Resilient Control based Frequency Regulation Scheme of Isolated Microgrids Considering Cyber Attack and Parameter Uncertainties

[1*]Dillip Kumar Mishra, [2]Prakash Kumar Ray, [1]Li Li, [3]Jiangfeng Zhang, [1]M. J. Hossain, [2]Asit Mohanty

[1]School of Electrical and Data Engineering, University of Technology, Sydney, NSW 2007, Australia

[2]Department of Electrical Engineering College of Engineering and Technology, Odisha, 751003, India

[3]Department of Automotive Engineering, Clemson University, Greenville, SC 29607, United States

Corresponding author: *dkmishra@ieee.org

Abstract: Cyber-physical attacks and parameter uncertainties are becoming a compelling issue on load frequency control, directly affecting the resilience (*i.e.*, reliability plus security) of the microgrid and multi-microgrid systems enabled by internet of things and the fifth generation communication system. A resilient system aims to endure and quickly restore a system's transients during extreme events. Therefore, it is critically important to have a resilient system to evade the total system failure or blackout in order to make them attack-resilient. With this objective, this paper presents a resilience-based frequency regulation scheme in a microgrid under different operating conditions, such as, step and random change in load and different wind speed patterns. Furthermore, a cyber-attack model is considered in the problem formulation to make the system robust against external attacks. To protect against the cyber-attack and parameter uncertainties in the system, different control schemes are employed, and their robustness characteristics are compared through various performance indices. Besides, the proposed control schemes are validated through a real-time software synchronisation environment, *i.e.*, OPAL-RT. As noted, the proposed type-2 fuzzy proportional-integral-derivative based controller provides the most significant improvement in the dynamic performance for frequency regulation compared to that of the others under the cyber-attack and uncertainties.

Keywords: Cyber Attack, Distributed Generation, Fuzzy PID Controller, Frequency Regulation, Microgrid, Resilience

1. Introduction

The electric power industry is one of the most elementary infrastructures, which needs to be secure, reliable, and sustainable. Over the past few decades, the complexity of power systems has been increasing due to renewable energy penetration, demand-side management, and power system reconfiguration [1]. On the other hand, extreme events like natural disasters and cyber-attacks have been increasing in the last decade, eventually impacting on the power industry, affecting social and economic activities. As traditional power networks are largely interconnected, they are more vulnerable

in the wake of extreme events, including cyber-attacks [2]. The past decade has seen the rapid development of power system reconfiguration, where the main aim was to convert power systems from bulk power to small-scale networks like microgrids (MGs) and smart grids [3]. Further, the roles of communication and other advanced technologies are used to enhance the reliability of a power system. As noted, the MG and smart grid technology have become more reliable by employing communication and control technologies (for example, internet-of-things and 5G communication systems) that enable data exchange information. However, due to the open wireless intrusion interface, hackers can falsify the signals transmitted via vulnerable units (e.g., remote terminal units); consequently, cyber threats happen, resulting in disruption of system stability [4]. As far as the power system stability is concerned, the frequency is an essential component that needs to be maintained within rigid limits for stable operation [5]. It is noted that a large deviation of frequency can result in the collapse of the power system network. With the above concern, the hacker can inject malicious data at the load point, generation point, breaker, or controller point, leading to mismatch in the generation and load demand, turning in frequency instabilities and power outages [6].

As cyber-attacks have been increasing in the past few decades, subsequently, a growing amount of research has been carried out to defend against cybersecurity threats. Examples of cyber-attacks are the StuxNet virus in Iran's nuclear power station [7] and KillDisk malware in Ukraine power system [8]. Thus, serious security challenges need to be accepted in the energy sector. Concerning these challenges, more recent attention has focused on providing cyber-resilient systems through different control schemes and robust design approaches. In [9], the cyber-physical resiliency metric is proposed, where the Ukraine cyber-attack is taken as the case study. Besides, several other attack-based studies have been carried out involving load balance schemes [10], economic dispatch [11], and bad data identification [12]. Further, a large body of research has been focused on defense strategies against cyber-attack in the power system context, through event-triggered approach [13], adaptive control against denial-of-service attack [14], additional control loop in defiance of denial-of-service attack [15], and multi-layer game theory against false data injection attack [16].

With the recent developments in the energy sector, the concept of a cyber-physical system (CPS) is crucial in integrating cyber layers with the physical layer. This system plays a vital role in critical infrastructure, which has been built with emerging and future smart facilities and subsequently enhances the quality of life [17]. The physical layer comprises distributed energy resources such as intermittent renewable energy sources, electric vehicles (EVs), and energy storage devices. The cyber layer involves cybernetics, distributed control mechanisms, actuators, and other control and metering devices.

Clearly, the most widely used renewable sources such as solar and wind energies are intermittent in nature, which could inevitably impact system stability and, in certain instances, lead to power failure. Moreover, due to intermittencies and the incorporation of power electronic devices into the system, the frequency profile can be significantly disturbed, which is the leading cause of the power failure. In the course of small frequency deviation, the participation of electric vehicles (EVs) and energy storage

devices could meet the load demand requirements and help in frequency stabilization [18]. However, it might fail to maintain grid stability in the aftermath of cyber-attack and parameter uncertainties [19].

Thus, to maintain grid stability, a proper control strategy should be adopted. Several techniques have been proposed to show the significance of control theory and its extensive applications to frequency control in the context of cyber-attacks, such as a secondary frequency control scheme under the latency attack [20], attack tolerant frequency regulation [21], delayed inputs threats-based design [22], a switching system-based frequency regulation scheme under the denial-of-service attacks [23], event triggering approaches [24]. Notably, the aforementioned studies achieved satisfactory control performance characteristics with certain limitations. However, concerning the CPS in frequency control design, renewable energy sources are essential and must be operated securely to meet the load requirement irrespective of their input variation. Thus, considering intermittencies and cyber-threat control mechanisms in a single framework is of utmost need, which is addressed in this paper.

An adaptive control method needs to be investigated to provide a resilient frequency control scheme by considering the cyber-threats and renewable uncertainties. Due to the advancement of control theory application, fuzzy logic control technique is introduced, which offers the ability to cope with uncertainties and various disturbances, including cyber-attacks. The type-1 fuzzy logic method has achieved a broader application area due to its coping capability with linguistic uncertainty generation. However, it is not suitable for dynamic uncertainties. Moving further fuzzy control, a type-2 fuzzy method has evolved, which can be used in a non-linear physical system. As noted from the literature, the type-2 fuzzy logic method has considerably enhanced performance in terms of stability [25, 26], uncertainties [27], and detection [28]. In addition, it offers a better cyber-attack control mechanism which is the main contribution to resiliency [29, 30]. More recently, literature has emerged that provides a load frequency control (LFC) scheme through fuzzy logic, which can be seen in [31-33]. These studies have certain limitations, such as not considering CPS, cyberattack scenarios, and parameter uncertainties. In order to make the system resilient in the context of LFC, all these factors need to be considered to show real-world phenomena, which are especially significant.

In this paper, type-1 and type-2 fuzzy logic control are applied for comparing their performance characteristics. Moreover, this study contributes to the cyber-resilience control-based frequency regulation scheme through the fuzzy logic method. This study aims to elucidate a type-2 fuzzy logic control-based resilient frequency regulation scheme in isolated MGs (IMGs) under parameter uncertainties and cyber-attack. It can help power system engineers understand the scenarios intuitively and the importance of proper control actions according to the available information (such as frequency, load data, and generation data) to ensure resiliency. The key contributions of this paper are as follows.

- Presenting a cyber-resilient frequency regulation scheme for IMGs considering cyber-attack, variation of solar insolation, and wind speed patterns.
- Quantifying the impact of the cyber-attack model with different uncertainties on the frequency deviation of IMGs using adaptive fuzzy logic methods.

- Studying the stability of the proposed system through the frequency domain approach and statistical analysis.
- Finally, validating the proposed system through the real-time simulation platform using OPAL-RT to show the effectiveness of the proposed controller with regard to resiliency.

The remainder of the paper comprises five sections. The paper begins with the introduction section, followed by the system modeling in Section 2. Thereafter, the simulation results are discussed in Section 3. Further, the extension of simulation work is validated through a real-time platform, presented in Section 4. Finally, Section 5 gives a brief conclusion and the scopes for future work.

2. System Configuration and Modeling

2.1. Microgrid Model

In this work, an interconnected microgrid is considered a physical system, and the sensory network is termed a cyber system as shown in Fig. 1. This study aims to show the microgrid's robustness as a means of the cyber-resilient system to evade the power system blackout and provide a stabilized frequency deviation profile considering the uncertainties and cyber-attack. With this objective, the proposed system is designed with two renewable sources (PV and wind), two storage units (flywheel energy storage devices (FESS) and battery energy storage devices (BESS)), an aggregated electric vehicle (EV), along with a diesel generator (i^{th} control area LFC scheme can be seen in Fig. 2). Besides, the distributed management system (DMS) is employed in the control center to coordinate the MG data and communicate the state information. Further, the sensory network is used to receive the signals from the output (i.e., frequency signal), and then to give a command to the actuator to change the generation accordingly to minimize the load demand-generation imbalance through set points, which can be done by the controller with tuned values. An attack model is considered in this work, which is able to change the area control error that could lead to a change in the frequency deviation significantly. Consequently, the system goes into an unstable zone. However, the countermeasure is taken to evade the system failure, and the frequency deviation is forced to zero or a negligible value through different control actions. The detailed modelling of the proposed system is as follows.

The wind power is modelled with (1) and (2) [34]. Eq. (1) represents the electric power output ($\mathcal{P}_W$) from the mechanical power, and Eq. (2) signifies the power output according to the wind speed ($\mathbb{w}_s$) in relation to the rated ($\mathbb{w}_{rated}$), cut-in ($\mathbb{w}_{cut-in}$), and cut-out wind speed ($\mathbb{w}_{cut-out}$), where ρ, $\mathcal{A}_s, \mathcal{C}_p$, $\mathbb{w}_s$, and $\mathcal{P}_{rated}$ are the air density in kg/m^3, blade swept-area in m^2, power coefficient, wind speed in m/s, and rated wind power in kW, respectively.

$$\mathcal{P}_W = \frac{1}{2} \times \rho \times \mathcal{A}_s \times \mathcal{C}_p \times \mathbb{w}_s^3 \tag{1}$$

$$\mathcal{P}_W = \begin{cases} 0, & \mathbb{w}_s < \mathbb{w}_{cut-in} \text{ or } \mathbb{w}_s > \mathbb{w}_{cut-out} \\ \mathcal{P}_{rated}, & \mathbb{w}_{rated} \le \mathbb{w}_s \le \mathbb{w}_{cut-out} \\ 0.01312\mathbb{w}_s^6 - 0.04603\mathbb{w}_s^5 + 0.3314\mathbb{w}_s^4 + 3.687\mathbb{w}_s^3 - 51.1\mathbb{w}_s^2 & \\ +2.33\mathbb{w}_s + 366 & \text{else} \end{cases} \quad (2)$$

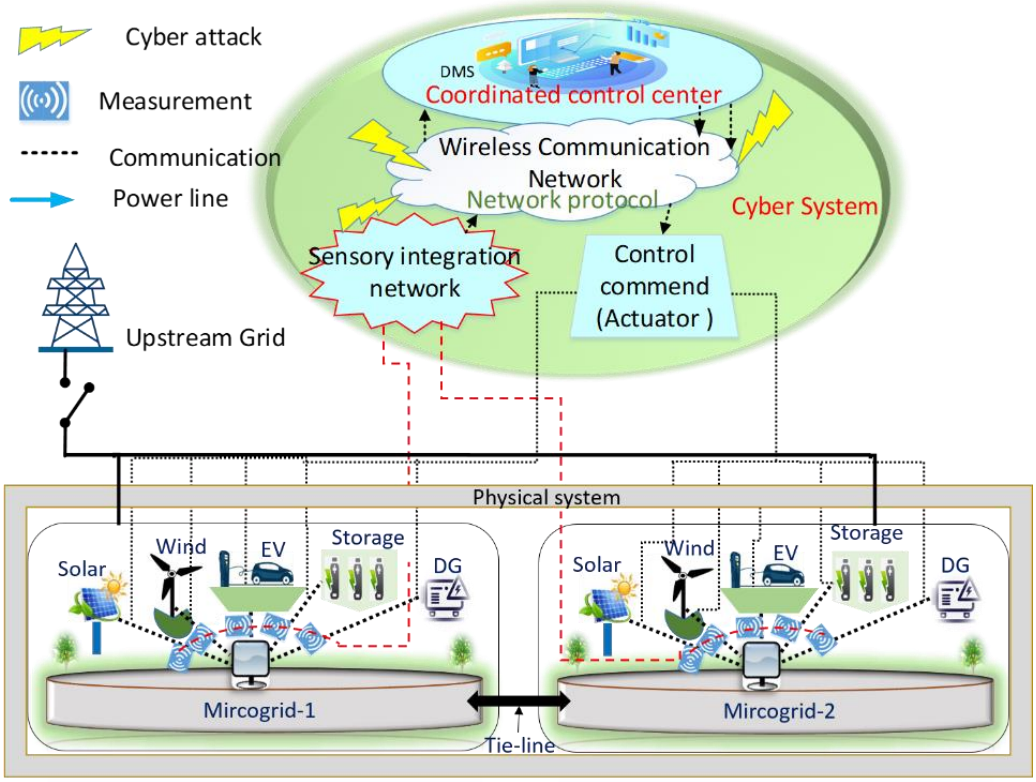


Fig. 1. Cyber-physical system

The PV system comprises the combination of series and parallel cells to provide the required voltage and current. The PV panel output depends on the solar insolation, which is a non-linear relationship with the PV current. Accordingly, the PV output ($\mathcal{P}_{PV}$) can be presented in (3), where $\eta, \emptyset, \mathcal{A}_m$, θ_A, $\mathcal{P}_{PV}$ are the PV array conversion efficiency, solar insolation in kW/m^2, area of measurement in m^2, and ambient temperature in ℃, PV output in kW, respectively.

$$\mathcal{P}_{PV} = [1 - 0.005\ (\theta_A + 25)]\eta \times \emptyset \times \mathcal{A}_m \quad (3)$$

The equivalent EV model [35] is considered in this study, where a number of EVs are charged at an EV fast-charging station, *i.e.*, vehicle-to-grid, is not considered. The total capacity of the aggregated EVs can be estimated as in (4) and expanded in (5), where the control time period is sampled by $\Delta\, t$, t represents a sampled time period, $\mathcal{P}_{EV}(t)$ denotes the total charging power at the station, $\mathcal{N}_{con}(t)$ is the numbers of connected EVs charging at this station at time t; $\mathcal{P}_{EV\_inv}$ is the average charging power at each charging point of this station (e.g., 50~150kW), initial numbers of charging EVs at time t_0 is represented as $\mathcal{N}_{ini}(t_0)$; newly connected EVs at time t are as $\mathcal{N}_{con\_in}(t)$, and the number of disconnected EVs is symbolized as $\mathcal{N}_{plug\_out}(t)$.

$$\mathcal{P}_{EV}(t) = \mathcal{N}_{con}(t) \times \mathcal{P}_{EV\_inv} \quad (4)$$

$$\mathcal{N}_{con}(t) = \mathcal{N}_{con}(t-1) + \mathcal{N}_{con\_in}(t) - \mathcal{N}_{plu\_out}(t) \quad (5)$$

$$= \mathcal{N}_{ini}(t_0) + \sum_{j=t_0+1}^{t} (\mathcal{N}_{con\_in}(j) - \mathcal{N}_{plu_{out}}(j))$$

Assume that each EV is charged for roughly the same time duration at this station with the same charging power $\mathcal{P}_{EV\_inv}$, and denote this averaged charging time as $k\Delta t$ (*e.g.*, 30 minutes). Then the amount of energy charged at time interval t is calculated as follows.

$$E_{EV}(t) = \mathcal{N}_{con}(t) \times \mathcal{P}_{EV\_inv} \times k\Delta t$$

Further, a storage device such as FESS stores the kinetic energy and the energy density, *i.e.*, $\mathcal{W}_{vol}$ is given in (6), where $\sigma_r = \varrho_m (l \times \omega_m^2)$. This design concept was modelled through a rotating flywheel rotor, which stores mechanical energy and then converts it into electrical energy. Eq. (7) gives the flywheel's kinetic energy, followed by (8) representing the maximum stored energy value. In (6)-(8), the parameters are the radial tensile stress (σ_r), material density (ϱ_m), circular path radium (l), spinning angular speed (ω_m), flywheel shape ($\mathcal{K}_F$), flywheel volume ($\mathcal{V}$), angular velocity (ω_{FH}), inertia ($\mathcal{J}$), and maximum tensile stress (σ_{r_Max}). Besides, the BESS and diesel generator are also incorporated into the system for load balancing, nullification of harmonics, and further improving the emergency voltage/frequency profile.

$$\mathcal{W}_{vol} = \frac{1}{2} \times \mathcal{K}_F \times \sigma_r \quad (6)$$

$$\mathcal{W}_{FESS} = \frac{1}{2} \times \mathcal{J} \times \omega_{FH}^2 \quad (7)$$

$$\mathcal{W}_{FESS\_Max} = \frac{1}{2} \times \mathcal{K}_F \times \mathcal{V} \times \sigma_{r\_Max} \quad (8)$$

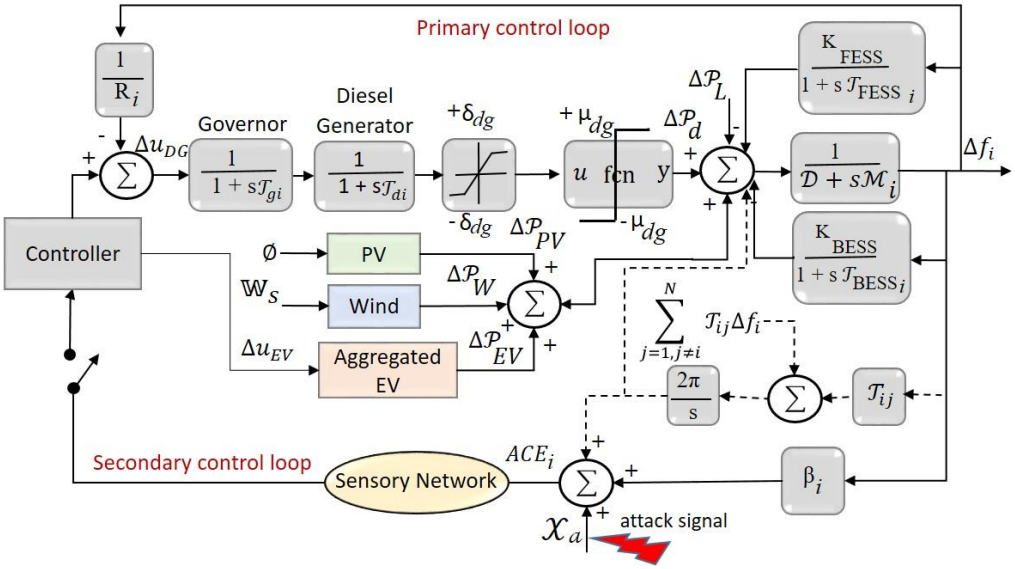


Fig. 2. LFC scheme of the i^{th} control area

The self-healing microgrid system is modelled in this section by implementing the wind, PV, EV, BESS, FESS, and the load unit, as shown in Fig. 2. It is represented in (9)-(13) as the linear state-space model in (9)-(10), followed by (11)-(13).

$$\dot{x}(t) = Ax(t) + Bu(t) + \mathcal{W}(t) \quad (9)$$

$$x^T(t) = [\Delta\mathcal{P}_{PV}\ \ \Delta\mathcal{P}_d\ \ \Delta\mathcal{P}_W\ \ \Delta\mathcal{P}_{EV}\ \ \Delta\mathcal{P}_{BESS}\ \ \Delta\mathcal{P}_{FESS}\ \ \Delta f] \quad (10)$$

$$y\,(t) = Cx(t) + Du(t) \quad (11)$$

$$\mathcal{W}^T(t) = [\,\Delta\mathcal{P}_L\ \mathfrak{B}_C] \quad (12)$$

$$y(t) = \Delta f \text{ and } u(t) = [\Delta u_d\ \ \Delta u_{EV}]^T \quad (13)$$

where $x, u, y, \mathcal{W}$ are the state, control input, output and disturbance variables; A, B, C, D are the state, input, output and feedthrough matrices; $\mathcal{P}_d$, $\mathcal{P}_{PV}$, $\mathcal{P}_W$, $\mathcal{P}_{EV}$, $\mathcal{P}_{BESS}$, $\mathcal{P}_{FESS}$, and $\mathcal{P}_L$ represent the diesel generator, solar, wind, electric vehicle, FESS, BESS and load dynamics, respectively; $\mathfrak{B}_C$ denotes the cyber-attack signal, regarded as the disturbance to the system, which can be $\mathcal{X}_a$ in Fig. 2 or a random cyber-attack pattern; Δu_d and Δu_{EV} represent the control input to the diesel generator and EV, respectively; the symbol Δ denote the change of variable from its nominal value; f is the frequency.

The total generation of the system ($\mathcal{P}_G$) can be presented as in (14), and then the balance between generation and load demand ($\Delta\mathcal{P}_e$) can be expressed in (15). In (14), $\mathcal{P}_{FESS}$ and $\mathcal{P}_{FESS}$ can be positive or negative, indicating storing or releasing the energy, respectively. The power balance equation of the LFC system can be presented as (16), followed by the system transfer function in (17). Then, the tie-line power change is represented in (18) [36, 37]. Finally, the objective function (obj) of the proposed system as an error function, *i.e.*, $ACE_i\ (t)$, is represented in (19).

$$\mathcal{P}_G = \mathcal{P}_W + \mathcal{P}_{PV} + \mathcal{P}_{EV} + \mathcal{P}_d + \mathcal{P}_{FESS} + \mathcal{P}_{BESS} \quad (14)$$

$$\Delta\mathcal{P}_e = \mathcal{P}_G - \mathcal{P}_L \quad (15)$$

$$\Delta f = \frac{\Delta\mathcal{P}_e}{Ms + D} \quad (16)$$

$$\mathcal{G}_{Sys} = \frac{\Delta f}{\Delta\mathcal{P}_e} = \frac{1}{Ms + D} \quad (17)$$

$$\Delta\mathcal{P}_{tie}^{i} = \sum_{\substack{j=1,\\ j\neq i}}^{\mathcal{N}} \Delta\mathcal{P}_{tie}^{ij} = \frac{2\pi}{s}\left[\sum_{j=1, j\neq i}^{\mathcal{N}} \Delta\mathcal{T}_{ij}\Delta f_i - \sum_{j=1, j\neq i}^{\mathcal{N}} \Delta\mathcal{T}_{ij}\Delta f_{ij}\right] \quad (18)$$

where $\mathcal{T}_{ij}$, D, and M signifies the synchronizing coefficient, equivalent damping constant, and equivalent inertia constant of the system; $\Delta\mathcal{P}_{tie}^{i}$ and $\mathcal{N}$ are the tie-line power flow exchange and the number of areas that are interconnected in the system, respectively.

$$ACE_i\ (t) = \beta_i\Delta f_i(t) + \sum_{j=1, j\neq i}^{\mathcal{N}} a_{ij}\Delta\mathcal{P}_{tie}^{ij}(t) \quad (19)$$

where $a_{ij} = \mathcal{P}_{ri}/\mathcal{P}_{rj}$ denotes the area capacity factor, $\mathcal{P}_{ri}$ and $\mathcal{P}_{rj}$ are the power capacities of the i-th and j-th areas, correspondingly, and ACE is the area control error.

The first term of (19) denotes per unit (pu) values in terms of frequency bias parameter (β in pu/Hz) and area frequency (Δf_i in Hz), where i is the index of the area. The second term denotes the pu values

of exchange power in terms of the area capacity factor (pu) and tie-line power (pu). Further, the dynamic model of an individual system can be expressed as follows in (20-24)[38].

$$\Delta\dot{f}_i(t) = \frac{1}{\mathcal{M}_i}\Delta\mathcal{P}_{di}(t) + \frac{1}{\mathcal{M}_i}\Delta\mathcal{P}_{PVi}(t) + \frac{1}{\mathcal{M}_i}\Delta\mathcal{P}_{Wi}(t) + \frac{1}{\mathcal{M}_i}\Delta\mathcal{P}_{EVi}(t) - \frac{1}{\mathcal{M}_i}\Delta\mathcal{P}_{Li}(t) - \frac{\mathcal{D}_i}{\mathcal{M}_i}\Delta f_i(t) \quad (20)$$

$$\Delta\dot{\mathcal{P}}_{di}(t) = \frac{1}{\mathcal{T}_{di}}\Delta u_{DGi}(t) - \frac{1}{\mathcal{T}_{di}}\Delta\mathcal{P}_{di}(t) \quad (21)$$

$$\Delta\dot{\mathcal{P}}_{PVi}(t) = \frac{1}{\mathcal{T}_{PVi}}\Delta\emptyset_i(t) - \frac{1}{\mathcal{T}_{PVi}}\Delta\mathcal{P}_{PVi}(t) \quad (22)$$

$$\Delta\dot{\mathcal{P}}_{Wi}(t) = \frac{1}{\mathcal{T}_{Wi}}\Delta\mathbb{W}_{si}(t) - \frac{1}{\mathcal{T}_{Wi}}\Delta\mathcal{P}_{Wi}(t) \quad (23)$$

$$\Delta\dot{\mathcal{P}}_{EVi}(t) = \frac{1}{\mathcal{T}_{EVi}}\Delta u_{EVi}(t) - \frac{1}{\mathcal{T}_{EVi}}\Delta\mathcal{P}_{EVi}(t) \quad (24)$$

2.2. ***Environmental uncertainties***

This study considers two types of environmental uncertainties, that is, solar insolation, and wind speed, which are vital for a reliable power supply with large-scale renewable generation. In addition, a continuous load change has been considered. As far as the load demand is concerned, practically, it is not constant, and so the change in load demand should be considered while designing the microgrid. Furthermore, two other uncertainties, such as solar insolation and wind speed, could affect the frequency response leading to microgrid failure [39]. Although the system can cope with the environmental uncertainties, however, in the event of a cyber-attack along with uncertainties, the magnitude of frequency deviation can be large, which may lead to collapse of the entire system, or a blackout. Nowadays, the cyber-physical power system is emerging since various sensor technologies, advanced control methods, and communication techniques are used to enhance the resiliency for consumers [40]. However, it is more vulnerable as it will be easy for a hacker to falsify the signals. Thus, all these considerations are significant while designing the microgrid. Further, a suitable control method for achieving stable operation in the microgrid is required to cope with uncertainties and cyber-related issues.

2.3. Cyber-attack

In the last few decades, the risk and severity of cyber-threat phenomena have considerably increased in the power system sector, as discussed in Section 1. Moreover, in an LFC system, two critical parameters, *i.e.*, frequency and tie-line power, are significantly important and potentially targeted by hackers. The hacker can falsify these parameter values to make the system more vulnerable through communication channels. Moreover, the attack can be made through the cyber layer or the physical layer (system or plant), where data-exchange information or other communications are being handled. Considering the cyber layer attack, it can be a data integrity attack or denial of service attack [14, 41].

On the other hand, considering the physical layer attack, the load can be changed to make the frequency unstable via an internet-based or direct approach termed a resonance attack [6]. Under the data integrity attack, the hacker can

- replace the measurement value known as replay attack;
- falsify the actual signal known as false data injection attack;
- cancel the effect of attack by estimating the system's output, and then subtracting it from the estimation reading known as covert attack.

Further, a false data injection attack is classified into two types: extraneous attack and scaling attack, as discussed below.

i. *Extraneous attack:* Considering the extraneous attack, hackers can attempt to add the disturbance signal as $\mathcal{X}_a$ at the sensor point, which will increase the magnitude of ACE. With this, the actual frequency can be greater/ less than the nominal frequency, which will cause system instability. In this type of attack, the measured value ($\mathcal{M}_{mea}$) is the addition of actual value ($\mathcal{M}_{actual}$) and disturbance signal ($\mathcal{X}_a$), as given in (25). The disturbance can be signum, sinusoidal, ramp, step, or random signal.

$$\mathcal{M}_{mea} = \mathcal{M}_{actual} + \mathcal{X}_a \tag{25}$$

ii. *Scaling attack:* In this type of attack, the hacker can attempt to modify the actual measurements to higher or lower values depending on the scaling attack constant ($\mathcal{K}_a$), which significantly impacts the difference between the load demand and generation. The actual value of the measurement can be multiplied by the attack parameter, as expressed in (26).

$$\mathcal{M}_{mea} = \mathcal{K}_a \times \mathcal{M}_{actual} \tag{26}$$

where, $\mathcal{K}_a$ is the scaling attack constant.

In this paper, the extraneous attack is considered in two forms; one is the cyber-attack pattern-1 ($\mathcal{X}_a$), as expressed in (27) and shown in Fig. 3(b), and the other one is cyber-attack pattern-2 as a random signal presented in Fig. 3(c), which can be placed before the actuator. These two attacks are considered in this work, and for counterbalance, a secondary controller is employed, designed through the fuzzy logic approach. The attack input of pattern-1 is given as $\mathcal{X}_a$, where the y_i is the system output as a function of frequency (Δf). The given cyber-attack model ($\mathcal{X}_a(t)$) is taken from [6], where it was applied at the load point; however, it is applied at the sensor point in this study.

$$\mathcal{X}_a(t) = -0.3 \times sign\left(y_i(t-0.25)\right) \tag{27}$$

$$sign\,(p) = \begin{cases} 1, & p > 0; \\ -1, & p \leq 0; \end{cases}$$

For instance, let the output signal generated from a signal generator be a sine wave with a delay component of 0.25. Further, a simple Matlab program can be embedded in the system to make a new signal referred to as a cyber-attack in this study, as shown in Fig. 3 (a-b).

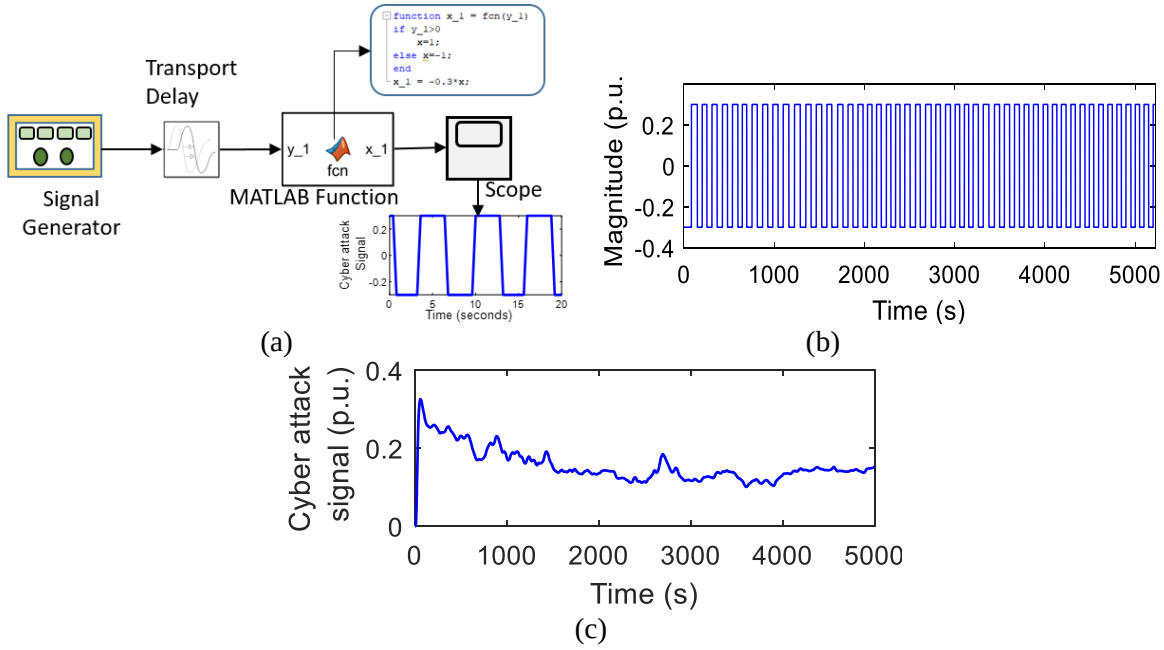


Fig. 3. Cyber-attack (a) signal generation, (b) pattern-1 generated from Fig. 3 (a), (c) pattern-2 as a random signal

With the cyber-attack signal, Eq. (19) can be modified as (28).

$$ACE_{i\_m}(t) = \beta_i \Delta f_i(t) + \sum_{j=1, j\neq i}^{N} a_{ij} \Delta \mathcal{P}_{tie}^{ij}(t) + \mathcal{X}_a(t) \tag{28}$$

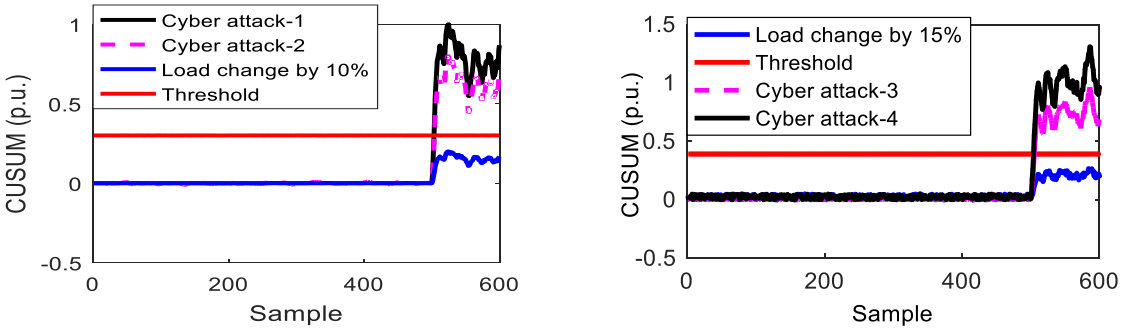
where $\mathcal{X}_a(t)$ is the cyber attack signal in (27).

Generally, the LFC system has been studied with the presumption of load deviation, which is very frequent. However, little attention has been paid to cyber-attack on the LFC system. The issue has grown in importance in light of major power outages due to cyber-attack such as Ukraine and Iran power plant attacks. Therefore, this study considers the cyber-attack as well as the load disturbance on the LFC system. To distinguish the level of fault whether the system is affected by load change or due to cyber-attack, the cumulative sum ($CUSUM$) based detection scheme is applied in this study. The $CUSUM$ checks the threshold value, either it is greater or lower, through the routine calculation of the difference between the current sample and the preceding sample. During steady-state, the sample difference is presumed to be zero or fixed [42]. However, in the wake of events, either load deviation or cyber-attack, the deviation in frequency and the corresponding $CUSUM$ will be dramatically high, which is discussed as follows. Eqs. (29) and (30) denote two complementary signals as current samples required for disturbance detection.

$$\mathcal{D}_{\hbar} = \mathcal{S}_{\hbar} \tag{29}$$

$$\mathcal{D}_{\hbar-1} = -\mathcal{S}_{\hbar} \tag{30}$$

where $\mathcal{S}_{\hbar}$ denotes the sample value of the signal at $\hbar^{th}$ time.



(a) (b)

Fig. 4. $CUSUM$

Using the signals mentioned above, the two-sided $CUSUM$ assessment is estimated as in (31) and (32).

$$\mathcal{G}_{k\_current} = max\left(\mathcal{G}_{k\_1\_current} + \mathcal{D}_{k} - \mathfrak{D}, 0\right) \quad (31)$$

$$\mathcal{G}_{k\_preceding} = max\left(\mathcal{G}_{k\_1\_preceding} + \mathcal{D}_{k-1} - \mathfrak{D}, 0\right) \quad (32)$$

where $\mathcal{G}_{k}$ and $\mathfrak{D}$ signifies the test statistics and drift parameter, respectively; $\mathcal{G}_{k\_current}$ and $\mathcal{G}_{k\_preceding}$ are the $CUSUM$ test value of the current and preceding signal with and without the inception of fault. In this case, if the cyber-attack happens, the $\mathcal{G}_{k}$ value will exceed the threshold value ($\mathcal{H}$), as given in (33).

$$\mathcal{G}_{k\_current} > \mathcal{H} \text{ or } \mathcal{G}_{k_{preceding}} > \mathcal{H} \quad (33)$$

It is noted that the value of $\mathcal{H}$ ought to be ideally zero.

As shown in Fig. 4, the output signal is sampled, where both steady-state and disruptive events are taken. It is revealed that when the load changes by 10% or 15%, the $CUSUM$ value is lower than the threshold. However, with cyber-attack, it increases significantly and exceeds the threshold value that is selected based on the comparison of estimated $CUSUM$ in different scenarios.

2.4.Control methods

As noted, frequency stabilization is vital to evade grid failure, and the regulation can be made through primary and secondary control. The primary control is the local control with a faster timescale through automatic feedback action, e.g., the governor and the secondary controller can be used to a wider network with a slower timescale through quasistatic control action. However, on the verge of a cyber-attack, the hacker can falsify the signal to mismatch the load demand-generation value, leading to an unstable grid or blackout. To this end, the secondary controller is vital and is a promising solution to avoid grid outages. With this objective, three different control methods have been incorporated and compared. From comparison, it is found that the T2FPID controller gives better performance, which is also validated through a real-time emulator, which verifies the controller effectiveness. A type-2 fuzzy logic method is significant in a complex, non-linear system, can control linguistic uncertainties, and is suitable for frequency attenuation with cyber-attack. In addition, it offers higher-degree-of freedom for better representation of uncertainty compared to the Type-1 fuzzy method. On the other hand, the upper and lower membership functions of the Type-2 fuzzy set may be used simultaneously in computing

each bound of the type-reduced interval. With these advantages, the Type-2 fuzzy method gives better transient performance against parameter uncertainties and cyber-attack. Furthermore, a PID controller is adopted, and an optimal value of the gains of the controller has been used to improve the system performance. It is assumed that the type-2 fuzzy PID controller is incorporated via two inputs of fuzzy logic, which will control the performance in both transient and steady-state outcomes for IMGs. The following sub-section discusses the secondary controllers, such as PID, type-1 fuzzy PID, and type-2 fuzzy PID, which are modelled and tested through the proposed system.

2.4.1. Method-1: PID controller

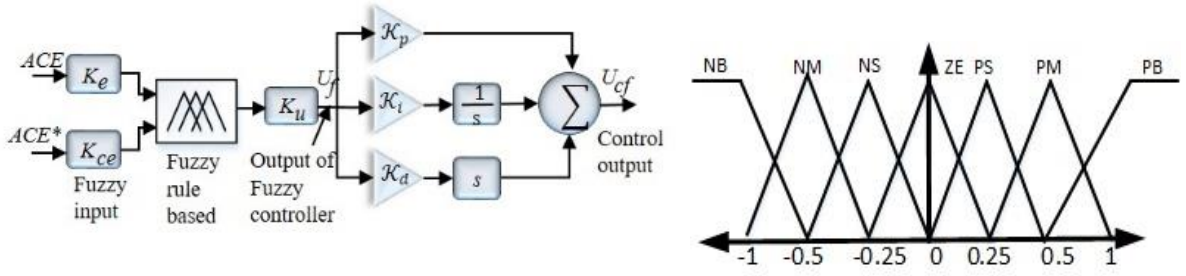
PID controller is a simple and effective control scheme that is popular for industrial use [43]. The output of the PID controller in the time-domain can be expressed as (34), where $u(t)$ is the control signal, and correspondingly, *e(t)* is the error signal.

$$u(t) = \mathcal{K}_p e(t) + \mathcal{K}_i \int_0^t e(\tau)d\tau + \mathcal{K}_d \frac{de(t)}{dt} \tag{34}$$

The role of the PID gains are: proportional gain ($\mathcal{K}_p$) responds to error response to disruption; integral gain ($\mathcal{K}_i$) minimizes the steady-state error, and derivative gain ($\mathcal{K}_d$) responds to transient behavior. However, this simple PID controller could not provide the frequency stabilization in the wake of extreme events. Therefore the advanced control methods are needed discussed as follows.

2.4.2. Method-2: Type-1 Fuzzy

The type-1 fuzzy-PID (T1FPID) controllers are widely used in control methods since traditional controllers are less efficient and more sluggish. Unlike the traditional controllers, which are premised on the basis of a linearized mathematical model, the fuzzy logic approach attempts to determine the control outputs directly from the measurements by the operators or users. Several studies have been attempted in LFC; for example, *Bevrani et al*. applied the fuzzy logic control scheme in LFC considering the wind power fluctuation and successfully minimized the system frequency and tie-line deviation [44]. In [45], the Fuzzy PI controller is used and also compared with the traditional PI controller, where it shows better frequency regulation characteristics.



(a) (b)

Fig. 5. (a) T1FPID structure, (b) Membership function

The structure of T1FPID is presented in Fig. 5 (a), where three main stages are included, namely fuzzification, rule base, and defuzzification. Further, the fuzzifier allocates the membership function

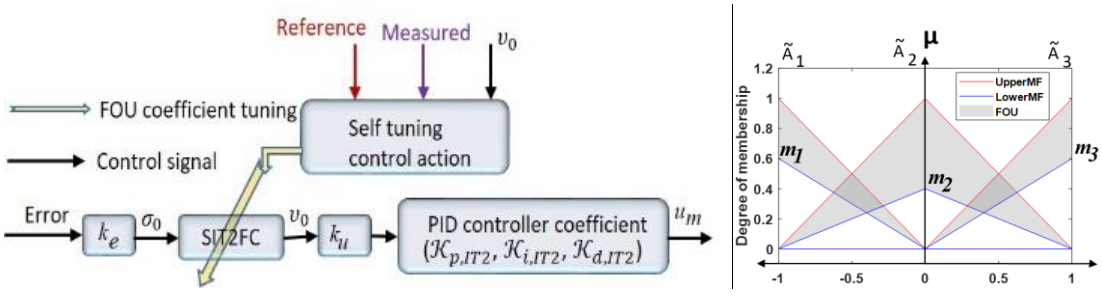
(MF) scales to the input and output variables as shown in Fig. 5 (b). It has been considered as Negative Big (NG), Negative Medium (NM), Negative Small (NS), Zero, Positive Big (PB), Positive Medium (PM), Positive Small (PS), having the values -1, -0.5, -0.25, 0, 1, 0.5, 0.25, respectively. In this structure, triangular MFs have been selected as it is a simple and easy tuning process.

The input of T1FPID is *ACE* and *ACE** (which is a derivative function of *ACE*), and out of fuzzy is U_f. Further, the control output of fuzzy is the input of the PID controller, and then the output of the T1FPID controller is U_{cf} and the output of fuzzy control (U_f) is the function of K_e, and K_{ce}, such as $U_f = f_{flc}(K_e\ ACE, K_{ce}\ ACE^*)$, where K_e and K_{ce} are the scaling parameters, and f_{flc} is the function of the fuzzy logic system.

2.4.3. Method-3: Type-2 Fuzzy-PID controller

Although the type-1 fuzzy has an excellent control characteristic, it is less significant in an unstructured environment because it cannot control linguistic uncertainties. Thus, to overcome the T1FPID limitation, the type-2 fuzzy PID controller (T2FPID) is adopted in this paper, which offers higher-degree-of freedom accomplished by the footprint of uncertainty. Indeed, the type-2 fuzzy controller is designed with two inputs, which are mostly used; however, some authors have developed a single input type-2 fuzzy controller (SIT2FC), which gives enhanced control performance and is simple in design [46]. This controller's main objective is to minimize the fluctuation of system frequency, and consequently, the error can also be decreased.

$$u_m = \mathcal{K}_u\left(\mathcal{K}_{p,IT2}v_0 + \mathcal{K}_{i,IT2}\int_0^t v_0\,dt + \mathcal{K}_{d,IT2}\frac{dv_0}{dt}\right) \tag{35}$$



(a) SIT2FC structure (b) triangular MFs of SIT2FC

Fig. 6. Type-2 Fuzzy

A traditional PID controller is cascaded to the T2FPID, which is inherited from three type-2 fuzzy mappings, shown in Fig. 6(a), and Fig. 6(b) represents the membership function. The input scaling factor k_e normnalizes the input, and is defined as $k_e = \frac{1}{e_{max}}$, where e_{max} denotes the maximum error. In this normalization, the antecedent membership functions are specified as [-1, 1]. In this structure, triangular type MFs ($\tilde{A}_i$) have been selected. Since the error is the frequency deviation, which will go through the scaling factor, it is converted into another factor as the input to a SIT2FC, *i.e.*, σ_0. Further, the control action denoted as u_m is regulated through the output of the controller, symbolized as v_0. Thus, the control action can be expressed as in (35), where $k_u = k_e^{-1}$ is the output of the scaling factor

and $\mathcal{K}_p$, $\mathcal{K}_i$ and $\mathcal{K}_d$ are the gains of the PID controller. The rule of the proposed type-2 fuzzy structure can be seen in (36).

$$\mathfrak{R}_i = "if\ \ \sigma \text{ is } \tilde{A}_i, \text{then } \mathcal{K} \text{ is } \mathcal{C}_i" = 1,2,3 \quad (36)$$

where $\mathfrak{R}$ and $\mathcal{C}$ define the rule and crisp value. The value of $\mathcal{C}_1, \mathcal{C}_2$, and $\mathcal{C}_3$ are -1, 0 and 1, respectively. Further, $\bar{\mu}\tilde{A}_i$ and $\underline{\mu}\tilde{A}_i$ are denoted as the upper and lower MFs, which offer an extra degree of freedom named as a footprint of uncertainty. This paper considers the symmetrical MFs, such as, $m_1 = m_3 = 1 - \Omega$ and $m_2 = \Omega$. The height of the lower MFs is scaled as 0.6, 0.4, and 0.6, corresponding to m_1, m_2, and m_3, respectively.

3. Case Study and Results

3.1. Simulation results

This section presents the transient analysis of the interconnected microgrid considering the step load, random load, and considering uncertainties like solar insolation, wind speed, and cyber-attack. In addition, three control methods are employed, such as conventional PID (CPID), T1FPID, and T2FPID controllers, and finally, the comparison characteristics are analyzed to identify the better controller. The interconnected MG system is simulated through the MATLAB/ Simulink environment, and the parameters of the system are presented in Appendix-A.

This study aims to show the system resiliency based on various operating scenarios and the malicious data injection, which can be seen by frequency deviation. As far as the frequency deviation is concerned, the frequency range limitation is ± 0.5 Hz (49.5 to 50.5) for 50 Hz, and beyond this value, the system can be collapsed. Hence, the frequency fluctuation should be in the range in which the system's objective function can be minimized, given in (34). On the other hand, cyber-attacks are increasing, which must be taken into account to design a resilient system. With this objective, this paper gives a resilient system solution of a microgrid for minimizing the frequency deviation in consequence of cyber-attack and uncertainties. In this study, the parameters are taken as per unit (p.u.) values except for wind speed ($\mathbb{W}_s$), which is in the range from 3 to 20 m/s. During the normal operation, the total power of each MG is 1.0 p.u. Moreover, the proposed system is simulated through different control methods, and the gains of the controller are presented in Table 1. By doing so, the frequency change characteristics are shown with different scenarios, illustrated as follows.

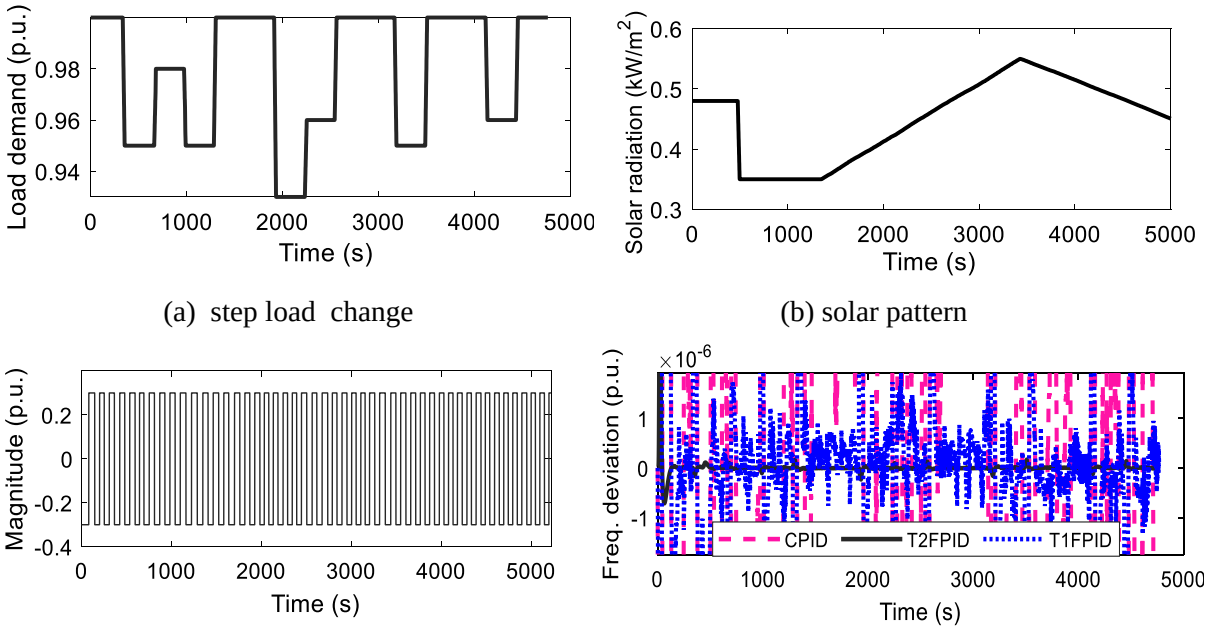
Table 1 Controller Gains

Controller	K_P	K_I	K_D
CPID	1.464	0.575	0.123
T1FPID	1.673	1.402	0.481
T2FPID	0.974	0.946	0.784

3.1.1. Scenario-1: Step load change and cyber-attack

In this scenario, the continuous step load change with a cyberattack such as an extraneous attack is considered. During the simulation, the wind speed is allowed to ± 5 % in continuous steps of the rated

value of 12 m/s. The load, solar, and cyber-attack patterns are presented in Fig. 7(a), (b), (c), respectively. In response to the aforementioned signal, the frequency deviation response is presented in Fig. 7(d). It is noted that the proposed T2FPID controller provides better performance as compared to the other controllers, with a cyberattack and variations in solar insolation, wind speed as well as load. Consequently, the system's objective function, *i.e.*, $ACE_{i\_m}\ (t)$ in addition to peak overshoot, settling time, and the statistical indices such as variance and standard deviations, are reduced, and frequency change within the reasonable limit is achieved, presented in Fig. 12(a).



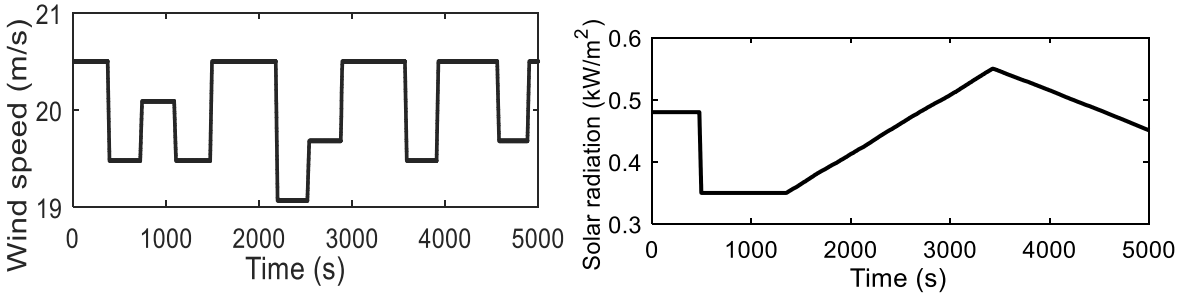
(a) step load change (b) solar pattern

(c) cyber-attack signal (d) frequency deviation of IMG

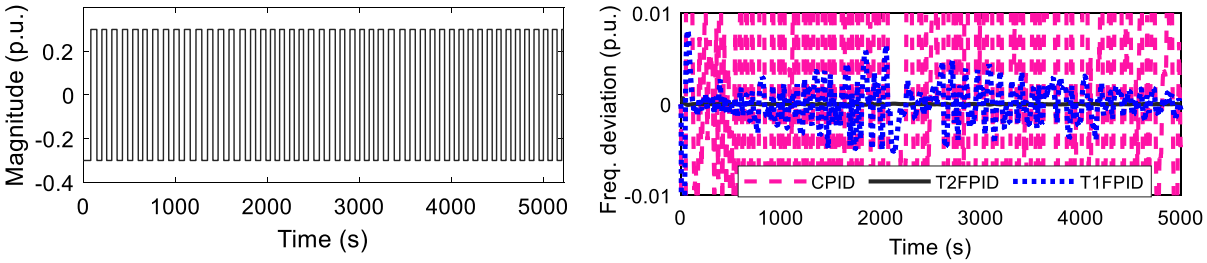
Fig. 7. Pattern and performance of scenario-1

3.1.2. Scenario-2: Continuous step change in wind speed and cyber-attack

This scenario holds the same solar profile, and the cyber-attack pattern is followed (as in scenario-1) with continuous (Fig. 8(a)) step change in wind speed, as well as load, is allowed to change in step with ± 5 % of the rated value of 1 p.u. The system is then simulated, and the frequency deviation characteristics and performance index are presented in Fig. 8(b) and Table 2, respectively.



(a) step change in wind speed (b) solar pattern



(c) cyber-attack signal (d) frequency deviation of interconnected IMG

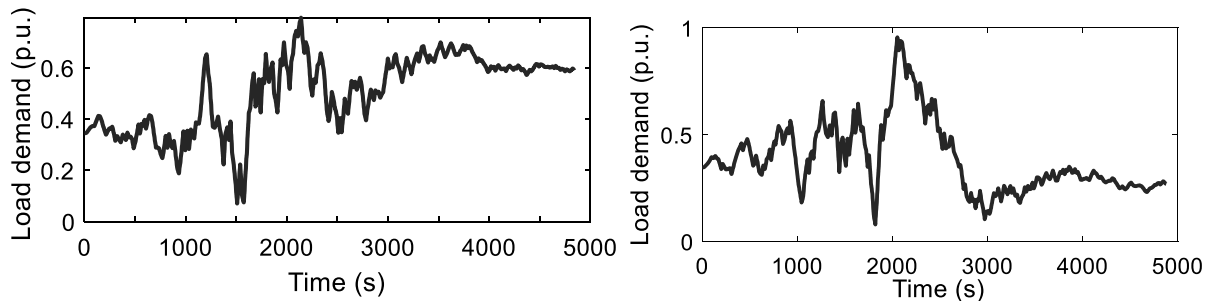
Fig. 8. Pattern and performance of Scenario-2

It is noticed that the frequency deviation of the system is minimized with continuous step load change and cyber-attack through the control actions. However, the T2FPID controller shows a better response than other controllers, as noticed from the indices as depicted in Fig. 12(b).

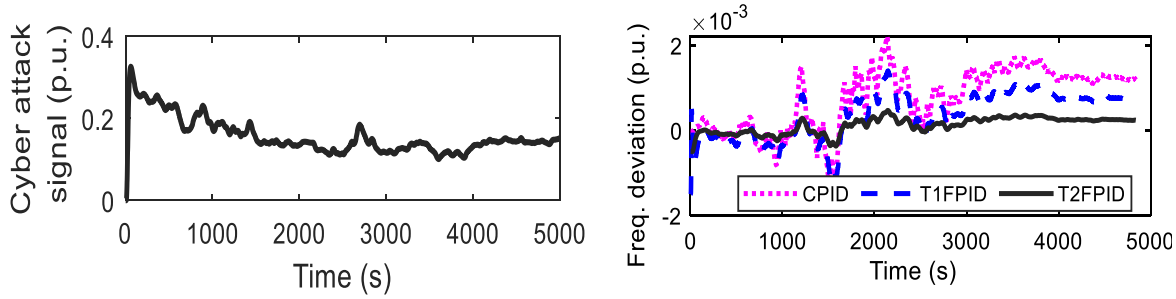
3.1.3. Scenario-3: Random change in load and cyber-attack

Further, the load (pattern-1 and pattern-2) and cyber-attack patterns are changed as random functions, as shown in Fig. 9(a-b) and (c), respectively. The solar insolation and wind speed patterns are varied in steps within ± 5 % of the rated values of 1000 W/m^2 and 12 m/s. Here, the main aim is to show how the frequency is affected in response to a random change in load and malicious data injection with uncertainties.

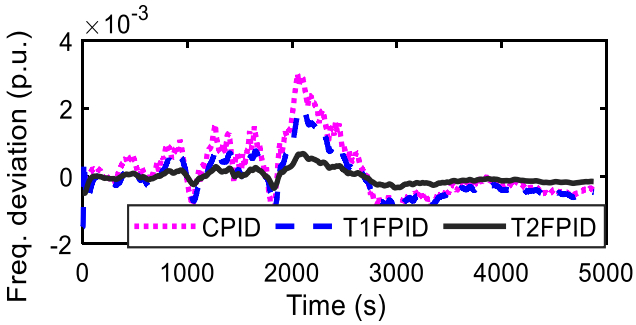
With reference to Fig. 9(a-b) and (c), the corresponding frequency change characteristics are illustrated in Fig. 9(d) and (e), respectively, and the performance indices can be seen in Fig. 12(c). It is observed that the proposed T2FPID controller provides robust performance with lower performance indices like peak overshoot, settling time, ISE, variance, and standard deviation.



(a) random load pattern-1 (b) random load pattern- 2



(c) cyber-attack pattern (d) frequency deviation of an IMG

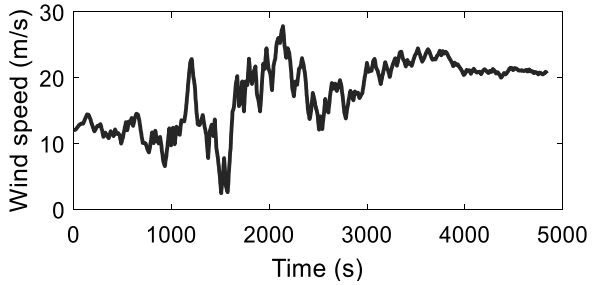


(e) frequency deviation of an IMG

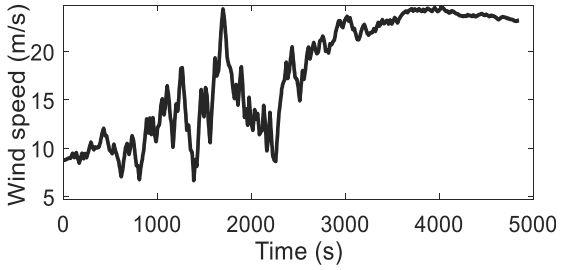
Fig. 9. Pattern and performance of Scenario-3

3.1.4. Scenario-4: Random change in wind speed and cyber-attack

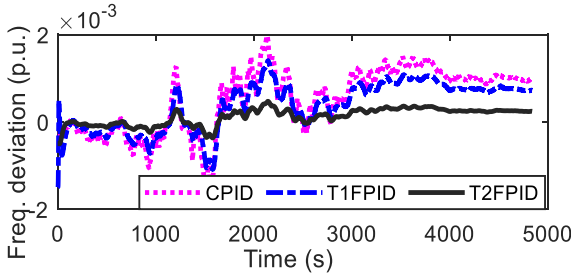
This study considers the wind speed pattern-1 and pattern-2 given in Fig. 10(a, b), and cyber-attack patterns same as Fig. 9(c) are changed in random, correspondingly. The solar insolation and load patterns are varied in steps within ± 5 % of the rated values of 1000 W/m^2 and 1 p.u., respectively.



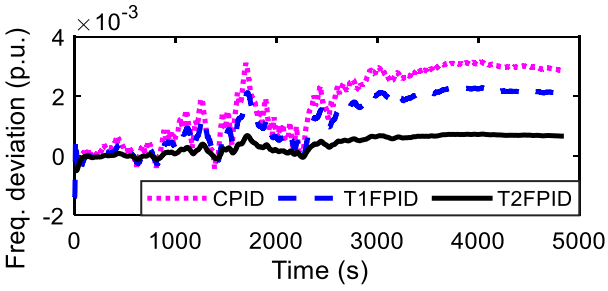
(a) wind speed pattern-1



(b) wind speed pattern-2



(c) frequency deviation of IMG



(d) frequency deviation of an IMG

Fig. 10. Pattern and performance of Scenario-4

Corresponding to the different wind speed patterns, as shown in Fig. 10(a) and (b) and the respective frequency performances are depicted in Fig. 10(d) and (e). Here, the frequency deviation is affected in response to a random change in wind speed and malicious data injection due to cyber-attacks. It indicates that the T2FPID controller can efficiently handle the frequency instabilities.

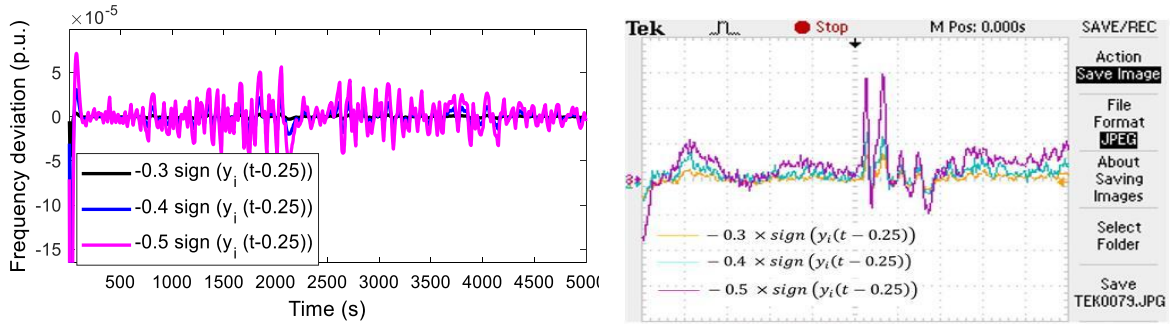
Concerning the CPID and T1FPID can also eliminate the frequency deviation to 0, but the settling is much higher than T2FPID. As can be seen from Figures 9(d & e) and 10(c & d), the frequency deviation is trending downward, which means it certainly comes to zero, but it will take more time. On

the other hand, the system has been simulated with continuous change in load, change in wind speed, and cyber-attacks, so only the T2FPID controller offers stable performance due to the ability of the type-2 fuzzy method.

Conversely, Fig. 12(a-d) demonstrates the comparison performance on the basis of a bar chart where four indices are shown, namely, peak overshoot, settling time, ISE, variance, and standard deviation. It is noted that the proposed controller delivers a robust performance and faster response.

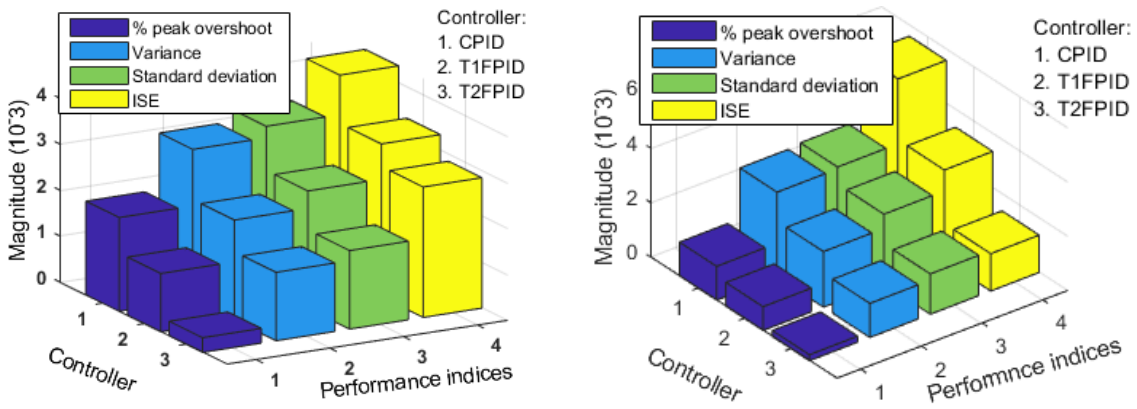
3.1.5. Scenario-5: Change in cyber-attack magnitude

The aim of this study is to show the system resiliency against cyber-attack. As noted, the magnitude of cyber-attack is significant because it can lead to the system collapse either fully or partially. The large cyber-attack could have a severe impact on the performance of a system, resulting in obliterating a system's stability. Considering the different magnitude of cyber-attack, this study has revealed the degree of tolerance of the proposed controller and its effectiveness in terms of transient responses. With reference to (27), the magnitude of the cyber-attack signal has been changed to 0.4 and 0.5, and the simulation is carried out. The variation of the magnitude of cyber-attack has substantially affected the optimal frequency regulation characteristics, as can be seen in Fig. 11. It is observed that with the magnitude of 0.3 and 0.4, the system can cope with the event; however, beyond this value, the system could not have better performances. Fig. 11(a) represents the simulation results, whereas Fig. 11(b) validates the result through a real-time environment.

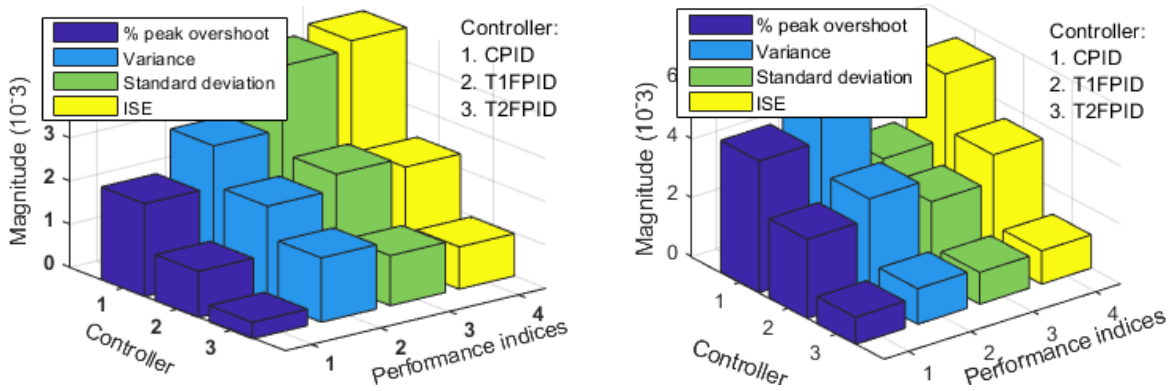


(a) Simulation result (b) Real-time validation

Fig. 11. Impact the variation of the cyber-attack magnitude on frequency deviation in IMG



(a) Performance indices of scenario-1 (b) Performance indices of scenario-2



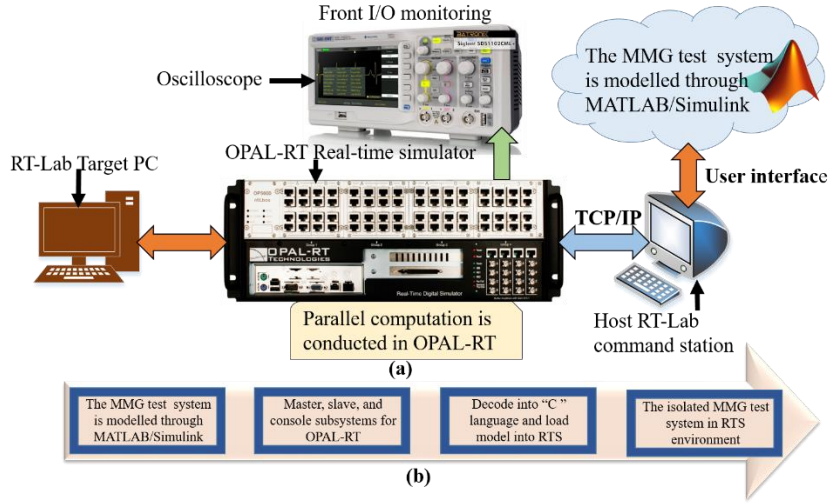
(c) Performance indices of scenario-3 (d) Performance indices of scenario-4

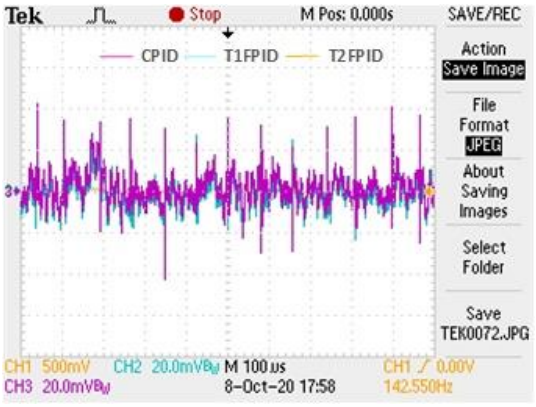
Fig. 12. Controller comparison and performance indices bar chart

3.2. Real-time validation using OPAL-RTs

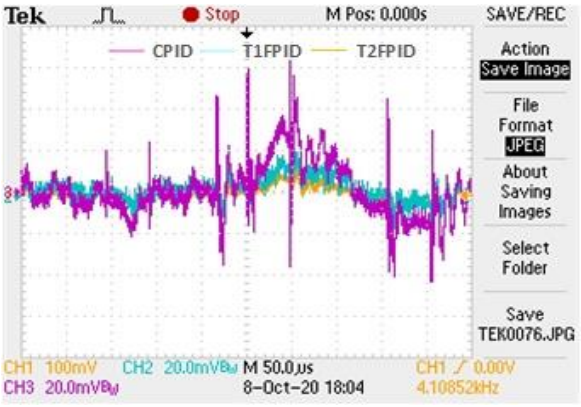
The real-time simulation environment study is presented in this sub-section through the OPAL-RT simulator to validate the simulation results, as discussed above. The OAPL-RT and RT-Lab system architecture is shown in Fig. 13(a), and the flow of validation starting from the Matlab model to real-time validation is also demonstrated in Fig. 13 (b). The real-time simulator, which is used for this study, is OPAL-RT 5142. The host PC specification is Windows 7, 32 bit, Xilinx v10.1, and Matlab 2016b version. In addition, OPALRT's adapter board supports the distributed processing, which operates faster with inbuilt FPGA. It delivers 2.6 GBits full duplex rates.

The OP 5142 board's main task is to infer the Simulink model into the target that integrates the FPGA in RT-Lab. With this, the real-time simulation can be done through a cluster to make it faster and distributed execution. The deviation in frequency for scenarios 1, 2, 3, and 4 are displayed in Fig. 13(c), (d), (e), (f), (g) and (h), respectively. In Fig. 13(c-h), the aqua colour represents the PID control-based characteristics while purple and coral colour characterizes the optimized-based PID control characteristics. It is observed that the frequency deviation is minimum using the proposed T2FPID controller in comparison to that of the other two under scenarios 1, 2, 3, and 4, respectively.

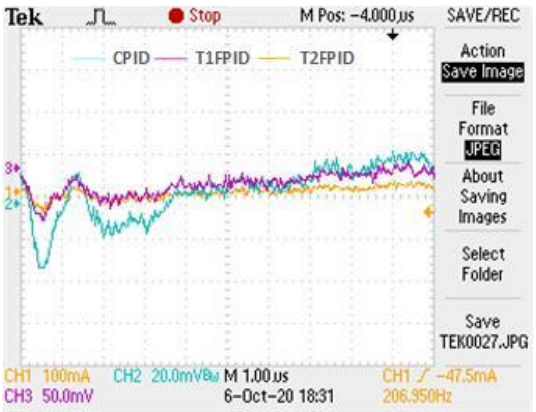

Front I/O monitoring
Oscilloscope
The MMG test system is modelled through MATLAB/Simulink
OPAL-RT Real-time simulator
RT-Lab Target PC
User interface
TCP/IP
Parallel computation is conducted in OPAL-RT
Host RT-Lab command station
(a)
The MMG test system is modelled through MATLAB/Simulink
Master, slave, and console subsystems for OPAL-RT
Decode into "C " language and load model into RTS
The isolated MMG test system in RTS environment
(b)


Tek
Stop
M Pos: 0.000s
SAVE/REC
CPID
T1FPID
T2FPID
Action
Save Image
File Format
JPEG
About Saving Images
Select Folder
Save
TEK0072.JPG
CH1 500mV CH2 20.0mVBW M 100µs CH1 ∕ 0.00V
CH3 20.0mVBW 8-Oct-20 17:58 142.550Hz

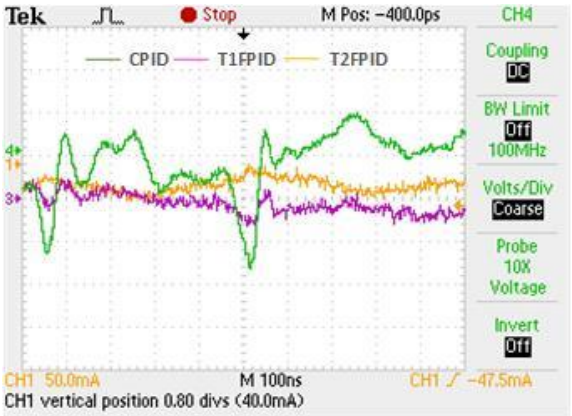
(c)


Tek
Stop
M Pos: 0.000s
SAVE/REC
CPID
T1FPID
T2FPID
Action
Save Image
File Format
JPEG
About Saving Images
Select Folder
Save
TEK0076.JPG
CH1 100mV CH2 20.0mVBW M 50.0µs CH1 ∕ 0.00V
CH3 20.0mVBW 8-Oct-20 18:04 4.10852kHz

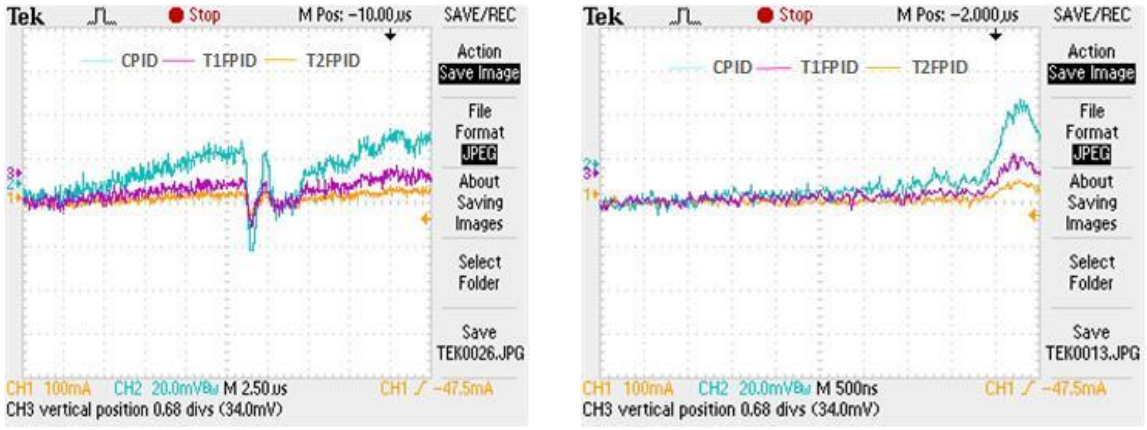
(d)


Tek
Stop
M Pos: -4.000µs
SAVE/REC
CPID
T1FPID
T2FPID
Action
Save Image
File Format
JPEG
About Saving Images
Select Folder
Save
TEK0027.JPG
CH1 100mA CH2 20.0mVBW M 1.00µs CH1 ∕ -47.5mA
CH3 50.0mV 6-Oct-20 18:31 206.950Hz

(e)


Tek
Stop
M Pos: -400.0ps
CH4
CPID
T1FPID
T2FPID
Coupling
DC
BW Limit
Off
100MHz
Volts/Div
Coarse
Probe
10X
Voltage
Invert
Off
CH1 50.0mA M 100ns CH1 ∕ -47.5mA
CH1 vertical position 0.80 divs (40.0mA)

(f)

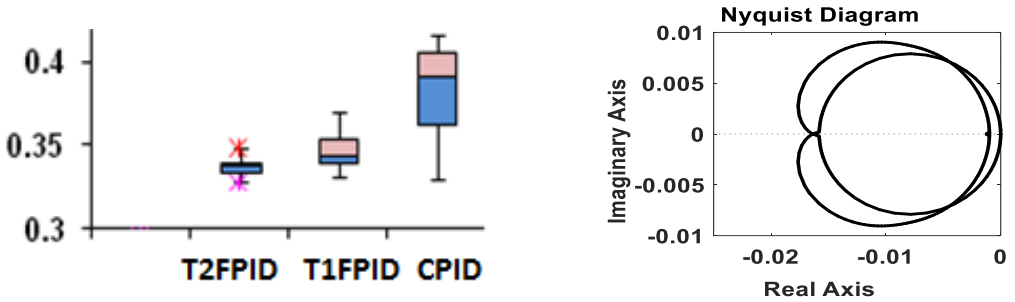


(g) (h)

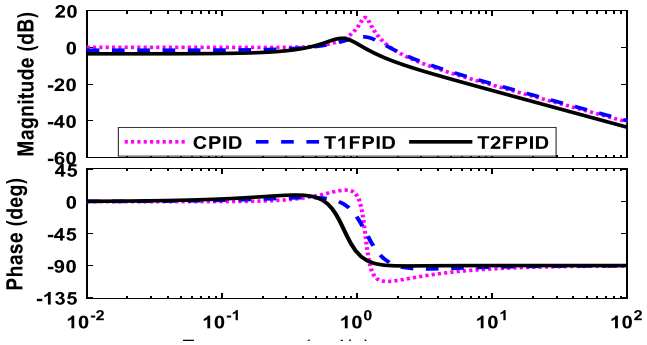
Fig. 13. Real-time study using OPAL-RT

3.3. Performance analysis using statistical parameters

In this subsection, the performance of the T2FPID, T1FPID, and CPID is tested in terms of the eigenvalue and damping factor. The eigenvalue analysis is done using mathematical modelling under different operating scenarios, as presented in Table 2. The system state matrix (A) is obtained from the state-space modelling of the power system, and then the eigenvalues, damping ratios are evaluated. To augment the validation, a comparison of different techniques is plotted in Box and whisker plot, as shown in Fig. 14(a). The Nyquist and Bode plots are displayed in Fig. 14(b) and (c) that represent different controller's stability performances. As noted, the Box and whisker plot signifies the variable data. Large range denotes more scattered data, which do not offer better stability characteristics. In this case, the proposed controller indicates the minimum width, which follows the better stability performance. Further, from Nyquist plot, it is shown that a stable response is ensured through the proposed controller. As per the Nyquist criterion, the Nyquist plot encircles –1 point P times counter clockwise, which signifies that the system is stable. Finally, the stability analysis is done through a Bode plot. As per the stability criteria, the more the gain margin and phase margin are, the more system stability will be. With this, the T2FPID controller-based LFC scheme gives a high value of gain margin and phase margin values; thus, the controller can be called as the best compared to others under operating scenarios.



(a) Box plot (b) Nyquist plot



(c) Bode plot

Fig. 14. Performance analysis using Box, Nyquist, and Bode plot

Table 2 Eigenvalue and damping ratio analysis

Operating Conditions	Methodology	Eigenvalues	Damping ratios
Scenario-1	CPID	-3.4532± *j*6.3217	0.4527
	T1FPID	-5.1463± *j* 7.3554	0.4836
	T2FPID	**-6.4858± *j* 8.5791**	**0.6395**
Scenario-2	CPID	-4.2674± *j* 5.6725	0.3021
	T1FPID	-6.6738± *j* 6.9681	0.4581
	T2FPID	**-7.1258± *j* 7.8249**	**0.6042**
Scenario-3	CPID	-4.2261± *j*5.6465	0.3869
	T1FPID	-5.8782± *j* 6.7586	0.5821
	T2FPID	**-7.1168± *j* 8.5883**	**0.7839**
Scenario-4	CPID	-5.2369± *j*6.6786	0.3869
	T1FPID	-7.3508± *j* 8.8286	0.5470
	T2FPID	**-8.0842± *j* 8.5704**	**0.7149**

4. Conclusion

This paper focuses on modeling and validating resilience-based frequency regulation schemes for isolated microgrids under different operating scenarios. By comprehensive simulation and real-time testing, the following key conclusions are drawn. Firstly, the model is simulated with step load change, step wind speed, and solar pattern. Secondly, random change in load, wind speed, and solar pattern is simulated. Thirdly, the cyber-attack model is incorporated and tested through three different controllers, where type-2 fuzzy PID shows better regulation and holds better resiliency characteristics with reduced error and other indices. Further, real-time simulation testing is performed through the OPAL-RT simulator, and it is revealed that the real-time results follow the simulation results, and the proposed controller plays a significant role in showing the robustness of the system. Finally, the various performance indices and system's stability are characterized by the percentage of peak overshoot, variance, standard deviation, ISE, eigenvalues, and stability curves, such as Nyquist and Bode plots.

Appendix-A: System data

Rating: PV = 30 kW; Wind = 100 kW; EV = 70 kW; DG = 100 kW; FESS = 45 kW; BESS = 45 kW $P_{L1} = P_{L2}$ = 200 kW Parameters: $\mathcal{T}_W$ = 1.5 s; $\mathcal{T}_{PV}$= 1.8 s; $\mathcal{T}_d$= 8 s; $\mathcal{T}_g$= 0.1 s; $\mathcal{T}_{BESS}$ = 0.1 s; $\mathcal{T}_{FESS}$ = 0.1 s δ_{dg} = 0.001 puMW/s; μ_{dg} = 0.04 puMW K_{BESS} = -0.003; K_{FESS} = -0.01; $\mathcal{M}$ = 0.4; $\mathcal{D}$ = 0.003

5. References

[1] J. Yan, "Energy Systems in Transition: Challenges and Opportunities," ed: Elsevier, 2020.

[2] E. D. Vugrin, M. J. Baca, M. D. Mitchell, and K. L. Stamber, "Evaluating the effect of resource constraints on resilience of bulk power system with an electric power restoration model," *International Journal of System of Systems Engineering,* vol. 5, no. 1, pp. 68-91, 2014.

[3] M. Panteli and P. Mancarella, "The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience," *IEEE Power and Energy Magazine,* vol. 13, no. 3, pp. 58-66, 2015.

[4] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 5, pp. 1932-1941, 2017.

[5] X. Shang-Guan, Y. He, C. Zhang, L. Jiang, J. W. Spencer, and M. Wu, "Sampled-data based discrete and fast load frequency control for power systems with wind power," *Applied Energy,* vol. 259, p. 114202, 2020.

[6] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, "Resonance attacks on load frequency control of smart grids," *IEEE Transactions on Smart Grid,* vol. 9, no. 5, pp. 4490-4502, 2017.

[7] M. Kenney, "Cyber-terrorism in a post-stuxnet world," *Orbis,* vol. 59, no. 1, pp. 111-128, 2015.

[8] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems,* vol. 32, no. 4, pp. 3317-3318, 2016.

[9] V. Venkataramanan, A. K. Srivastava, A. Hahn, and S. Zonouz, "Measuring and Enhancing Microgrid Resiliency Against Cyber Threats," *IEEE Transactions on Industry Applications,* vol. 55, no. 6, pp. 6303-6312, 2019.

[10] Y. Tan, Y. Li, Y. Cao, M. Shahidehpour, and Y. Cai, "Severe cyber attack for maximizing the total loadings of large-scale attacked branches," *IEEE Transactions on Smart Grid,* vol. 9, no. 6, pp. 6998-7000, 2018.

[11] P. Li, Y. Liu, H. Xin, and X. Jiang, "A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 10, pp. 4343-4352, 2018.

[12] W. Bi, K. Zhang, Y. Li, K. Yuan, and Y. Wang, "Detection scheme against cyber-physical attacks on load frequency control based on dynamic characteristics analysis," *IEEE Systems Journal,* vol. 13, no. 3, pp. 2859-2868, 2019.

[13] J. Liu, Y. Gu, L. Zha, Y. Liu, and J. Cao, "Event-Triggered $ H_\infty $ Load Frequency Control for Multiarea Power Systems Under Hybrid Cyber Attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* vol. 49, no. 8, pp. 1665-1678, 2019.

[14] K.-D. Lu, G.-Q. Zeng, X. Luo, J. Weng, Y. Zhang, and M. Li, "An Adaptive Resilient Load Frequency Controller for Smart Grids With DoS Attacks," *IEEE Transactions on Vehicular Technology,* vol. 69, no. 5, pp. 4689-4699, 2020.

[15] Z. Cheng, D. Yue, S. Hu, C. Huang, C. Dou, and L. Chen, "Resilient load frequency control design: DoS attacks against additional control loop," *International Journal of Electrical Power & Energy Systems*, vol. 115, p. 105496, 2020.
[16] Q. Wang, W. Tai, Y. Tang, M. Ni, and S. You, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 169-177, 2019.
[17] M. Jin *et al.*, "Energy-cyber-physical systems," *Applied Energy*, vol. 256, p. 113939, 2019.
[18] H. Zhang, X. Li, X. Liu, and J. Yan, "Enhancing fuel cell durability for fuel cell plug-in hybrid electric vehicles through strategic power management," *Applied Energy*, vol. 241, pp. 483-490, 2019.
[19] M. R. Khalghani, J. Solanki, S. Solanki, M. H. Khooban, and A. Sargolzaei, "Resilient Frequency Control Design for Microgrids Under False Data Injection," *IEEE Transactions on Industrial Electronics*, 2020.
[20] C. Chen, Y. Chen, K. Zhang, M. Ni, S. Wang, and R. Liang, "System redundancy enhancement of secondary frequency control under latency attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 647-658, 2020.
[21] C. Chen, K. Zhang, M. Ni, and Y. Wang, "Cyber-attack-tolerant Frequency Control of Power Systems," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 2, pp. 307-315, 2020.
[22] A. Sargolzaei, K. Yen, and M. N. Abdelghani, "Delayed inputs attack on load frequency control in smart grid," in *ISGT 2014*, 2014, pp. 1-5: IEEE.
[23] X.-C. ShangGuan *et al.*, "Switching system-based load frequency control for multi-area power system resilient to denial-of-service attacks," *Control Engineering Practice*, vol. 107, p. 104678, 2021.
[24] X. Zhou, Z. Gu, and F. Yang, "Resilient event-triggered output feedback control for load frequency control systems subject to cyber attacks," *IEEE Access*, vol. 7, pp. 58951-58958, 2019.
[25] B. Xiao, H.-K. Lam, and H. Li, "Stabilization of interval type-2 polynomial-fuzzy-model-based control systems," *IEEE Transactions on Fuzzy Systems*, vol. 25, no. 1, pp. 205-217, 2016.
[26] H.-K. Lam and L. D. Seneviratne, "Stability analysis of interval type-2 fuzzy-model-based control systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 38, no. 3, pp. 617-628, 2008.
[27] H.-K. Lam, H. Li, C. Deters, E. L. Secco, H. A. Wurdemann, and K. Althoefer, "Control design for interval type-2 fuzzy systems under imperfect premise matching," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 2, pp. 956-968, 2013.
[28] Y. Pan and G.-H. Yang, "Event-triggered fault detection filter design for nonlinear networked systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 11, pp. 1851-1862, 2017.
[29] X. Li and D. Ye, "Asynchronous event-triggered control for networked interval type-2 fuzzy systems against dos attacks," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 2, pp. 262-274, 2020.
[30] O. Linda, M. Manic, J. Alves-Foss, and T. Vollmer, "Towards resilient critical infrastructures: Application of Type-2 Fuzzy Logic in embedded network security cyber sensor," in *2011 4th International Symposium on Resilient Control Systems*, 2011, pp. 26-32: IEEE.
[31] A. D. Shakibjoo, M. Moradzadeh, S. Z. Moussavi, A. Mohammadzadeh, and L. Vandevelde, "Load frequency control for multi-area power systems: A new type-2 fuzzy approach based on Levenberg–Marquardt algorithm," *ISA transactions*, 2021.
[32] Z. Farooq, A. Rahman, and S. A. Lone, "Load frequency control of multi-source electrical power system integrated with solar-thermal and electric vehicle," *International Transactions on Electrical Energy Systems*, p. e12918, 2021.
[33] M.-H. Khooban, T. Dragicevic, F. Blaabjerg, and M. Delimar, "Shipboard microgrids: A novel approach to load frequency control," *IEEE Transactions on Sustainable Energy*, vol. 9, no. 2, pp. 843-852, 2017.

[34] A. A. El-Fergany and M. A. El-Hameed, "Efficient frequency controllers for autonomous two-area hybrid microgrid system using social-spider optimiser," *IET Generation, Transmission & Distribution,* vol. 11, no. 3, pp. 637-648, 2017.
[35] T. Masuta and A. Yokoyama, "Supplementary load frequency control by use of a number of both electric vehicles and heat pump water heaters," *IEEE Transactions on smart grid,* vol. 3, no. 3, pp. 1253-1262, 2012.
[36] S. A. Hosseini, M. Toulabi, A. S. Dobakhshari, A. Ashouri-Zadeh, and A. M. Ranjbar, "Delay compensation of demand response and adaptive disturbance rejection applied to power system frequency control," *IEEE Transactions on Power Systems,* vol. 35, no. 3, pp. 2037-2046, 2019.
[37] S. F. Aliabadi, S. A. Taher, and M. Shahidehpour, "Smart deregulated grid frequency control in presence of renewable energy resources by EVs charging control," *IEEE Transactions on Smart Grid,* vol. 9, no. 2, pp. 1073-1085, 2016.
[38] M. H. Khooban, "An Optimal Non-Integer MPC-based Load Frequency Control for Modern AC Power Grids with V2G Technology," *IEEE Transactions on Energy Conversion,* 2020.
[39] L. Luo *et al.,* "Optimal scheduling of a renewable based microgrid considering photovoltaic system and battery energy storage under uncertainty," *Journal of Energy Storage,* vol. 28, p. 101306, 2020.
[40] H. Sun, C. Peng, D. Yue, Y. L. Wang, and T. Zhang, "Resilient load frequency control of cyber-physical power systems under QoS-dependent event-triggered communication," *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* vol. 51, no. 4, pp. 2113-2122, 2020.
[41] A. M. Mohan, N. Meskin, and H. Mehrjerdi, "A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems," *Energies,* vol. 13, no. 15, p. 3860, 2020.
[42] S. Mohanty, A. Pradhan, and A. Routray, "A cumulative sum-based fault detector for power system relaying application," *IEEE transactions on power delivery,* vol. 23, no. 1, pp. 79-86, 2007.
[43] M. Farahani, S. Ganjefar, and M. Alizadeh, "PID controller adjustment using chaotic optimisation algorithm for multi-area load frequency control," *IET Control Theory & Applications,* vol. 6, no. 13, pp. 1984-1992, 2012.
[44] H. Bevrani and P. R. Daneshmand, "Fuzzy logic-based load-frequency control concerning high penetration of wind turbines," *IEEE systems journal,* vol. 6, no. 1, pp. 173-180, 2011.
[45] I. Kocaarslan and E. Çam, "Fuzzy logic controller in interconnected electrical power systems for load-frequency control," *International Journal of Electrical Power & Energy Systems,* vol. 27, no. 8, pp. 542-549, 2005.
[46] A. Sarabakha, C. Fu, E. Kayacan, and T. Kumbasar, "Type-2 fuzzy logic controllers made even simpler: From design to deployment for UAVs," *IEEE Transactions on Industrial Electronics,* vol. 65, no. 6, pp. 5069-5077, 2017.