

# Adaptive Protection for Preserving Microgrid Security

Saeed Teimourzadeh, *Student Member, IEEE*, Farrokh Aminifar, *Senior Member, IEEE*, Mahdi Davarpanah, and Mohammad Shahidehpour, *Fellow, IEEE*

**Abstract**— The low inertia renders renewable-based microgrids ( $\mu$ Gs) more susceptible to incipient faults and makes it more difficult for distributed systems to maintain a reasonable margin for dynamic security. This paper studies the  $\mu$ G security using a three-stage approach to the power system protection. The first stage considers offline analyses of synchronous generator-based distributed energy resources (SGBDERs) and inverter-based distributed energy resources (IBDERs) for establishing dynamic security models in  $\mu$ Gs. The required data and settings are also determined at this stage. The second stage uses the first stage models for the online calculation of equilibrium points, regions of attraction, and protection zones for SGBDERs and IBDERs operations. This stage adapts to different conditions for  $\mu$ G operations. The third stage is responsible for the real-time protection of  $\mu$ Gs. This stage uses the real-time data for the fast detection of dynamic security status and protection of  $\mu$ Gs. Simulation results presented in the paper demonstrate the adaptive features of the proposed scheme.

**Index Terms**— Microgrid protection, dynamic security, region of attraction (ROA), equilibrium point (EP).

## NOMENCLATURE

### Sets, Indices, and Operators

|           |  |
|-----------|--|
| $\mu B$   | Set of buses                                     |
| $\mu DER$ | Set of DERs                                      |
| $R$       | Set of real numbers                              |
| $\mu$     | Index for $\mu G$                                |
| $m, e$    | Indices for mechanical and electrical quantities |
| $RT$      | Index for real-time value                        |
| $s, c$    | Indices for SGBDERs and IBDERs, respectively     |
| $0$       | Subscript for initial condition                  |
| $*$       | Superscript for EP                               |
| $\Delta$  | Difference operator                              |
| $\bullet$ | Derivative operator                              |
| $\  \ $   | Norm operator                                    |

### Parameters

|                       |  |
|-----------------------|--|
| $n$                   | Dimension of state space                         |
| $\sigma, \epsilon$    | Small positive values                            |
| $\omega_0$            | Nominal synchronous speed (Radians/second)       |
| $D$                   | Damping factor (MW/Hz)                           |
| $H$                   | Inertia constant (seconds)                       |
| $E$                   | Voltage amplitude (p.u.)                         |
| $Y_{js}(\theta_{js})$ | Modulus (argument) of admittance matrix elements |
| $P$                   | Active power (p.u.)                              |
| $Q$                   | Reactive power (p.u.)                            |
| $T$                   | Torque (N.m)                                     |
| $m_{if}$              | Voltage set point of IBDER (p.u.)                |
| $I_{set}$             | Current set point of IBDER (p.u.)                |

$k_p, k_I$  Control coefficients of IBDER

### Variables

|              |  |
|--------------|--|
| $\mathbf{x}$ | Vector of state variables                  |
| $t$          | Time (seconds)                             |
| $\omega$     | Angular velocity of rotor (Radians/second) |
| $\delta$     | Rotor angle (Radians)                      |
| $I_o$        | Output current of IBDER (p.u.)             |
| $\varphi$    | Angle of $I_o$ (Radians)                   |

## I. INTRODUCTION

THE manifested merits of distributed energy resources (DERs) in power systems have given rise to significant interests in microgrid ( $\mu$ G) developments at regional levels. The  $\mu$ G benefits include enhancements in power system reliability, resilience, economics, security, and sustainability. The merits of  $\mu$ G development also consider significant reductions in transmission system congestion and deferral of power system expansion in densely populated regions and socially unstable territories of the world [1]-[3]. Such benefits are challenged by technical issues pertaining to  $\mu$ G planning, operation, control, and protection [4]-[7]. In particular,  $\mu$ G security issues are highlighted among the major concerns for using inverter-based DERs (IBDERs) and synchronous generator-based DERs (SGBDERs) in  $\mu$ Gs [8], [9].

The lack of dynamic security in  $\mu$ Gs, which is due to low inertia (inertia constant that is smaller than 2 seconds) and long fault clearing time in  $\mu$ Gs, is considered a serious challenge to power system distribution operations [10], [11]. The security issue will be exacerbated by the proliferation of distributed devices and  $\mu$ Gs which continue to grow in power distribution systems. In practice, dynamic security deals with the ability of  $\mu$ Gs to maintain synchronism when the  $\mu$ Gs are subjected to severe disturbances [12]. The loss of synchronism that is also referred to as the out-of-step condition or pole slip incident requires the deployment of out-of-step relays which operate based on the mho characteristic and blinder as a common practice to tackle dynamic security [13].

Several out-of-step protection schemes were proposed earlier, which were mostly applied to bulk power systems with considerable inertia and deemed inefficient for  $\mu$ G operations. The drawback of these methods is that they require a long time to detect unsecured states, presumably after a few pole-slip incidents, which could damage DERs or interrupt loads in  $\mu$ Gs. Certain procedures and grid codes have recommended to disconnect DERs upon the occurrence of any faults [14], [15], which render  $\mu$ Gs inefficient for maintaining the supply of electricity in island mode when critical circumstances are eminent. In [16], undervoltage relay was exposed to out-of-step protection. However, improper selections of undervoltage relay settings and inadequate schemes for power distribution protection could also lead to unnecessary tripping of DERs. Another out-of-step protection relay for  $\mu$ Gs was proposed in

S. Teimourzadeh, F. Aminifar, and M. Davarpanah are with the School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Tehran, 11365-4563, Iran (e-mail: [teimourzadeh@ut.ac.ir](mailto:teimourzadeh@ut.ac.ir), [faminifar@ut.ac.ir](mailto:faminifar@ut.ac.ir), [m.davarpanah@ut.ac.ir](mailto:m.davarpanah@ut.ac.ir)). M. Shahidehpour is with the Electrical and Computer Engineering Department, Illinois Institute of Technology, Chicago, IL 60616 USA (e-mail: [ms@iit.edu](mailto:ms@iit.edu)).

[10] which applied sensitivity analyses to special operation cases in distributed power systems.

A proper protection scheme for preserving the dynamic security in  $\mu$ Gs should be fast and accurate to prevent any unnecessary tripping of DERs considering the effect of non-rotating IBDERs in low inertia  $\mu$ Gs. To fulfill such requirements, we propose an adaptive three-stage protection scheme in this paper, which is presented as follows: The first stage represents offline analyses of SGBDERs and IBDERs for establishing dynamic security models in  $\mu$ Gs. The required data and settings are also determined at this stage. The second stage is for online calculations of equilibria, regions of attraction, and protection zones for SGBDERs and IBDERs operations. The third stage is responsible for the real-time protection of  $\mu$ G state by issuing proper trip commands. This stage includes a fast detection of dynamic state for protection and preserving the  $\mu$ G security. The simulation studies validate the effectiveness of the proposed method for a fast and precise detection of dynamic state in  $\mu$ Gs.

## II. MATHEMATICAL BACKGROUND OF ADAPTIVE PROTECTION

The terms and definitions utilized in our paper are discussed as follows [17], [18].

Consider a nonlinear system model as:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) \quad (1)$$

where,  $\mathbf{f}: S \rightarrow R^n$  is a continuously differentiable function from a domain  $S \subseteq R^n$  into  $R^n$ .

**Definition 1:**  $\phi(t; \mathbf{x}_0)$  is the solution of (1), with an initial value of  $\mathbf{x}(0) = \mathbf{x}_0$ , evaluated at time  $t \geq 0$ .  $\phi(t; \mathbf{x}_0)$  is the system trajectory which crosses  $\mathbf{x}_0$ .

**Definition 2:** A vector  $\mathbf{x}^* \in R^n$  is an equilibrium point (EP) of (1) if  $\mathbf{f}(\mathbf{x}^*) = \mathbf{0}$ .

**Definition 3:** The  $\mathbf{x}^*$  associated with (1) is:

(i) a stable EP (SEP), if for any  $\varepsilon \geq 0$ , there exists  $\sigma = \sigma(\varepsilon)$  so that

$$\|\mathbf{x}_0\| \leq \sigma \Rightarrow \|\phi(t; \mathbf{x}_0)\| \leq \varepsilon \quad \forall t \geq 0; \quad (2)$$

(ii) an unstable EP (UEP), if (2) does not hold;

(iii) an asymptotically SEP if (2) and (3) are fulfilled

$$\|\mathbf{x}_0\| \leq \sigma \Rightarrow \lim_{t \rightarrow \infty} \phi(t; \mathbf{x}_0) = \mathbf{x}^*. \quad (3)$$

**Definition 4:** The region of attraction (ROA) associated with an asymptotically SEP, say  $\mathbf{x}^*$ , is defined as:

$$\Omega = \left\{ \mathbf{x} \in R^n \mid \lim_{t \rightarrow \infty} \phi(t; \mathbf{x}_0) = \mathbf{x}^* \right\} \quad (4)$$

The ROA associated with an asymptotically SEP is a set of points, say  $\Omega$ , such that any trajectory originating from  $\mathbf{x}_0 \in \Omega$  at time 0 will be attracted to the SEP.

**Definition 5:**  $\Lambda \subseteq R^n$  is a positively invariant set of (1) if  $\mathbf{x}_0 \in \Lambda$  implies  $\phi(t; \mathbf{x}_0) \in \Lambda$  for  $t \geq 0$ . Hence, if a solution resides in a positively invariant set at some time intervals, the solution will stay within the set in any future time intervals.

**Theorem 1 (Lyapunov's indirect method):** Let  $\mathbf{A}$  be a Jacobian matrix of (1) at  $\mathbf{x}^*$ :

$$\mathbf{A} = \frac{\partial \mathbf{f}}{\partial \mathbf{x}} \bigg|_{\mathbf{x}=\mathbf{x}^*} = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \cdots & \frac{\partial f_n}{\partial x_n} \end{bmatrix} \bigg|_{\mathbf{x}=\mathbf{x}^*} \quad (5)$$

The  $\mathbf{x}^*$  is an asymptotically SEP of (1) if all eigenvalues associated with  $\mathbf{A}$  are located on the left-half plane. Likewise,  $\mathbf{x}^*$  is a UEP if  $\mathbf{A}$  has eigenvalues on the right-half plane. UEP is called nodal source if all eigenvalues have positive real parts. On the contrary, UEP is saddle point if some eigenvalues have positive real parts while others have negative real parts.

In this paper, first the  $\mu$ G dynamic security model is devised using (1). Then, *Definitions 1, 2, 3*, and *Theorem 1* are applied to calculate EPs and identify associated stability features. The ROA computed by *Definitions 4* and the invariant property presented in *Definitions 5* are deployed next to establish the protection zone.

## III. PROPOSED METHODOLOGY

The  $\mu$ G protection methodology considering the proposed three stages is depicted in Fig. 1. The objective is to calculate and preserve the dynamic security in  $\mu$ Gs by determining out-of-step protection requirements.

In Fig. 1, the offline analyses at Stage 1 are performed initially to devise the dynamic security models of  $\mu$ Gs. Stage 2 defines the  $\mu$ G protection zone using the online  $\mu$ G data and calculates EPs by applying the online data to the Stage 1 model. Then the ROA associated with the asymptotically SEP is calculated and the protection zone is formed using the calculated ROA. Stage 3 introduces the real-time protection where the  $\mu$ G state variables are monitored in real-time. At this Stage, the trip command is issued if the protection zone boundary is violated.

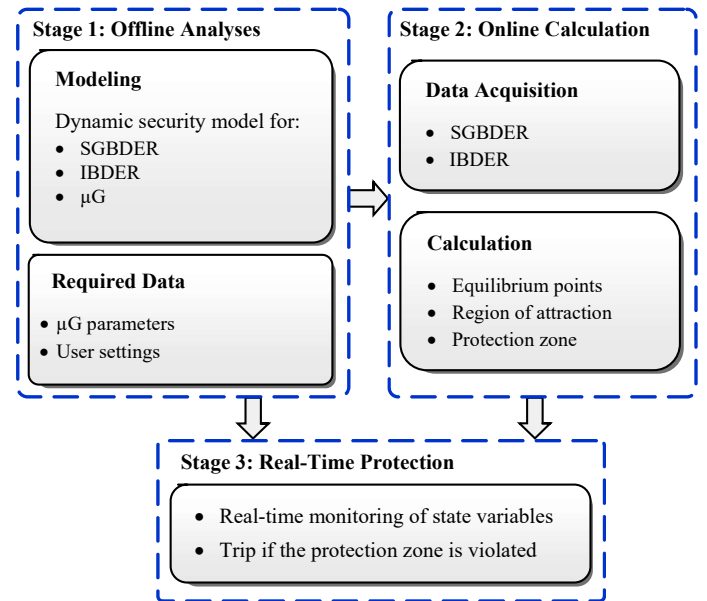


Fig. 1. Proposed adaptive protection Scheme.

The data transferred among the blocks are as follows.

- $\mu$ G dynamic security model and parameters are transferred

- from Stage 1 to Stage 2;
- User settings are transferred from Stage 1 to Stage 3; and,
- Protection zone is transferred from Stage 2 to Stage 3.

The detailed formulation for each stage is given as follows.

#### A. Stage 1: Offline Analysis

The schematic diagram of a  $\mu$ G incorporating SGBDERs and IBDERs is depicted in Fig. 2. In the case of  $\mu$ G faults, the role of the main grid, which is regarded as an infinite bus, is crucial in managing the  $\mu$ G security. Considering the one-machine-infinite-bus model of SGBDER for the dynamic security assessment, we have (stated in p.u.),

$$\begin{cases} \dot{\delta}_s = \omega_0 \cdot \Delta \omega_s \\ \dot{\Delta \omega}_s = (P_s^m - P_s^e - D_s \Delta \omega_s)(2H_s)^{-1} \end{cases} \quad (6)$$

where,

$$P_s^e = E_s^2 Y_{ss} \cos \theta_{ss} + \sum_{\substack{j \in \mu B \\ j \neq s}} E_j E_s Y_{js} \cos(\delta_s - \delta_j - \theta_{js}) \quad (7)$$

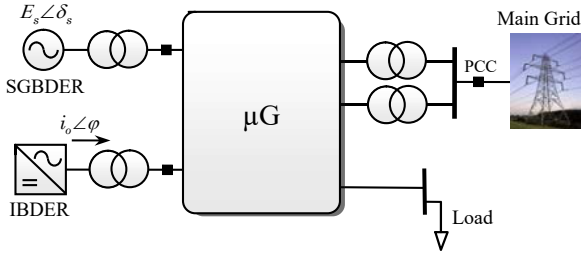


Fig. 2. Schematic diagram of a  $\mu$ G.

DERs operate in the P-Q mode during  $\mu$ G grid-connected operating condition. Accordingly, the role of main grid is dominant as compared with that of local DERs in managing  $\mu$ G voltage particularly when DERs are connected to the main bus of  $\mu$ G. Here, the dynamics of  $E_s$  could be disregarded while devising a dynamic security model. This simplification also eases the calculation of ROA and the protection zone. For IBDERs, a fault condition is modeled by the droop-based control scheme, which is equivalent to a synchronverter [19], [20]. The synchronverter mimics the dynamics of a synchronous generator which is depicted in Fig. 3 and modeled by (8)-(10) [21], [22]:

$$T_c^e = 1.5 m_f i_f I_o \cos(\delta_c - \varphi) \quad (8)$$

$$Q = 1.5 m_f i_f I_o \sin(\delta_c - \varphi) \quad (9)$$

$$E = \dot{\delta}_c m_f i_f \sin \delta_c \quad (10)$$

Hence, the dynamics of a synchronverter (stated in p.u.) are described as:

$$\begin{cases} \dot{\delta}_c = \omega_0 \cdot \Delta \omega_c \\ \dot{\Delta \omega}_c = (P_c^m - P_c^e - D_c \Delta \omega_c)(2H_c)^{-1} \end{cases} \quad (11)$$

where,

$$P_c^e = 1.5 m_f i_f I_o \cos(\delta_c - \varphi) \quad (12)$$

At a pre-fault condition,  $P_c^e$  is constant which results in constant  $I_o$ . The voltage dip imposed by a fault leads to an

increase in  $I_o$ . However,  $I_o$  is limited to avoid any damages to power electronic switches. A current source is used to model the IBDER fault condition as represented by Fig. 4, in which we disregard the dynamics of internal loops of IBDER because of its fast response [23], [24].

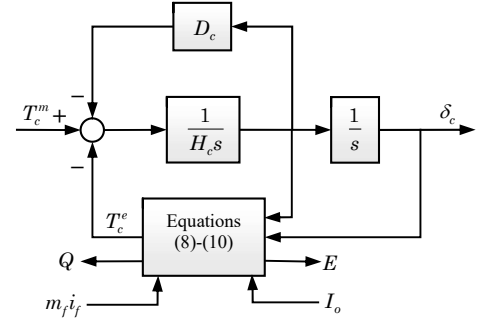


Fig. 3. Block diagram of a synchronverter.

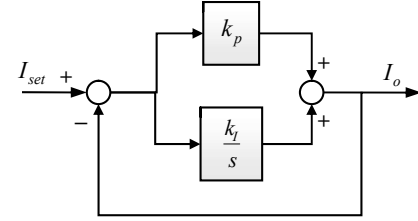


Fig. 4. Dynamics of  $I_o$  for transition from pre-fault to during the fault status.

The state space model in Fig. 4 is expressed in (13), and the fault condition of IBDER is modeled using (11)-(13):

$$\dot{I}_o = (1 + k_p)^{-1} [k_i (I_{set} - I_o) + k_p \dot{I}_{set}] \quad (13)$$

Note that  $I_{set}$  is constant and its derivative,  $\dot{I}_{set}$  stated in (13) is zero. Once the model for representing the dynamic security of SGBDER and IBDER is devised, the  $\mu$ G dynamics are expressed as:

$$\dot{\delta}_\mu = \sum_{i \in \mu DER} H_\mu^{-1} H_i \dot{\delta}_i \quad (14)$$

$$H_\mu = \sum_{i \in \mu DER} H_i \quad (15)$$

$$D_\mu = \sum_{i \in \mu DER} D_i \quad (16)$$

$$\begin{cases} \dot{\delta}_\mu = \omega_0 \cdot \Delta \omega_\mu \\ \dot{\Delta \omega}_\mu = (2H_\mu)^{-1} \left[ \sum_{i \in \mu DER} (P_i^m - P_i^e) - D_\mu \Delta \omega_\mu \right] \end{cases} \quad (17)$$

Inserting (7) and (12) into (17) yields:

$$\begin{cases} \dot{\delta}_\mu = \omega_0 \cdot \Delta \omega_\mu \\ \dot{\Delta \omega}_\mu = (2H_\mu)^{-1} \left[ \sum_{i \in \mu DER} P_i^m - E_s^2 Y_{ss} \cos \theta_{ss} \right. \\ \quad \left. - \sum_{\substack{j \in \mu B \\ j \neq s}} E_j E_s Y_{js} \cos(\delta_s - \delta_j - \theta_{js}) - D_\mu \Delta \omega_\mu \right. \\ \quad \left. - 1.5 m_f i_f I_o \cos(\delta_c - \varphi) \right] \\ \dot{I}_o = (1 + k_p)^{-1} [k_i (I_{set} - I_o)] \end{cases} \quad (18)$$

The small-scale DERs in  $\mu$ Gs see the main grid as an infinite bus with comparatively large inertia ( $H_{\text{main grid}} \gg H_{\mu\text{G}}$ ) which remains almost secured in  $\mu$ Gs disturbances. This issue is more evident when DERs with similar oscillations, representing one equivalent DER against the main grid, are connected to the main bus of  $\mu$ G. Accordingly,  $\mu$ G dynamics are commonly assessed using an equivalent DER against the main grid. Note that the proposed formulation can be extended to multi-DER  $\mu$ Gs.

### B. Stage 2: Online calculation

Given the  $\mu$ G topology and the parameters presented in (18), Stage 2 which is updated periodically, acquires the online data of  $\mu$ G representing DER operating points as well as bus voltages. Consider the  $\mu$ G depicted in Fig. 5 in which the rated power of the SGBDER is 5MVA and  $I_{\text{set}}$  during the fault is 2 p.u.  $k_p$  and  $k_I$  are set at 0.1 and 200, respectively [10], [24].

Applying the model presented in (18) to the power system in Fig. 5 yields:

$$\begin{cases} \dot{\delta}_\mu = \omega_0 \Delta \omega_\mu \\ \dot{\Delta \omega}_\mu = (2H_\mu)^{-1} [P_s^m + P_c^m - E_s V_m X_s^{-1} \sin \delta_\mu - 1.5 m_f i_f I_o \cos(\delta_c - \varphi) - D_\mu \Delta \omega_\mu] \\ \dot{I}_o = (1 + k_p)^{-1} [k_I (I_{\text{set}} - I_o)] \end{cases} \quad (19)$$

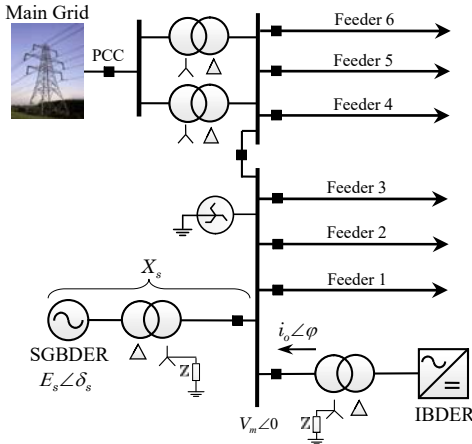


Fig. 5. The power system under study.

The data acquired at Stage 2 are  $P_s^m$ ,  $P_c^m$ ,  $m_f i_f$ , and  $I_{\text{set}}$ . The corresponding EPs for (19) are computed using Definition 2,

$$EP = \begin{cases} EP^{(1)}: & \delta_\mu^* = \sin^{-1} \Gamma & \Delta \omega_\mu^* = 0 & I_o^* = I_{\text{set}} \\ EP^{(2)}: & \delta_\mu^* = \pi - \sin^{-1} \Gamma & \Delta \omega_\mu^* = 0 & I_o^* = I_{\text{set}} \end{cases} \quad (20)$$

where,

$$\begin{aligned} \Gamma &= [P_m - V_c I_{\text{set}}] P_{\text{max}}^{-1}, P_m = P_s^m + P_c^m \\ P_{\text{max}} &= E_s V_m X_s^{-1}, V_c = 1.5 m_f i_f \cos(\delta_c - \varphi) \end{aligned} \quad (21)$$

Here, the EP security is investigated for calculating the ROA. The Jacobian matrix of (19) and eigenvalues are given as:

$$A^{(1,2)} = \begin{bmatrix} 0 & -P_{\text{max}} \cos \delta_\mu^{*(1,2)} & 0 \\ \omega_0 & -D_\mu & 0 \\ 0 & -V_c & -k_I (1 + k_p)^{-1} \end{bmatrix}^T \quad (22)$$

$$\lambda^{(1,2)} = \begin{cases} -k_I (1 + k_p)^{-1} \\ -0.5 D_\mu + 0.5 \sqrt{-D_\mu^2 - 4 \omega_0 P_{\text{max}} \cos \delta_\mu^{*(1,2)}} \\ -0.5 D_\mu - 0.5 \sqrt{-D_\mu^2 - 4 \omega_0 P_{\text{max}} \cos \delta_\mu^{*(1,2)}} \end{cases} \quad (23)$$

For  $EP^{(1)}$ ,  $-D_\mu^2 - 4 \omega_0 P_{\text{max}} \cos \delta_\mu^{*(1)}$  is negative which results in an imaginary eigenvalue. The real part of eigenvalues associated with  $EP^{(1)}$  is negative and  $\lambda^{(1)}$  is located on the left-half plane. However,  $EP^{(2)}$  possess at least one eigenvalue on the right-half plane representing UEP. Hence, according to Theorem 1,  $EP^{(1)}$  is an asymptotically SEP. Once the EPs and their dynamic properties are identified, the ROA for the asymptotically SEP is calculated.

The ROA associated with an asymptotically SEP is an open, connected, and invariant set that the boundaries are restricted by trajectories which can be characterized by limit cycles or stable trajectories of saddle points. According to Theorem 1, the UEP in our case is a saddle point that associated stable trajectory is used to calculate the ROA. The numerical approach is used here which is a common practice in the literature [17]. Fig. 6 depicts the ROA of  $EP^{(1)}$  considering 2.5 MW and 1 MW as the operating points for SGBDER and IBDER, respectively. Note that (19) describes complete dynamics of the system depicted in Fig. 5 regardless of parameter values. The numerical value of parameter  $D_\mu$  associated with this system is considered negligible in Fig. 6.

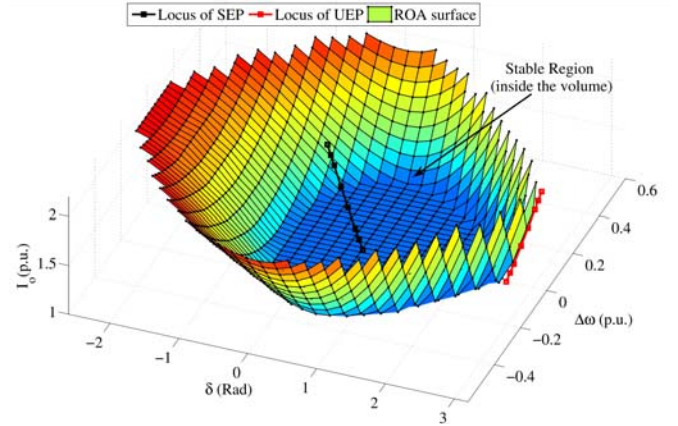


Fig. 6. The shear of ROA for the system represented by (19).

Fig. 7 illustrates the ROA in a two-dimensional plane with the invariant property of trajectories stated in Definition 5. In Fig. 7 (a), the trajectories located inside the ROA are stable and those outside the ROA are unstable. During a fault, the initial SEP is shifted within the ROA which could subsequently result in unsecured status. Fig. 7(b) depicts the during fault trajectories of the operating point. The dynamic security of  $\mu$ G is preserved as long as the EP stays within ROA. In Fig. 7(b), all fault trajectories are originated from SEP which is the system operating point in a pre-fault condition. Here, UEP cannot not be excited as the  $\mu$ G pre-fault condition.

The ROA depends on two factors, i.e. connection style of DERs to the infinite bus, particularly SGBDER, and operating point of  $\mu$ G. There are two alternatives for placing SGBDER in  $\mu$ Gs, namely SGBDER connected to the main bus and SGBDER located along the feeder. The ROA is affected by the  $\mu$ G topology alterations when SGBDER is located along the



feeder and the enumeration of all possible scenarios is difficult for such a case. However, ROA will not be affected by any alterations in  $\mu G$  topology or feeder configuration when SGBDER is connected to the main bus. Accordingly, we assume the SGBDER connection style to the main bus is fixed using the parameters stated at Stage 1. We consider the effect of  $\mu G$  operating point at Stage 2.

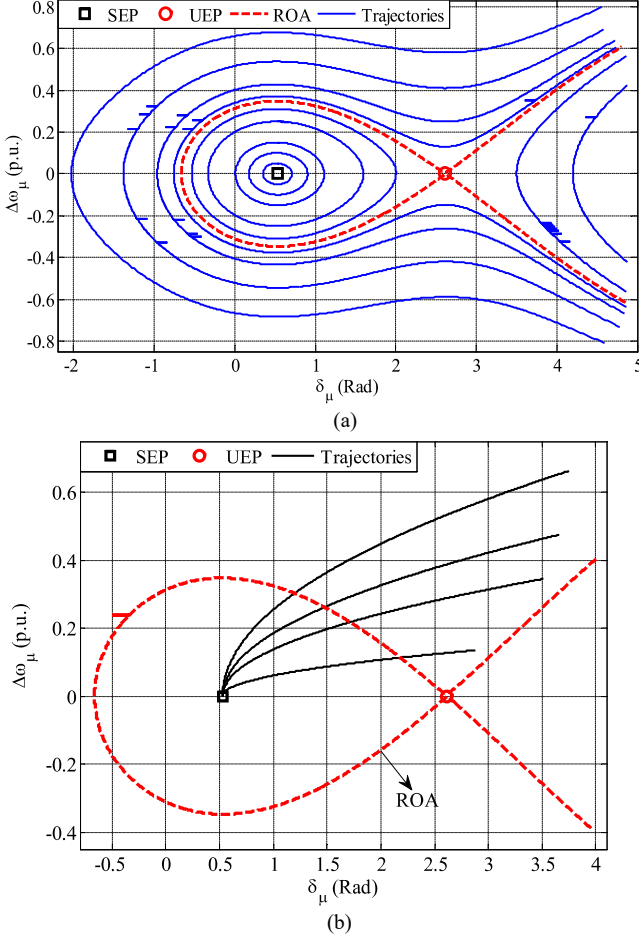


Fig. 7. ROA and operating point trajectories: a) without fault b) with fault.

In (19),  $V_m$  and  $X_s$  are the only topology-dependent elements.  $V_m$  is regulated by the dominant main grid. Here, the voltage drop which is due to a topology alteration is trivial representing almost equal  $V_m$  values at pre-fault and post-fault conditions. In Fig. 5,  $X_s$  is the equivalent impedance located between  $E_s$  and  $V_m$  (infinite bus) which is determined based on the SGBDER connection style to the main bus. Here, the SGBDER connection is through a step-up transformer using a fixed value for  $X_s$  in pre-fault and post-fault conditions.

One may utilize the entire ROA as a security index, in which the inside and the outside of ROA would be labeled as blocking and tripping zones, respectively. However, we can demonstrate that the ROA portion, designated as a protection zone, is sufficient for developing the proposed security measure. During the fault,  $V_m$  in (19) is roughly zero and the dynamic of  $\Delta\omega_\mu$  is written as:

$$\dot{\Delta\omega_\mu} = u_1 - u_2 \Delta\omega_\mu \quad (24)$$

where,

$$u_1 = (2H_\mu)^{-1}(P_m - V_c I_o), \quad u_2 = D_\mu (2H_\mu)^{-1} \quad (25)$$

If we solve the differential equation (24) and use  $\Delta\omega_\mu = \Delta\omega_\mu^*$  as the initial condition, we have:

$$\Delta\omega_\mu = u_1 u_2^{-1} (1 - e^{-u_2 t}) \quad \forall t \geq 0 \quad (26)$$

$\delta_\mu$  can be computed by placing (26) in (19) and solving the associated differential equation with  $\delta_\mu = \delta_\mu^*$  as the initial condition. Accordingly,

$$\delta_\mu = u_1 u_2^{-1} [t + u_2^{-1} e^{-u_2 t} - u_2^{-1}] + \delta_\mu^* \quad \forall t \geq 0 \quad (27)$$

In (26)-(27), both  $\Delta\omega_\mu$  and  $\delta_\mu$  increase monotonically during a fault, considering  $\Delta\omega_\mu \geq \Delta\omega_\mu^*$  and  $\delta_\mu \geq \delta_\mu^*$ , without violating the ROA. The intersection of these three constraints represents the protection zone, depicted in Fig. 8, in which the ROA is initiated from UEP and terminated at point A which includes the Stage 2 solution.

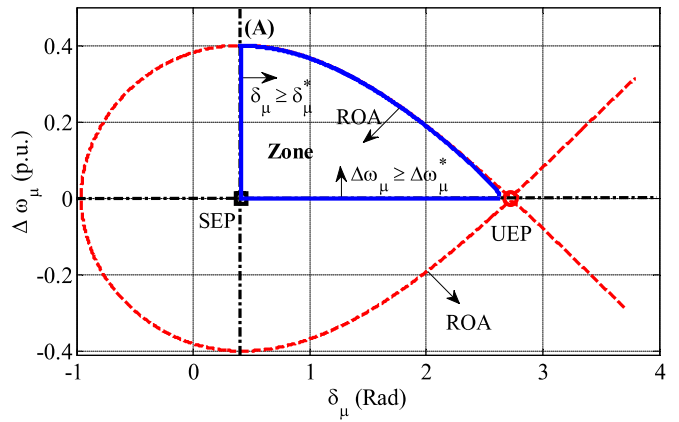


Fig. 8. Protection zone with blocking and tripping regions.

### C. Stage 3: Real-Time Protection

This stage monitors the  $\mu G$  state variables, i.e.  $\delta_\mu$ ,  $\Delta\omega_\mu$ , and  $I_o$ , and maps the trajectory, calculated at Stage 2, to the protection zone. The trip command will be issued once the trajectory violates the protection zone.

The integration sequence of Stages 1, 2, and 3 is stated as follows: For a given  $\mu G$ , Stage 1 is carried out only once to determine the required ingredients for Stages 2 and 3. Afterwards, the protection zone associated with the acquired online data is calculated at Stage 2 and the stage is updated periodically to renew the protection zone based on the changes in the  $\mu G$  operating point. In a fault condition, Stage 3 maps the trajectory of real-time data within the protection zone calculated in Stage 2 and the trip command will be issued once the trajectory violates the protection zone.

Fig. 9 depicts the flowchart of the proposed method. In Fig. 9, the online data used at Stage 2 are given in block 1. The acquired data included in block 2 will be checked at block 3 and the corresponding changes are applied to the model in (19) for calculating EPs, ROA, and protection zones (blocks 5-8). Otherwise, the algorithm will wait for  $t_{set}$  to check the changes at block 4. The data required for Stage 3 are reported in block 9. After the real-time data acquisition (block 11), the algorithm looks for any  $\mu G$  faults (block 12). In a fault condition, the real-time IBDER current,  $I_o^{RT}$ , which was not acquired as an input, will be calculated in block 13.

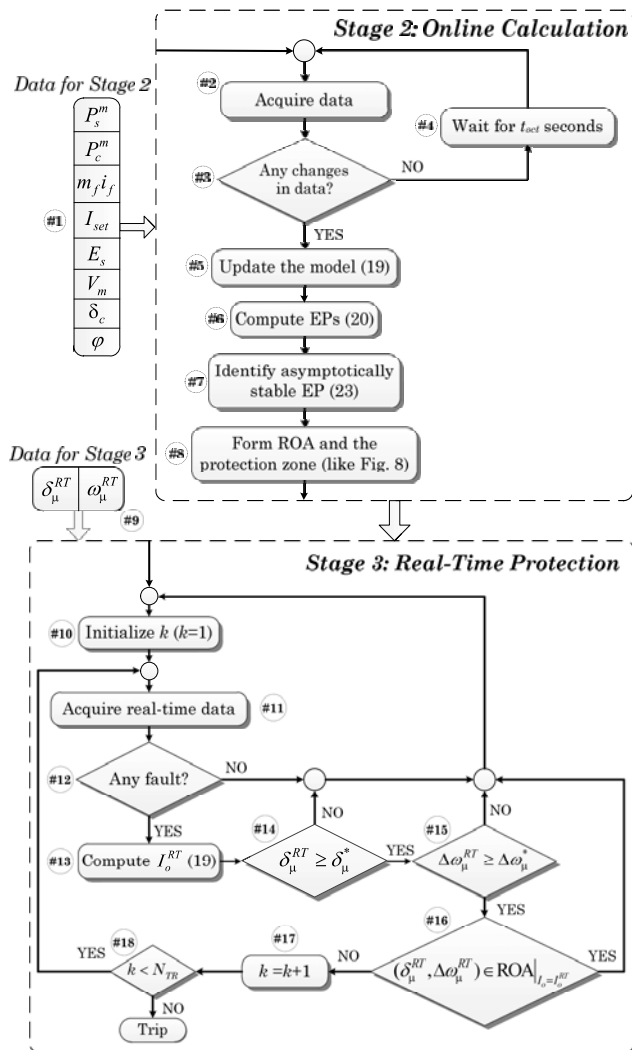


Fig. 9. Flowchart of the proposed adaptive protection approach.

To avoid the communication cost for the measured state variables,  $\delta_\mu$ ,  $\Delta\omega_\mu$ ,  $I_o$ , the relays located at SGBDER will monitor the real-time values of  $\delta_\mu, \Delta\omega_\mu$  locally. Using (19), we develop the dynamic behavior of  $I_o$ , depicted in Fig. 10, which requires the initial conditions of  $I_o$  and  $I_{set}$  calculated at Stage 2, and the IBDER fault contribution.

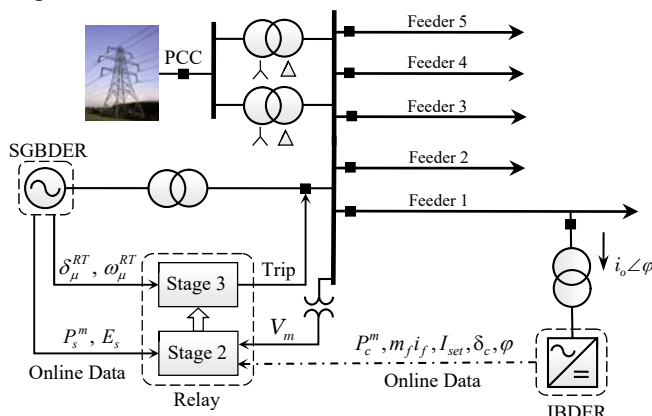


Fig. 10. Schematic of  $\mu G$  for the implementation of the proposed method.

Once  $I_o$  is calculated in block 13, state variables will be compared with zonal boundary quantities (blocks 14-16). Next,

if block 16 indicates that the protection zone is violated, the subsequent  $N_{TR}$  samples will also be reviewed in blocks 12-18 for examining the proposed outcome. Accordingly, the trip command will be issued when a specific number of samples signal a violation (i.e., block 16 with “NO” output). However, considering a large  $N_{TR}$  could prolong the process for examining the security; however, a small  $N_{TR}$  might result in unreliable decisions. Thus, a compromise should be considered when selecting the number of samples.

In Fig. 9, the online computations are performed at Stage 2, when the system is in its normal condition. For any change in the online data, Stage 2 renews the protection zone very fast. This process depends on the updating rate of data acquisition system which provides the online data for Stage 2. While the update could be made in seconds, the Stage 2 computation for forming the protection zone takes about 50ms (using a personal computer with Intel Core™ i5 CPU @2.8 GHz) as depicted in Fig. 8. Accordingly, the protection zone associated with an operation condition is made available upon any updates in online data. The real-time protection process at Stage 3 takes only a few milliseconds.

## IV. SIMULATION RESULTS

This section applies the proposed protection scheme to the system depicted in Fig. 5. The case studies considering complete models and associated controllers for SGBDER, IBDER are performed using the DiGSILENT Power Factory software. The deployed governor and excitation system models for SGBDER are HYG0V and IEEE DC1A whose parameters are given in Tables I and II, respectively [26], [27]. The IBDER parameters are similar to those of Section III.B.

TABLE I  
PARAMETERS CONSIDERED FOR HYGOV MODEL

| Parameter              | Value      | Parameter           | Value       |
|------------------------|------------|---------------------|-------------|
| Temporary Droop        | 0.1 (p.u.) | No Load Flow        | 0.01 (p.u.) |
| Governor Time Constant | 10 (s)     | Permanent Droop     | 0.04 (p.u.) |
| Filter Time Constant   | 0.1 (s)    | Minimum Gate Limit  | 0 (p.u.)    |
| Servo Time Constant    | 0.5 (s)    | Gate Velocity Limit | 0.15 (p.u.) |
| Turbine Gain           | 1 (p.u.)   | Maximum Gate Limit  | 1 (p.u.)    |

TABLE II  
PARAMETERS USED FOR IEEE DC1A MODEL

| Parameter                   | Value       | Parameter           | Value      |
|-----------------------------|-------------|---------------------|------------|
| Measurement Delay           | 0.02 (s)    | Saturation Factor 1 | 3.9 (p.u.) |
| Controller Gain             | 200 (p.u.)  | Saturation Factor 2 | 0.1 (p.u.) |
| Controller Time Constant    | 0.03 (s)    | Saturation Factor 3 | 5.2 (p.u.) |
| Exciter Constant            | 1 (p.u.)    | Saturation Factor 4 | 0.5 (p.u.) |
| Exciter Time Constant       | 0.2 (s)     | Min Output          | -10 (p.u.) |
| Stabilization Path Gain     | 0.05 (p.u.) | Max Output          | 10 (p.u.)  |
| Stabilization Time Constant | 1.5 (s)     |                     |            |

Given a rate of 20 samples per cycle,  $N_{TR}$  is assumed to be 6. Also, SGBDER and IBDER operating points are 2.5 MW and 1 MW, respectively. The simulation results for a three-phase fault in the middle of feeder 1 are illustrated in Fig. 11 with state space representations shown in Fig. 12. Here, a three-phase fault is considered since it encompasses other types of faults. In Fig. 11,  $\delta_\mu$ ,  $\Delta\omega_\mu$ , and  $I_o$  are increased after a fault inception (T1 in Fig. 11). This trend is observable until the fault clearance, i.e., T2 and T3 for Cases I and II, respectively. The behavior of state variables from pre-fault condition, namely SEP in Fig. 12, until the fault clearance, T2 and T3, follows the dynamics depicted in Fig. 7(b). The IBDER response to a fault is also depicted in Fig. 11(c) which shows

an increase in  $I_o$  that is limited to 2 p.u. This behavior also follows the dynamics presented in Fig. 4. These observations confirm the accuracy of the model proposed in (19).

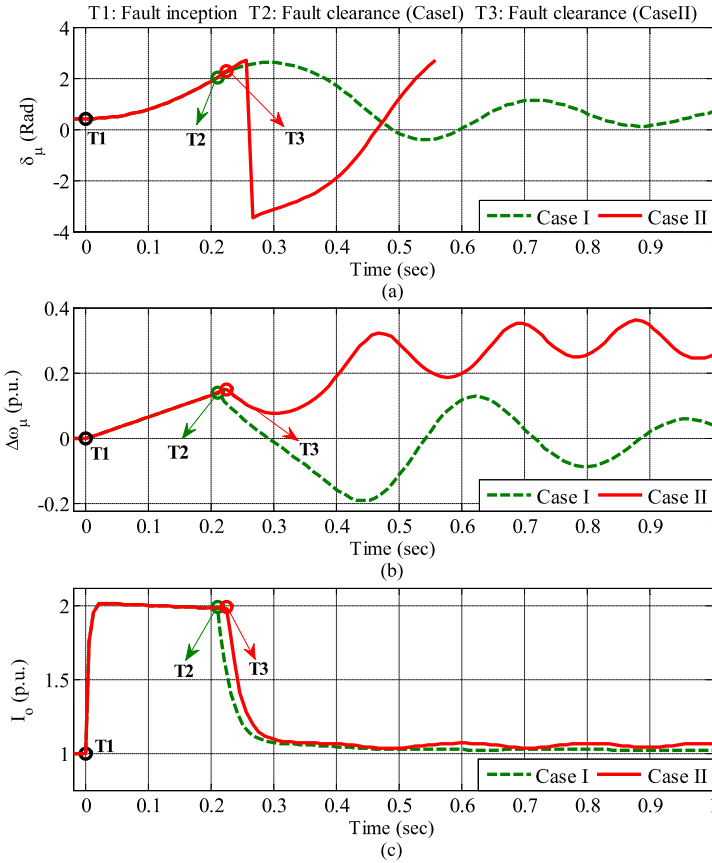


Fig. 11. Simulation results: a)  $\delta_\mu$ , 2)  $\Delta\omega_\mu$ , 3)  $I_o$ .

The fault clearance for Cases I and II occurs at 210 and 225 ms, respectively. In this example, Case I is secured and Case II is unsecured because the fault clearance for Case I lies within the ROA (T2 in Fig. 12); while the fault clearance associated with Case II is outside ROA at T3, which is located on an unstable trajectory. This observation reveals that the ROA can be applied as an efficient index for measuring the  $\mu$ G security.

For the sake of comparison, the performances of conventional out-of-step scheme (CS) and the proposed scheme (PS) in Case II are depicted in Fig. 13. The CS settings are stated using [13]. The CS discriminates between secured and unsecured conditions based on the behavior of impedance trajectory in crossing the blinders. The protection zone of CS and associated blinders are depicted in Fig. 13(a). Here, the vertical line with square markers represents the impedance between SGBDER and the main grid. In a fault condition, the impedance trajectory,  $Z_{seen}$ , rapidly enters the zone by crossing one of the blinders, say B1. After the fault clearance, the impedance trajectory tends to exit the zone. As demonstrated, the trajectory exits the zone by crossing blinder B2 and enters the zone again by crossing B1 which means that Case II is unsecured [13]. According to Fig. 13 (b), the unsecured state is also detected by the PS as the fault trajectory violates the proposed zone. However, the results show that the PS can detect the unsecured state within  $T_i^{PS}$  which is much quicker than that of CS, i.e.,  $T_i^{CS}$ . Fig. 14 shows that PS detects the

unsecured status before the pole slip instant and CS detects it after the occurrence of pole slip incident. This feature for prompting the detection of dynamic security status fits well with the  $\mu$ G out-of-step protection requirements.

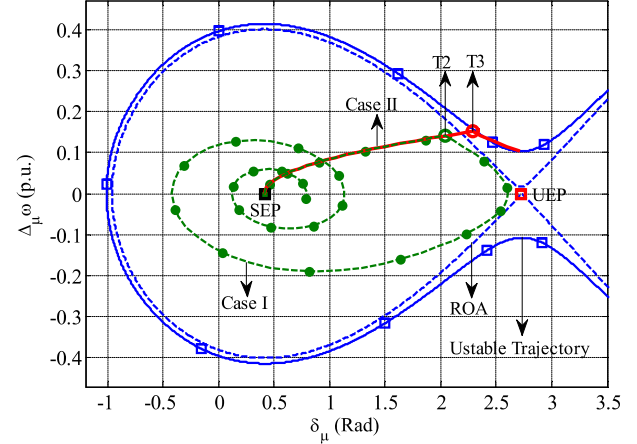


Fig. 12. State space representation (Case I: dashed line, Case II: solid line).

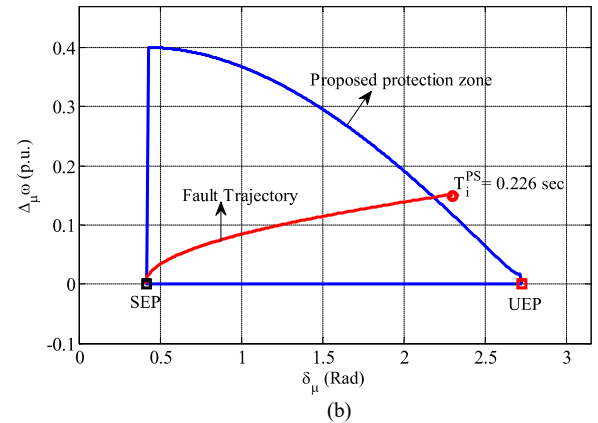
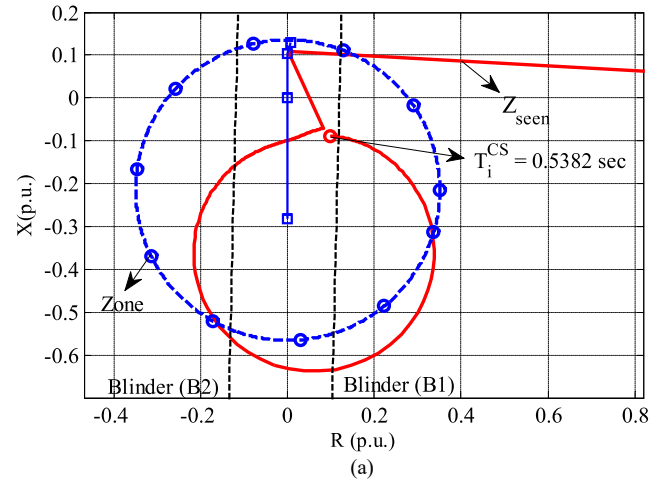


Fig. 13. Simulation results for Case II: a) CS b) PS.

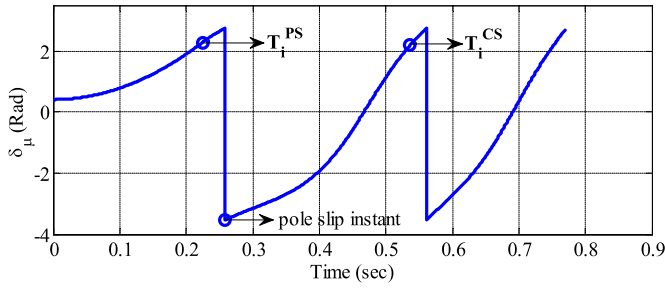


Fig. 14. Detection of dynamic security status by PS and CS.

To validate the PS adaptability, the simulation results are reported in Table III for various operating points of  $\mu$ G as well as fault clearing times. Here, the PS performance is compared with those of CS and undervoltage scheme [13], [28]. In Table III, PS can detect the dynamic security status in all listed cases. However, in most cases, the CS accuracy is of concern. For instance, in Case 4, the trip command is issued by the undervoltage scheme while the system status is secured. The dynamic security is maintained because the FCT associated with Case 4 is less than CCT. However, the undervoltage scheme utilizes the voltage amplitude as a protection index which may not provide a precise insight on security. One may apply the undervoltage scheme while using a setting that is adaptive with the loading level. Accordingly, CCT should be computed which may require more comprehensive time-domain simulation studies. Similar discussions apply to Cases 3, 8-9, and 16-23. This undesirable behavior renders the undervoltage scheme unreliable for the out-of-step protection in  $\mu$ Gs.

The proposed method offers out-of-step protection excluding CCT index. The CCT values in Table III are not used for relay setting; they are rather used to investigate the failure reasons of undervoltage and conventional schemes. According to Table III, CS has a better performance than the undervoltage scheme from a security point of view; however, in Cases 5, 9, and 20, CS fails to accurately identify the dynamic system status. Here, failures happen when FCT is close to CCT and the operating point is close to the border of security region. Accordingly, CS cannot offer a precise decision on security because the effect of IBDERs is not considered by CS. In addition, CS applications result in a slow detection of dynamic security status in Cases 6-7, 10-15, and 21-23. Considering these observations, we conclude that the  $\mu$ G out-of-step protection requirements are not often fulfilled by CS. In contrast, PS offers a mechanism for an accurate and fast detection of dynamic security status which considers the impact of IBDERs in  $\mu$ Gs.

TABLE III  
SIMULATION RESULTS

| LL <sup>1</sup> | Case | $P_m$ (MW) |       | CCT <sup>2</sup> | FCT <sup>3</sup> | ST <sup>4</sup> | Ti (ms) |     |                  |
|-----------------|------|------------|-------|------------------|------------------|-----------------|---------|-----|------------------|
|                 |      | $P_g$      | $P_c$ |                  |                  |                 | PS      | CS  | UVS <sup>5</sup> |
| I               | 1    | 2.5        | 1     | 218              | 150              | S <sup>6</sup>  | --      | --  | --               |
|                 | 2    | 2.5        | 1     |                  | 180              | S               | --      | --  | --               |
|                 | 3    | 2.5        | 1     |                  | 200              | S               | --      | --  | 200              |
|                 | 4    | 2.5        | 1     |                  | 210              | S               | --      | --  | 200              |
|                 | 5    | 2.5        | 1     |                  | 217              | S               | --      | 603 | 200              |
|                 | 6    | 2.5        | 1     |                  | 220              | U <sup>7</sup>  | 224     | 536 | 200              |
|                 | 7    | 2.5        | 1     |                  | 230              | U               | 224     | 499 | 200              |
| II              | 8    | 3.5        | 0.5   | 168              | 150              | S               | --      | --  | 200              |
|                 | 9    | 3.5        | 0.5   |                  | 167              | S               | --      | 600 | 200              |

|     |    |     |     |     |     |   |     |     |     |
|-----|----|-----|-----|-----|-----|---|-----|-----|-----|
| III | 10 | 3.5 | 0.5 | 320 | 180 | U | 175 | 443 | 200 |
|     | 11 | 3.5 | 0.5 |     | 200 | U | 175 | 383 | 200 |
|     | 12 | 3.5 | 0.5 |     | 210 | U | 175 | 372 | 200 |
|     | 13 | 3.5 | 0.5 |     | 217 | U | 175 | 365 | 200 |
|     | 14 | 3.5 | 0.5 |     | 220 | U | 175 | 365 | 200 |
|     | 15 | 3.5 | 0.5 |     | 230 | U | 175 | 360 | 200 |
|     | 16 | 1.5 | 2   |     | 200 | S | --  | --  | 200 |
|     | 17 | 1.5 | 2   |     | 220 | S | --  | --  | 200 |
|     | 18 | 1.5 | 2   |     | 250 | S | --  | --  | 200 |
|     | 19 | 1.5 | 2   |     | 280 | S | --  | --  | 200 |
|     | 20 | 1.5 | 2   |     | 300 | S | --  | 545 | 200 |
|     | 21 | 1.5 | 2   |     | 330 | U | 327 | 593 | 200 |
|     | 22 | 1.5 | 2   |     | 350 | U | 327 | 563 | 200 |
|     | 23 | 1.5 | 2   |     | 380 | U | 327 | 544 | 200 |

<sup>1</sup> Loading level, <sup>2</sup> Critical clearing time (ms), <sup>3</sup> Fault clearing time (ms), <sup>4</sup> Status, <sup>5</sup> Undervoltage scheme, <sup>6</sup> Secured, <sup>7</sup> Unsecured.

## V. CONCLUSIONS

This paper dealt with the detection of dynamic security status in  $\mu$ Gs through a three-stage adaptive protection approach. An effective model for the detection of dynamic security status of  $\mu$ Gs incorporating SGBDERs and IBDERs was presented. A new ROA-based protection zone was introduced for the detection of dynamic security status. The accuracy of the proposed model was verified by several simulations which also implied that the proposed scheme offers an adaptive behavior with respect to  $\mu$ G operating conditions. The proposed studies concluded that 1) The  $\mu$ G out-of-step protection requirements, including the speed and the accuracy for the detection of dynamic security status, are seldom fulfilled by conventional approaches including out-of-step and undervoltage schemes; 2) The proposed approach provides a quick detection of dynamic security status which often occurs prior to a pole slip incident; 3) ROA is an efficient index for measuring dynamic security and distinguishing secured from unsecured cases; and 4) The proposed scheme offers fast and accurate detection of dynamic security status considering the impacts of IBDERs on designated  $\mu$ Gs. An extension of the proposed scheme for preserving the dynamic security of hybrid AC/DC  $\mu$ Gs will be considered in our future work.

## REFERENCES

- [1] M. Shahidehpour and J. F. Clair, "A functional microgrid for enhancing reliability, sustainability, and energy efficiency," *The Electricity Journal*, vol. 25, no. 8, pp. 21-28, 2012.
- [2] A. Gholami, F. Aminifar, and M. Shahidehpour, "Front lines against the darkness: enhancing the resilience of the electricity grid through microgrid facilities," *IEEE Electr. Mag.*, vol. 4, no. 1, pp. 18-24, 2016.
- [3] L. Che, M. Khodayar, and M. Shahidehpour, "Only Connect: Microgrids for Distribution System Restoration," *IEEE Power Energy Mag.*, vol. 12, no. 1, pp. 70-81, 2014.
- [4] V. Madani *et al.*, "Distribution automation strategies challenges and opportunities in a changing landscape," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 2157-2165, 2015.
- [5] R. Das *et al.*, "Distribution automation strategies: evolution of technologies and the business case," *IEEE Trans. Smart Grid*, vol. 6, pp. 2166-2175, 2015.
- [6] L. Che, M. E. Khodayar, and M. Shahidehpour, "Adaptive protection system for microgrids: protection practices of a functional microgrid system," *IEEE Electr. Mag.*, vol. 2, no. 1, pp. 66-80, 2014.
- [7] S. Teimourzadeh, F. Aminifar, M. Davarpanah, and J. M. Guerrero, "Macroprotections for microgrids: toward a new



protection paradigm subsequent to distributed energy resource integration," *IEEE Ind. Electron. Mag.*, vol. 10, no. 3, pp. 6-18, 2016.

- [8] R. Majumder, "Some aspects of stability in microgrids," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3243-3252, 2013.
- [9] I. Xyngi, A. Ishchenko, M. Popov, and L. Van der Sluis, "Transient stability analysis of a distribution network with distributed generators," *IEEE Trans. Power Syst.*, vol. 24, no. 2, 2009.
- [10] R. Razzaghi, M. Davarpanah, and M. Sanaye-Pasand, "A novel protective scheme to protect small-scale synchronous generators against transient instability," *IEEE Trans. Ind. Electron.*, vol. 60, no. 4, pp. 1659-1667, 2013.
- [11] S. Teimourzadeh, M. Davarpanah, F. Aminifar, and M. Shahidehpour, "An adaptive auto-reclosing scheme to preserve transient stability of microgrids," *IEEE Trans. Smart Grid*, 2016, to be published.
- [12] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. NY, USA: McGraw-Hill, 1994.
- [13] D. Reimert, *Protective relaying for power generation systems*. Boca Raton, FL, USA: CRC Press, 2005.
- [14] "IEEE standard for interconnecting distributed resources with electric power systems," *IEEE Std 1547-2003*, pp. 1-28, 2003.
- [15] F. Iov, A. D. Hansen, P. E. Sorensen, and N. A. Cutulus, "Mapping of grid faults and grid codes," Riso Nat. Lab., Tech. Univ. Denmark, Roskilde, Denmark, Tech. Rep., 2007.
- [16] E. J. Coster, J. M. A. Myrzik, and W. L. Kling, "Influence of protection on transient stability of medium voltage grids including distributed generation," in *Proc. Univ. Power Eng. Conf.*, England, 2007, pp. 1054-1059.
- [17] H. Khalil, *Nonlinear Systems*. NJ, USA: Prentice hall, 2002.
- [18] S. H. Zak, *Systems and control*. NY, USA: Oxford university press, 2003.
- [19] J. Rocabert, A. Luna, F. Blaabjerg, and P. Rodriguez, "Control of power converters in ac microgrids," *IEEE Trans. Power Electron.*, vol. 27, no. 11, pp. 4734-4749, 2012.
- [20] S. D. Arco and J. A. Suul, "Equivalence of virtual synchronous machines and frequency-droops for converter-based microgrids," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 394-395, 2014.
- [21] Q. C. Zhong and G. Weiss, "Synchronverters: inverters that mimic synchronous generators," *IEEE Trans. Ind. Electron.*, vol. 58, no. 4, pp. 1259-1267, 2011.
- [22] Z. Shuai, Y. Hu, Y. Peng, C. Tu, and Z. J. Shen, "Dynamic Stability Analysis of Synchronverter-dominated Microgrid Based on Bifurcation Theory," *IEEE Trans. Ind. Electron.*, 2017, to be published.
- [23] N. Bottrell and T. C. Green, "Comparison of current-limiting strategies during fault ride-through of inverters to prevent latch-up and wind-up," *IEEE Trans. Power Electron.*, vol. 29, no. 7, pp. 3786-3797, 2014.
- [24] F. Katiraei, M. R. Iravani, and P. W. Lehn, "Micro-grid autonomous operation during and subsequent to islanding process," *IEEE Trans. Power Del.*, vol. 20, no. 1, pp. 248-257, 2005.
- [25] M. Barnes *et al*, "Real-world microgrids-an overview," in *Proc. IEEE Int. Conf. Syst. of Syst. Eng. (SoSE)*, 2007, pp. 1-8.
- [26] Feltes *et al*, J, "Review of existing hydroelectric turbine-governor simulation models," Argonne National Laboratory (ANL) 2013.
- [27] D. Lee, D. Baker, and K. Bess, "IEEE Recommended practice for excitation system models for power system stability studies," *IEEE Std 421.5-2005*, 2005.
- [28] I. Xyngi, A. Ishchenko, M. Popov, and L. v. d. Sluis, "Transient stability analysis of a distribution network with distributed generators," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 1102-1104, 2009.

## BIOGRAPHIES

**Saeed Teimourzadeh** (S'15) received the B.Sc. (Hons.) and M.Sc. (Hons.) degrees in electrical engineering from the University of Tabriz, Tabriz, Iran, in 2012 and 2014, respectively. He is currently pursuing the Ph.D. degree in the School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran. Since 2016, he has been a Research Associate with the Electrical and Computer Engineering Department at the Illinois Institute of Technology (IIT), Chicago, IL, USA. His research interests include microgrid protection, control and stability, and smart grid initiatives.

**Farrokh Aminifar** (SM'15) has been collaborating with the Robert W. Galvin Center for Electricity Innovation with the Illinois Institute of Technology, Chicago, IL, USA, since March 2009. He is currently an Assistant Professor with the School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran. His research interests include wide-area measurement systems, power system expansion planning and reliability assessment, and smart grid initiatives.

**Mahdi Davarpanah** received the M.Sc. and Ph.D. degrees in electrical engineering from the University of Tehran, Tehran, Iran, in 2005 and 2013, respectively. Currently, he is an Assistant Professor with the School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran. His research interests include power system protection, control, and transients.

**Mohammad Shahidehpour** (F'01) is a University Distinguished Professor, and the Bodine Chair Professor and Director of the Robert W. Galvin Center for Electricity Innovation at Illinois Institute of Technology, Chicago, IL, USA. He was a recipient of the IEEE PES Outstanding Power Engineering Educator Award. Dr. Shahidehpour is a member of the U.S. National Academy of Engineering and a Fellow of the American Association for the Advancement of Science (AAAS).