time Delay

In order to perform global control actions in a timely manner, the WAMPAC scheme must act prior to the tripping of local protection systems. This fact highlights the importance of getting a quick response from all the process involved in the WAMPAC structure, which comprise: the time delay for phasor measurement, fiber-optic communications, PDC throughput including wait time for slowly arriving packets, transfer trip, and circuit breaker tripping or closing [24].

In this connection, it is highly important to consider the total WAMPAC communication time delay in order to be sure the vulnerability assessment will orient timely control actions.
Table 1.3  Time delay of a WAMPAC scheme per process [24].

<table>
<thead>
<tr>
<th>Process</th>
<th>Time delay in 60-Hz cycles</th>
<th>Time delay (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMU measurement</td>
<td>3</td>
<td>50</td>
</tr>
<tr>
<td>Fiber-optic communications</td>
<td>2</td>
<td>33</td>
</tr>
<tr>
<td>PDC throughput</td>
<td>2</td>
<td>33</td>
</tr>
<tr>
<td>Transfer trip</td>
<td>1</td>
<td>17</td>
</tr>
<tr>
<td>Circuit breaker</td>
<td>2–5</td>
<td>33–83</td>
</tr>
<tr>
<td>Total WAMPAC time delay</td>
<td>10–13</td>
<td>167–217</td>
</tr>
</tbody>
</table>

This time delay depends on the complexity of each power system, and it has to be determined prior the development of the WAMPAC scheme. For instance, Table 1.3 presents some reference values that orient a typical WAMPAC communication time delay [24].

1.5 The Fundamental Role of WAMS in Dynamic Vulnerability Assessment

As described in the previous section, PMUs are able to provide time-synchronized phasor data with delays of less than 200 ms, which contain valuable dynamic information that could indicate, in real time, the system vulnerability status and potential collapses [7]. These post-contingency data are fundamental to developing methodologies capable of assessing dynamic vulnerability in real time. The huge potential of the dynamic information immersed in PMU data actually allows the assessment of both tasks involved in the concept of vulnerability: (i) the system security level (static and dynamic security), and (ii) the tendency to change the system conditions to a critical state that is called the “Verge of Collapse State.”

For instance, synchronized measurements obtained from Wide Area Monitoring Systems (WAMS) can be used to detect a possible system separation, to monitor the voltage and frequency of critical nodes, or to check power flows in important branches in order to analyze congestion. PMU data could also be used to analyze poorly-damped power system oscillations [25], to carry out transient stability assessment (TSA) [26, 27], or to develop closed loop control schemes in order to improve system stability [12].

A characteristic ellipsoid (CELL) method to monitor the power system dynamic behavior and provide wide area situational awareness using PMU data is presented in [13]. A logic-based method to identify a contingency severity and to assess voltage stability from PMU data is proposed in [28]. These approaches permit the assessment of post-contingency system security level, but they do not consider the tendency of the system to change its conditions to a critical state.

Some methods to perform real time TSA are summarized in [26]. From these methods, Emergency Single Machine Equivalent (E-SIME) seems attractive for real time applications. This method uses the multi-machine rotor angles (δ) and the system accelerating power (Pa) to establish a One Machine Infinite Bus equivalent (OMIB) in
order to predict transient instability, using data obtained from PMUs. In this approach, the calculus of the mechanical variables and the prediction of the Pa–δ curves provoke time delays and accuracy problems. In this same context, [26] presents a method for TSA based on post-contingency area-based center-of-inertia (COI) referred rotor angles estimation from PMU measurements. To this aim, several off-line tasks were addressed to deal with issues regarding the selection of PMU monitoring locations, reduction of data volume, and definition, training, and tuning of a suitable support vector regressor (SVR).

A scheme based on phase-space visualization, which allows finding patterns that could indicate a possible collapse, is presented in [29]. This method permits monitoring of phase-space curves of critical variables and providing early warning, but it needs to draw images in order to find the similarities among them, which makes an automatic response difficult.

A technique for prediction of the transient stability status of a power system following a large disturbance such as a fault, based on synchronously measured samples of the magnitudes of voltage phasors at major generation centers, is presented in [30]. The voltage samples are taken immediately after a fault is cleared and used as inputs to a binary classifier based on a support vector machine (SVM) to identify the transient stability status. This approach considers that there exist PMUs installed in all generators’ terminal buses, and does not contemplate any feature extraction technique in order to reduce the amount of classifier input data; this increases the dimensionality of the problem and might provoke mistakes and delays in the training stage.

A data mining-based framework for performing power system vulnerability assessment and predicting system instabilities that may lead to possible system cascading failure is presented in [31]. Based on Monte Carlo methods, power system contingency data of dynamic and steady state simulations are generated. These data are then analyzed via advanced data mining methods, based on a combination between Graph Theory, Local Correlation Network Pattern (LCNP) and Kernel Based Classification, to find the most relevant system information or patterns with respect to system instability; this is then used for achieving instability prediction based on PMU measurements as well as generator variable measurements. This method suggests using the first 10 or 20 system variables (including generator and system variables) with the greatest chi-square (obtained from LCNP) as the features of the prediction model. This method presents the drawbacks of using too many variables, including those belonging to generators that are not easily to be available (such as rotor angle, speed, mechanical power, etc.) Additionally, results of classification accuracy show a recall (i.e., dependability) of around 93%, which might be improved by using a different data analysis technique.

A vulnerability assessment method for quickly assessing the multi-area power system post-contingency vulnerability status, mainly as regards rotor angle stability, is developed in [32]. This method uses PMU data to compute Wide Area Severity Indices (WASI), as an extension of the severity indices firstly presented in [33]. These WASI are calculated in the frequency domain through applying the Short Time Fourier Transform (STFT) to data obtained from PMUs located in specific system buses, determined by a coherency criterion defined in [34] and improved in [35]. A systematic scheme for rapidly classifying the stability status resulted from WASI using fuzzy rule-based classifiers is presented in [36]. This classifier uses large-size decision trees (DTs) to generate initial accurate classification boundaries for decision making as early as 1 or 2 s after fault
clearing. A WASI-based model-predictive framework for determining fast catastrophe precursors in a bulk power system has been presented in [37]. These fast catastrophe predictors use random-forest (RF) learning in order to increase the classification accuracy, showing excellent performance as regards typical DTs. In [38], a comparison between several data mining classifiers, such as artificial neural network (ANN), SVM, DT, Fuzzy DT, Fuzzy ID3 (Iterative Dichotomiser 3), and RF is performed; from this, the RF-based predictor is the only one to achieve more than 99.0% accuracy based on WASI. However, the RF has poor transparency characteristics and might exhibit over-fitting problems. In this connection, a more transparent predictor is suggested to be used in [38] at the expense of loss of accuracy. WASI offer a novel concept in power system real time VA that reasonably permits estimating the tendency of the system to change its conditions to a critical state. Nevertheless, these indices present the problem of showing a considerable large overlapping zone. For instance, test results in [37] conclude that “75% of stable cases verify the relationship FastWASI300ms < −2.5, while for 75% unstable cases, FastWASI300ms > −2.5.” This fact denotes that the overlapping zone is formed by 25% of stable cases belonging to the region of the unstable cases and vice versa. This large overlapping range is the main reason for classification difficulties.

A data-mining-based approach for predicting power system post-contingency vulnerability status in real time is proposed in [10]. To this aim, system dynamic vulnerability regions (DVRs) are first determined by applying singular value decomposition, by means of empirical orthogonal functions (EOFs), to a post-contingency database obtained from Phasor Measurement Units (PMUs) adequately located throughout the system. In this way, the obtained pattern vectors (EOF scores) allow mapping the DVRs within the coordinate system formed by the set of EOFs, which permits revealing the main patterns buried in the collected PMU signals. The database along with the DVRs enable the definition, training, and identification of a support vector classifier (SVC), which is employed to predict the post-contingency vulnerability status as regards three short-term stability phenomena, that is: transient stability, short-term voltage stability, and short-term frequency stability (TVFS). Enhanced procedures for feature extraction and selection as well as heuristic optimization-based parameter identification are proposed to ensure a robust performance of the SVC. This method allows the assessment of system vulnerability for three different phenomena, estimating the system tendency of changing its conditions to the Verge of Collapse State, and overcomes the drawback of large overlapping caused by applying other types of signal processing tools.

The potential applications for DVA make PMUs fundamental in the basic architecture of a self-healing grid. However, despite the valuable dynamic data obtained from PMUs, they are not able to give any information about system health by themselves. So, it is necessary to develop mathematical tools capable of quickly analyzing the data in order to accurately assess dynamic vulnerability in real time. This is a very novel research area in which further investigation is needed to improve tools and methods, so that in the future, Dynamic Vulnerability Assessment would be performed with confidence as an important element of a self-healing grid structure.

An additional aspect to be considered is PMU data quality. In fact, synchronized measurements will be used as input to control and protection systems after the DVA has determined the necessity of performing corrective control actions; therefore, it is fundamental to have enough confidence about data obtained from the PMUs. In this connection, it is necessary to carry out an evaluation of the performance of PMUs under
Dynamic conditions for previous application in DVA and further control schemes. This is because system perturbations provoke different transients that cause current and voltage wave distortions, such as peaks, sags, frequency variations, oscillations, harmonics, DC components, and so on, which affect the accuracy of synchronized measurements [21]. In this connection, prior to the development and enforcement of dynamic applications, it is necessary to evaluate the performance of PMUs under possible dynamic conditions, which might be used in order to specify the minimum requirements of the devices. This need is essential in order to guarantee the PMUs satisfactorily fulfill the guidelines suggested by the IEEE C37.118.1-2011 standard [23] to assure dynamic compliances, depending on the required application. For instance, the PMUs have to accomplish one of the two performance class filters: P class or M class. P class is for applications requiring fast response whereas M class better adjusts for applications of greater precision. So, depending on the specific application, a different combination of errors from the magnitude and phase angle measurements might be specified in order to get the desired TVE [23].

In summary, based on the presented literature review, WAMS has been determined as the fundamental source of data useful for being the input to adequate mathematical tools capable of assessing vulnerability in real time. To accomplish this function, some basic requirements are necessary, such as the implementation of PMUs with confident enough phasor estimation algorithms, robust communication and information technology systems and, mainly, the development and application of proper mathematical methodologies capable of analyzing huge volumes of data in real time, in order to give confident early warning indicators as soon as the different vulnerability phenomena evolve in real time.

1.6 Concluding Remarks

The lack of investment, the use of congested transmission lines, and other technical reasons, such as environmental constraints, have been dangerously pushing Bulk Power Systems close to their physical limits. Under these conditions, certain sudden perturbations can cause cascading events that may lead to system blackouts. In this connection, it is crucial to ensure system security, so the development of protection systems that allow guaranteeing of service continuity is required. Nevertheless, these remedial action schemes are usually set to operate when specific pre-established operational conditions are reached, so they are unable to work under unconsidered contingencies that might entail cascading events. Thus, the control of the system and the protection triggering should be adjusted depending on the real time progress of a given event, emphasizing the need to develop a “self-healing grid.” Real time Dynamic Vulnerability Assessment (DVA) is a fundamental task within this self-healing grid structure, and PMU-based methods show a huge potential for performing this smart grid application, since they have the capability to detect the necessity of performing the remedial action. DVA has to be carried out in order to trigger adequate corrective control actions that mitigate the consequences of the disturbances and reduce the possibility of system blackouts. This task has opened a very novel research area, where further investigation is needed.
References


