Received: 17 September 2021 | Revised: 7 December 2021 | Accepted: 25 July 2022 | IET Cyber-Physical Systems: Theory & Applications

DOI: 10.1049/cps2.12033

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

# NEFTSec: Networked federation testbed for cyber-physical security of smart grid: Architecture, applications, and evaluation

Vivek Kumar Singh[1] | Manimaran Govindarasu[2] | Donald Porschet[3] | Edward Shaffer[3] | Morris Berman[3]

[1]Cyber Security and Resilience, National Renewable Energy Laboratory (NREL), Golden, Colorado, USA

[2]Department of Electrical and Computer Engineering, Iowa State University, Ames, Iowa, USA

[3]US CCDC Army Research Laboratory (ARL), Adelphi, Maryland, USA

**Correspondence**

Vivek Kumar Singh, Cyber Security and Resilience, National Renewable Energy Laboratory (NREL), Golden, CO 80401, USA.
Email: vsingh@iastate.edu

**Funding information**

US Department of Energy, the Office of Electricity Delivery and Energy Reliability's Cybersecurity of Energy Delivery Systems program, Grant/Award Number: DE-EE0008773; United States National Science Foundation, Grant/Award Number: 1446831

**Abstract**

As today's power grid is evolving into a densely interconnected cyber-physical system (CPS), a high fidelity and multifaceted testbed environment is needed to perform cybersecurity experiments in a realistic grid environment. Traditional standalone CPS testbeds lack the ability to emulate complex cyber-physical interdependencies between multiple smart grid domains in a real-time environment. Therefore, there are ongoing research and development (R&D) efforts to develop an interconnected CPS testbed by sharing geographically dispersed testbed resources to perform distributed simulation while analysing simulation fidelity. This paper presents a networked federation testbed for cybersecurity evaluation of today's and emerging smart grid environments. Specifically, it presents two novel testbed architectures, including cyber federation and cyber-physical federation, identifies R&D applications, and also describes testbed building blocks with experimental case studies. It also presents a novel co-simulation interface algorithm to facilitate distributed simulation within cyber-physical federation. The resources available at the PowerCyber CPS security testbed at Iowa State University (ISU) and the US Army Research Laboratory are utilised to develop this platform for performing multiple experimental case studies pertaining to wide-area protection and control applications in power system. Finally, experimental results are presented to analyse the simulation fidelity and real-time performance of the testbed federation.

**KEYWORDS**

cyber-physical systems, cybersecurity, hardware-in-the loop simulation, phasor measurement, power grids, testbed federation

## 1 | INTRODUCTION

Cyber-physical system (CPS) testbeds play a vital role in the design, development, and evaluation of state-of-the-art research solutions, technologies, and tools for securing the smart grid against cybersecurity threats. Generally, the smart grid CPS testbed consists of a hybrid combination of hardware, software, emulators, and simulators that are interconnected through a communication network to emulate the real-world grid [1]. The commercial off-the-shelf (COTS) real-time simulator simulates complex power systems at the same rate as 'wall-clock time' in customised time steps, supports industry-grade communication protocols, and also facilitates hardware in the loop (HIL) testing using high-speed input/output (I/O) ports. Most of the previous studies related to cybersecurity research in smart grids were based on traditionally isolated CPS testbeds that do not provide a realistic platform for experimental testing and also face several challenges, such as scalability, fidelity, and heterogeneity to emulate complex power systems in a cyber-physical testbed environment. One of the potential solutions is to develop a bank of locally connected simulators, coupled with hardware devices and software products. This effort requires significant investments in resources, time, and labour, which are not available in every research centre and therefore renders such scenarios practically infeasible.

Development of an interconnected networked federation testbed (NEFTSec) assists in performing sophisticated, high fidelity, and attack-defence module-based cybersecurity experiments in the smart grid. It is based on the notion of pooling different testbed resources across geographically dispersed research centres in a distributed manner through a common network like the internet or intranet and development of an integrated real-time testbed environment to emulate the real-grid infrastructure. The recent survey [2] on smart grid CPS testbeds presents a systematic study on existing testbeds across the globe. It also discusses how the interconnection of multiple testbeds using virtual private networks (VPN) can enhance individual testbed capabilities while supporting several research areas. Further, the National Institute for Standards and Technology [3] highlighted the need for modular and composable testbeds with remote federation functionality that are interoperable with remote facilities across the nation.

### 1.1 | Motivation

Developing a federated testbed is a non-trivial task as it requires a comprehensive understanding of grid network topology, key applications, and a strong commitment and consensus between federating participants to support multiple interfaces with a minimum of failure points. In [4], the conceptual architecture of sharing the phasor measurement unit (PMU) data using the industry-grade North American SynchroPhasor Initiative (NASPI) is presented, which is a collaborative effort between the U.S. Department of Energy and North American Electric Reliability Corporation, for sharing phasor data among utilities and industry vendors. However, the authors of [5] have discussed challenges related to fidelity, Quality of Services (QoS), and cyber-physical security of the interconnected networks of control centres and utilities in the NASPI architecture. Further, there is little advancement on developing implementable architectures, CPS benchmark models, and cybersecurity threat analyses to validate the conceptual NASPI architecture in grid networks. For the above-discussed reasons, it is imperative to develop a NEFTSec to address the evolving cybersecurity challenges in power systems.

In our previous work, we have shown the performance evaluation of machine learning-based anomaly detector for wide-area protection scheme (WAPS) using cyber federation testbed [6]. In this work, we present several applications of federation testbeds, discuss different conceptual architectures, propose a co-simulation interface algorithm (CIA) for distributed simulation with a detailed analysis, and provide a quantitative performance evaluation of different federation architectures during real-time simulation.

### 1.2 | Contributions

The key contributions of this paper include:

1. It is one of the first efforts to discuss several applications of NEFTSec, explore its conceptual architectures, and present its experimental design and implementation in a cyber-physical testbed environment.
2. CIA is proposed to perform federation-based distributed simulation using geographically dispersed testbeds in real time.
3. Experimental testing and evaluation are performed to analyse network packets (latency and bandwidth) and simulation fidelity during the distributed simulation.
4. Quantitative comparison of different federation architectures using simulation parameters during a real-time HIL simulation.

The rest of this paper is organised as follows: Section 2 presents an overview of relevant literature that describes different federated testbeds. Several applications, architecture, and design of NEFTSec are presented in Section 3. Section 4 presents the proposed CIA for the distributed cyber-physical federation. Section 5 and Section 6 present various case studies and their experimental evaluation in the real time. Finally, Section 7 provides the conclusions with a brief description of future works.

## 2 | RELATED WORKS

Existing challenges in the design and development of a federated testbed are extensively discussed in other research communities that focus on Internet of Things (IoT), networking, and cyber systems [7]; however, there exist few research efforts that encompass federation-related works in the context of smart grid cybersecurity. To develop a high fidelity, economical, and scalable testbed, researchers from several universities and research laboratories are working together to develop federated testbeds across hundreds or thousands of miles for specific applications in a power system domain.

Table 1 presents a condensed synthesis of key contributions related to the existing federated testbeds that are developed for specific applications in power systems. In [8], the National Renewable Energy Laboratory (NREL) and Pacific Northwest National Laboratory federated to develop a power hardware-in-the-loop-based co-simulation platform for testing multiple solar inverters (hardware) with two large-scale distribution systems: the IEEE 123 node and 8500 node test feeders. This federation platform applied JavaScript Object Notation (JSON)-based data exchange protocol and User Datagram Protocol (UDP) protocol is used at the transport layer while ignoring missing and delayed packets during the distribution simulation at a timestep of 1 s. Further, the NREL and Idaho National Laboratory (INL) federated their testbeds to demonstrate their capabilities and computed a real-time latency of 28 milliseconds between their networks [9]. The authors of [10] presented the DETER-WAMS-ExoGENI testbed by federating a real-time digital simulator (RTDS)-phasor measurement unit (PMU) testbed at the North Corolina State University with

**TABLE 1** A summary of work related to developing federated testbed

| Participants | Key contributions |
|---|---|
| NREL and PNNL [8] | PHIL co-simulation testing for distributed energy resources in distribution systems (IEEE 123 and 8500 node feeders). |
| NREL and INL [9] | Demonstration of data exchange at 1200 samples/sec with an average delay of 28 milliseconds. |
| NCSU and DETER-USC [10] | Cyber federation using cyber computing platform (cyber system) with HIL system (physical system) |
| ISU and DETER-USC [11] | Cyber federation of substation and control centre networks for WAPAC cybersecurity |
| Politecnico di Milano and University of South Carolina [12] | Remote model validation using the physical device and the virtual testbed model |
| Florada State University and University of Alberta [13] | Thermal and electric simulation using distant real-time simulators |
| INL, RWTH Aachen university, and other institutions [14] | PHIL distributed simulation of transatlantic HVDC interconnection between the transmission systems |

Abbreviations: HIL, hardware in the loop; HVDC, high-voltage direct current; INL, Idaho National Laboratory; ISI, Information Science Institute; ISU, Iowa State University; NCSU, North Corolina State University; PHIL, power hardware-in-the-loop; PNNL, Pacific Northwest National Laboratory; RWTH, Rheinisch-Westfälische Technische Hochschule; WAPAC, wide-area protection and control.

the Defence Technology Experimental Research (DETER) testbed at the University of Southern California (USC) to perform an impact analysis of cyberattacks on wide-area damping control (WADC). The PowerCyber testbed at Iowa State University (ISU) also performed cyber federation with the DETER testbed at the Information Science Institute of USC to emulate substation and control centre networks in power grids. In this study, the authors only performed physical-level impact analysis of cyberattacks in wide-area protection and control [11]; however, a network-level analysis is also critical to support reliable communication and data exchange between federated testbeds.

The geographically dispersed real-time distributed simulation (GD-RTDS) is one of the key applications of networked federation that facilitates the integration of distant real-time simulators to simulate complex power systems by partitioning them into multiple subsystems without abstracting individual system components. One of the earliest developments of a virtual environment to support the GD-RTDS is reported in 2005 [12] to perform a remote model validation using a LabVIEW virtual instrument and virtual testbed interaction. In Ref. [13], the authors demonstrated the GD-RTDS platform by accurately performing thermo-electric co-simulation using two distant simulators. The authors of Ref. [14] presented a *VILLAS-framework* for performing distributed simulation of a trans-atlantic high-voltage direct current interconnection between the transmission systems of the United States and European grids. This platform is developed through the leading collaboration of INL and Rheinisch-Westfälische Technische Hochschule Aachen University and was joined later by other US national laboratories and institutions in United States, Germany, and Italy.

Since the decoupling point and the selection of the decoupling methods affect the stability and performance of a distribution simulation, a transmission line modelling (TLM)-based decoupling technique is proposed to perform GD-RTDS using the MATLAB-Simulink environment [15] and real-time simulators [16]. In [17], the authors showed the application of real-time OPAL-RT simulators to perform the electromagnetic transient (EMT), three-phase transient stability (TS), and hybrid TS-EMT simulations for a small distributed power network. Further, the advancements in GD-RTDS have been presented by introducing interface algorithms for system decoupling, time delay compensation, and superior simulation fidelity while exchanging data over the internet [18, 19].

Phasors-based CIA [19] is well-recognised to be the current state-of-the-art solution to facilitate the geographically distributed co-simulation as it exhibits a higher degree of simulation fidelity than other methods. The previously proposed CIAs [19–22] are mostly focussed on interfacing transmission and distribution systems that exhibit slow transients and less complexity as compared to performing co-simulation at multiple transmission systems.

A review of literature indicates that none of these efforts address the challenges of developing a robust platform and implementable architecture to support the federation-based cybersecurity experiments in the smart grid domain. Also, it is imperative to develop a CIA and analyse its performance during the GD-RTDS for transmission systems using the federation platform. The rest of this paper discusses several applications, implementable design of NEFTSec, and experimental evaluations for multiple case studies.

## 3 | APPLICATIONS, ARCHITECTURE, AND DESIGN

### 3.1 | Research applications

Federating existing smart grid CPS testbeds enhances collaboration and productive investments without revealing proprietary information between participants. It provides educational and research-integrated platforms for large-scale experimentation with diverse network topology and devices. In general, it can be applied for a comprehensive set of applications that are represented in Figure 1 and elaborated in greater details below.

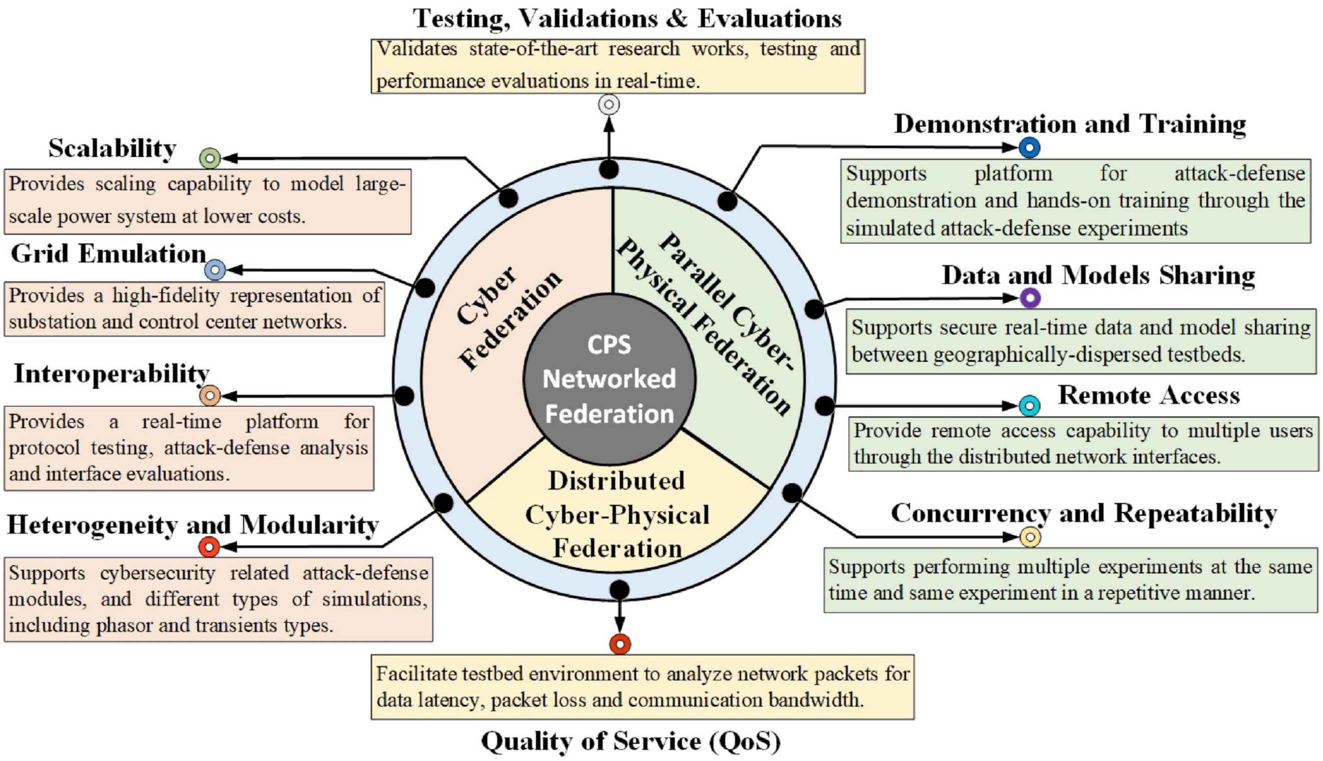

Testing, Validations & Evaluations
Validates state-of-the-art research works, testing and performance evaluations in real-time.
Scalability
Provides scaling capability to model large-scale power system at lower costs.
Grid Emulation
Provides a high-fidelity representation of substation and control center networks.
Interoperability
Provides a real-time platform for protocol testing, attack-defense analysis and interface evaluations.
Heterogeneity and Modularity
Supports cybersecurity related attack-defense modules, and different types of simulations, including phasor and transients types.
Demonstration and Training
Supports platform for attack-defense demonstration and hands-on training through the simulated attack-defense experiments
Data and Models Sharing
Supports secure real-time data and model sharing between geographically-dispersed testbeds.
Remote Access
Provide remote access capability to multiple users through the distributed network interfaces.
Concurrency and Repeatability
Supports performing multiple experiments at the same time and same experiment in a repetitive manner.
Cyber Federation
Parallel Cyber-Physical Federation
Distributed Cyber-Physical Federation
CPS Networked Federation
Facilitate testbed environment to analyze network packets for data latency, packet loss and communication bandwidth.
Quality of Service (QoS)

FIGURE 1 Types and applications of networked federation testbed (NEFTSec)

(1) ***Scalability***: Addresses this challenge by leveraging computational, hardware, and software resources from CPS testbeds. In particular, the scalability in power systems is resolved by performing distributed simulation and co-simulation using distant real-time simulators. Further, the scalability in cyber systems is accomplished by leveraging computational resources, such as server racks from other CPS testbeds, and modelling virtual sensors and actuators to emulate physical devices.

(2) ***Grid Emulation (Fidelity)***: Emulates substation and control centre networks with industry-grade communication protocols while simulating complex power system dynamics in a HIL environment. This provides a high fidelity representation of geographically dispersed grid elements for industrial, academic, and broader public users.

(3) ***Remote Access***: Provides remote access capability to multiple users using internet-based network interfaces to conduct multiple and coordinated cybersecurity-based attack-defence experiments [20].

(4) ***Testing, Validation, and Evaluation***: Since the current operational systems cannot be utilised to perform cyber-physical security-related experiments, the NEFTSec provides a platform to test, validate, and evaluate the performances of state-of-the-art research and engineering solutions in real time.

(5) ***Demonstration and Training***: Provides a unique demonstration platform by simulating realistic cyber-attacks and possible defence measures [23, 24]. In addition, it serves as a powerful training ground to provide hands-on cybersecurity training and hacking exercises in grid security.

(6) ***Quality of Service (QoS)***: Supports QoS assessments by analysing network packets for data latency, packet loss, and communication bandwidth for a reliable communication network between CPS testbeds.

(7) ***Heterogeneity and Modularity***: Incorporates heterogeneity by simulating different components of power systems utilising phasor and transient simulations as well as performing hybrid simulations. It also supports modularity by integrating several modules from different CPS testbeds, including physical and cyber system modules, communication modules, and cybersecurity attack-defence modules.

(8) ***Concurrency and Repeatability***: Supports concurrency by performing multiple CPS experiments in a parallel or distributed manner. Further, it supports repeatability by allowing federating participants to perform the same experiment multiple times.

(9) ***Data and Models Sharing***: Since the availability of real-world data capturing cyber-physical properties is limited and sensitive to the utility's operation, the NEFTSec assists in sharing data and models to multiple participants simultaneously in a distributed manner to facilitate multiple CPS experiments and use cases without affecting real-world operations.

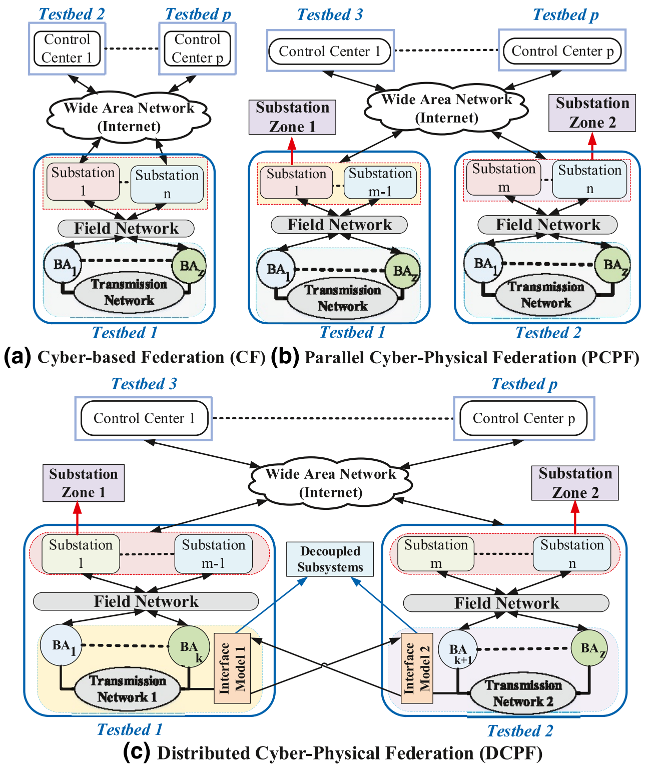
(10) ***Interoperability***: Supports interoperability by providing a real-time platform for communication protocol testing, attack-defence analysis, and experimental evaluation of interconnected testbed network interfaces.

## 3.2 | Conceptual architecture

Figure 2 shows the conceptual architecture of NEFTSec that emulates different types of cyber-physical interactions between substation and control centre networks while simulating the power system. The power grid topology is represented through balanced authority areas ($BA_1 \ldots BA_z$) that are interconnected through the transmission network. Specifically, it is classified into two broad categories: 1) Cyber (network)-based federation (CF) and 2) Cyber-physical-based federation (CPF).

### 3.2.1 | Cyber (network)-based federation

This architecture, as shown in Figure 2a, emulates the wide-area communication between a group of substations and control centres using cyber and physical components of geographically dispersed CPS testbeds. In this architecture, the substation topology, including power system simulators, field network, sensors, actuators, etc., is emulated in one testbed (i.e. Testbed 1), while other testbeds (i.e. Testbed 2… Testbed P) are emulating local or regional control centres that receive grid measurements to support wide-area monitoring, protection, and control (WAMPAC) applications in real time.



(a) Cyber-based Federation (CF) (b) Parallel Cyber-Physical Federation (PCPF)

(c) Distributed Cyber-Physical Federation (DCPF)

**FIGURE 2** Conceptual architecture of the networked federation testbed (NEFTSec)

### 3.2.2 | Cyber-physical-based federation

This architecture emulates geographically dispersed multiple substations and control centres (local and regional) and supports bi-directional data exchange between them. Based on the grid topology, it is classified into two broad categories: (1) Parallel CPF (PCPF) and (2) Distributed CPF (DCPF).

(1) **Parallel CPF (PCPF)**: In this architecture, the distant power system simulators and emulators, synchronised with a Global Positioning System (GPS) clock signal, are running identical power system models with the same time step in parallel; however, grid measurements are collected from substation zones and are forwarded to control centres that are emulated in different CPS testbeds. For example, as shown in Figure 2b, Testbed 1 emulates substation 1 to substation $m - 1$ as substation zone 1 and Testbed 2 emulates substation $m$ to substation $n$ as substation zone 2 while executing the same power system model in real time. This architecture is highly suitable for cyberattack analysis on wide-area measurements during a steady state. Note that the proper analysis of system models, network traffic, and synchronisation of control signals is required to accurately capture transient responses in multiple simulators during injected disturbances.
(2) **Distributed CPF (DCPF)**: This architecture facilitates distributed simulation in transmission systems and co-simulation of transmission and distribution systems by splitting a complex power system into multiple subsystems and executing the decoupled subsystems in distant simulators that are synchronised to a GPS clock signal. Figure 2c presents the DCPF in a transmission system where Testbed one executes decoupled subsystem 1 that includes $BA_1$ to $BA_k$ and Testbed two executes decoupled subsystem 2 that includes $BA_{k+1}$ to $BA_z$. System variables are exchanged at communication points using interface models (i.e. interface models 1 and 2). Further, it emulates geographically dispersed substations and control centres, similar to the PCPF. Although it exhibits high computational efficiency, there exist particular challenges in terms of model partitioning and synchronisation, time delay, and data exchange rates that may affect the stability and accuracy of the DCPF during the real-time simulation.

## 3.3 | Federated testbed design

Figure 3 presents a high-level design architecture of NEFTSec for implementing the aforementioned conceptual architectures and performing cybersecurity-related experiments. We have explored the NASPI network (NASPInet) architecture [4] to develop this industry-grade infrastructure to support the bi-directional sharing of data in secure, reliable, and robust ways. Figure 4 presents the HIL federated testbed that facilitates the supervisory control and data acquisition (SCADA)

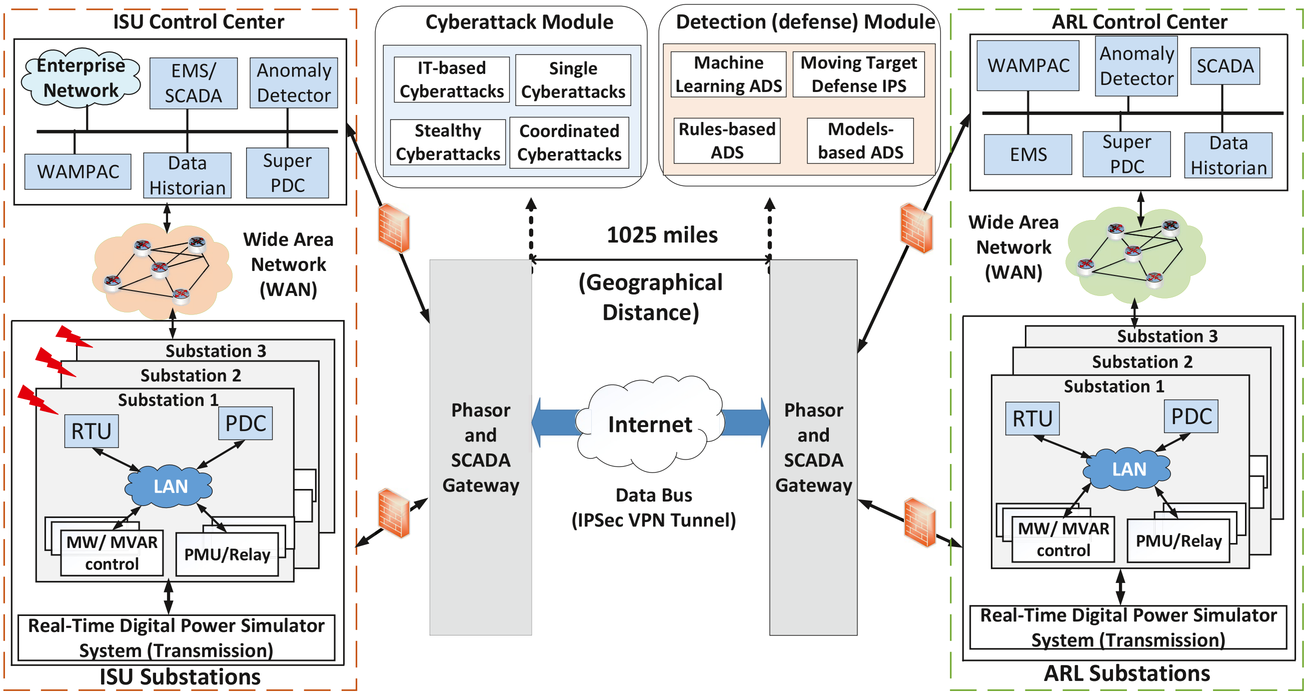


FIGURE 3 NASPInet-inspired high-level design architecture of networked federation testbed (NEFTSec)

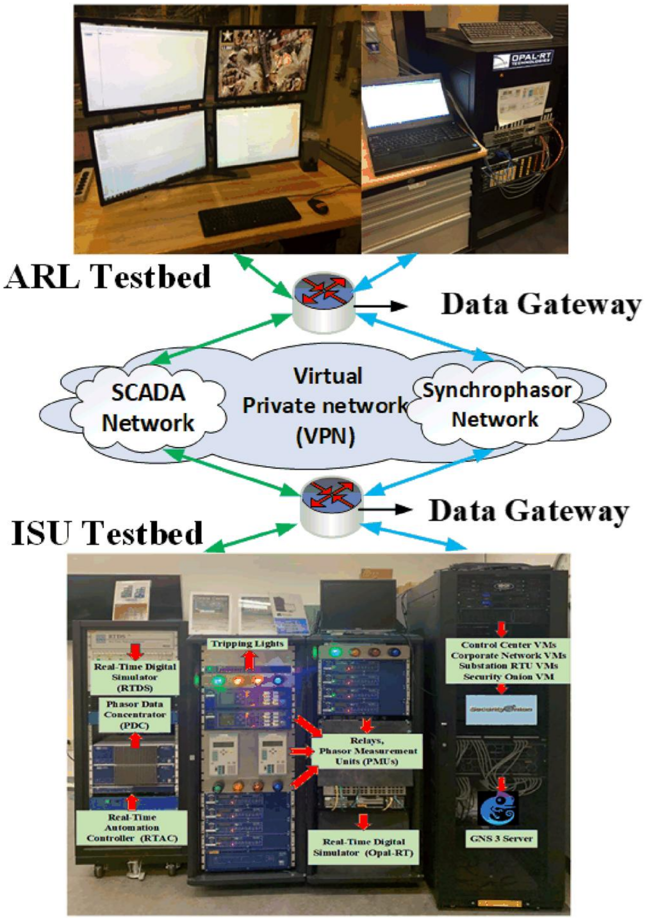

OPAL-RT
ARL Testbed
Data Gateway
SCADA Network
Virtual Private network (VPN)
Synchrophasor Network
Data Gateway
ISU Testbed
Real-Time Digital Simulator (RTDS)
Phasor Data Concentrator (PDC)
Real-Time Automation Controller (RTAC)
Tripping Lights
Relays, Phasor Measurement Units (PMUs)
Real-Time Digital Simulator (Opal-RT)
Control Center VMs
Corporate Network VMs
Substation RTU VMs
Security Onion VM
GNS 3 Server

FIGURE 4 Hardware-in-the-loop (HIL) federated testbed using Iowa State University (ISU) and Army Research Laboratory (ARL) testbeds

and synchrophasor-based closed-loop communication using resources of these two testbeds. Generally, the conceptual architecture of NASPInet consists of a data bus (DB) and phasor gateways, where the grid measurements are shared among multiple utilities and control centres in the standard, secure, expandable, and decentralised fashion. The major components are elaborated in this section.

**Data bus (DB)**: Includes a wide-area network (WAN) and the associated services to enable the connection, QoS, data monitoring, etc. In this architecture, we have chosen the internet-based communication medium for the WAN and the internet protocol security (IPSec) VPN tunnel is configured with the UDP protocol. The two separate networks exchange the internal and end point certificates to allow secure communication at a geographical distance of 1025 miles.

**Data Gateway**: Provides a sole access point for sending and receiving data through the DB. We have deployed pfSense software at the ISU network as a data gateway. It is configured as a firewall and router to configure devices, monitor network packets, and QoS.

**Substation Network**: The PowerCyber substation network consists of various field devices, such as multifunctional relays (SIPROTEC 7SJ610/7SJ82) and PMUs (Schweitzer Engineering Laboratories [SEL]-421), which communicates to the station phasor data concentrators (PDC) (SEL-3573) and remote terminal units (RTUs; SICAM PAS and SEL-Real-Time Automation Controller) using communication protocols (Distributed Network Protocol 3, International Electrotechnical Commission (IEC) 61850, and IEEE C37.118), also shown in Figure 4. It also uses real-time simulators (OPAL-RT and RTDS) to simulate the power system topology. From the Army Research Laboratory (ARL) testbed, the OPAL-RT is utilised to simulate the power system topology and to model virtual PMUs and relays that interact with software-based PDCs and RTUs [23].

**Control Centre Network**: The PowerCyber control centre network at ISU includes Siemens and General Electric energy management system (EMS)/SCADA systems (Siemens Power, GE e-terraplatform) with WAMPAC applications, data servers (open-PDC, Open Platform Communications and MySQL servers), and a real-time visualisation dashboard. Similar sets of open-source software are operating at the ARL control centre network to support grid communication and EMS-based WAMPAC applications.

**Cyberattack Module**: It includes a library of software components that are grouped together as a module to implement cyberattacks in a federated testbed environment. This module includes IT-based attacks (ping, nmap scanning, and OpenVAS scanning), single cyberattacks (line tripping attack and denial of service attack), stealthy cyberattacks (Man-in-the-Middle (MITM) attack and malware installation), etc., and coordinated cyberatttacks as discussed in previous works [6, 23, 24].

**Detection (Defence) Module**: It includes state-of-the-art detection and defence solutions, such as rule, model, and machine learning-based anomaly detection systems, moving target defence, etc., as developed in earlier research efforts [23, 24], which can be utilised to test, validate, and evaluate system performances with a detailed network analysis using this NEFTSec platform.

## 4 | DISTRIBUTED CYBER-PHYSICAL FEDERATION

### 4.1 | Proposed co-simulation interface algorithm

As a time-domain signal is not appropriate for sending instantaneous values through the packet-based communication [16] in DCPF, the CIA is proposed that couples the decoupled subsystems, simulated in the electromagnetic transient (EMT) domain at distant locations. Figure 5 shows the proposed CIA that facilitates the bi-directional communication between two decoupled subsystems, subsystem $X$ and subsystem Y while assuming a balanced three-phase system. It consists of several steps that are discussed in greater details here. The overall proposed CIA is summarised in Algorithm 1.

**Step 1** (Apply TLM): This decoupling technique transforms the given system into its Norton equivalent form and voltage sources are connected at the boundary buses, which interchange their respective values at each time step to determine the parameters of the companion model. The voltages at subsystem $X$, $Vxs_{abc}(t_k)$, and subsystem Y, $Vys_{abc}(t_k)$, at a time step, $t_k$, are computed using Equations (1) and (2) for all three phase sources. The impedance, $Z_l$, for an inductor is $L/T$, where $T$ is a simulation time step and $L$ is an inductance. Note that this TLM technique is selected because of its high efficiency and accuracy of decoupling the given system into several subsystems [25].

$$Vxs_{abc}(t_k) = I_x(t_k) * Z_l + Vyd_{abc}(t_k) \tag{1}$$

$$Vys_{abc}(t_k) = I_y(t_k) * Z_l + Vxd_{abc}(t_k) \tag{2}$$

**Step 2** (Estimate phasor values): Convert the time domain signal, $Vxs_{abc}(t_k)$, coming from the subsystem $X$, into a phasor domain by decomposing the instantaneous three-phase voltage signals ($Vxs_a$, $Vxs_b$, and $Vxs_c$) into the dq0 frame by computing direct ($Vxs_d$), quadrature ($Vxs_q$), and zero components ($Vxs_0$) using Park's transformation, by substituting (3) into (4), and later computing the fundamental frequency ($f_o$) and angle ($\omega_o t_k$) of three-phase voltages using the synchronous reference-frame phase-locked loop [26]. Finally, the decomposed components are converted into a phasor domain, ($Vpxs$ $(t_k)$ = [$Vmx$, $\theta_{ix}$, $T_{gps}$]), by computing voltage magnitude ($Vmx$) and phase angle ($\theta_{ix}$) with a time stamp ($T_{gps}$) of the fundamental frequency of a given signal, $Vxs_{abc}(t_k)$, over a running window of one cycle based on the Fourier analysis of a periodic voltage signal, as shown in Equations (5)–(8). The magnitude and phase angle are computed as $Vmx = \sqrt{a^2 + b^2}$ and $\theta_{ix}$ = arctan$(b/a)$. Same sequence of steps is followed to compute $Vpys(t_k)$ from $Vys_{abc}(t_k)$.

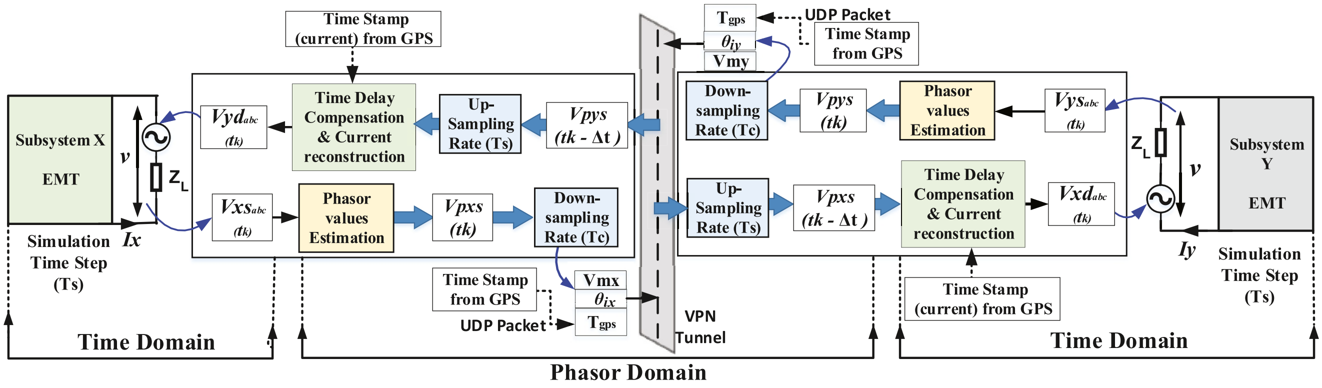


**FIGURE 5** Proposed co-simulation interface algorithm (CIA) for geographically dispersed real-time distributed simulation in transmission systems

**Algorithm 1 Proposed CIA for GD RTDS**

```
$Vxs_{abc}$ $Vxd_{abc}$ : set $Z_l = L/T$ and $T_c$
while $t \geq t_o$ do
    Compute $Vpxs(t_k) = [Vm, \theta_i, T_{gps}]$
    Exchange data at sampling rate $T_c$
    Calculate Vxd$_{abc}$
    if models converge then
        continue simulation
    else
        stop the simulation
    end
    Similarly, compute $Vyd_{abc}$ from $Vys_{abc}$ in parallel
end
```

$$P = \frac{2}{3}\begin{bmatrix} \cos(\omega t) & \cos(\omega t - 2\pi/3) & \cos(\omega t + 2\pi/3) \\ -\sin(\omega t) & -\sin(\omega t - 2\pi/3) & -\sin(\omega t + 2\pi/3) \\ 1/2 & 1/2 & 1/2 \end{bmatrix} \tag{3}$$

$$\begin{bmatrix} Vxs_d \\ Vxs_q \\ Vxs_o \end{bmatrix} = P \begin{bmatrix} Vxs_a \\ Vxs_b \\ Vxs_c \end{bmatrix} \tag{4}$$

$$Vxs_{abc}(t_k) = a\cos(\omega_o t_k) + b\sin(\omega_o t_k) \tag{5}$$

$$a = \frac{2}{T}\int_{t-T}^{t} Vxs_{abc}(t_k)\cos(\omega_o t_k)dt \tag{6}$$

$$b = \frac{2}{T}\int_{t-T}^{t} Vxs_{abc}(t_k)\sin(\omega_o t_k)dt \tag{7}$$

$$\omega_o = (2\pi f_o), T = \frac{1}{f_o} \tag{8}$$

**Step 3** (Compute down-sampling rate ($T_c$)): This step computes $T_c$ by performing a closed-loop testing between two distant simulators as needed for reliable data exchange over the VPN tunnel, and later re-scaling (up-sampling) to the original simulation time step ($T_s$) at the receiving end to facilitate the EMT simulation.

**Step 4** (Perform time-delay compensation and signal reconstruction): This step includes voltage signals reconstruction by computing $Vxd_{abc}(t_k)$ at the subsystem Y and $Vyd_{abc}(t_k)$ at the subsystem X. For computing $Vxd_{abc}(t_k)$, the time delay is compensated by adding a phase shift [27], ($2\pi f_o \Delta t_k$), as shown in Equation (9). In this equation, $\Delta t_k$ is the computed time difference at the simulation time $t_k$ between the current GPS time stamp of the received signal and the sent one. Note that the GPS time clock also provides a standard time reference-based synchronisation to minimise model error due to out-of-step starting times between distant simulators.

$$Vxd_{abc}(t_k) = V\,mx(t_k)\sin\left(\int 2\pi f t_k + \phi_i(t_k) + 2\pi f_o \Delta t_k\right) \tag{9}$$

**Step 5** (Interchange phasor values): Continue interchanging system variables ($Vpxs$ & $Vpys$) in the phasor domain at a lower sampling rate ($T_c$) between two distant simulators at communication end points. If the partitioned models converge, continue with the GD-RTDS, otherwise stop the simulation.

## 5 | CASE STUDIES AND EXPERIMENTAL SETUP

### 5.1 | Cyber federation case study

The cyber federation relies on an internet-based communication medium that is subject to various delays, such as network processing delay, transmission delay, etc., as well as packet loss. This platform is utilised to analyse the wide-area communication network during bi-directional data exchange between substation and control centre networks for the EMS-based WAMPAC applications in real time.

### 5.2 | Distributed cyber-physical federation case study

This platform is utilised to perform GD-RTDS on transmission systems in the EMT domain. In this context, we have developed a TLM-based CIA to maintain simulation fidelity during GD-RTDS. We have utilised this CPF platform for cybersecurity-based experimental testing, signal analysis, and validation of the proposed CIA in real time.

### 5.3 | Experimental setup

Figure 6 presents a HIL experimental setup to perform CF- and DCPF-related cybersecurity experiments in the EMT domain. During the CF, the substation network is operating in the PowerCyber testbed, where the modified IEEE 39 bus system is running as a test case in the ARTEMiS-SSN (eMEGASIM) solver using the OPAL-RT simulator. The simulator is also mapped to physical relays with modelled transmission lines using the IEC-61850 (Generic Object Oriented System-wide Events) protocol. The virtual PMU drivers are also modelled to send phasor measurements to the ARL control centre to support synchrophasor-based WAMPAC applications. During the DCPF-based GD-RTDS experiment, a first-order two-bus system is decoupled at the transmission line to partition into load and source subsystems. A voltage source with an impedance is connected in series to represent the missing subsystem. The partitioned load and source subsystems are running in the PowerCyber and ARL testbeds in the OPAL-RT real-time simulators at a smaller time step of 50 $\mu$s ($T_s$) that are located at a geographical distance of around 1025 miles. Further, these simulators are synchronised to a GPS time clock while exchanging bi-directional data over the internet-based IPSec VPN tunnel.

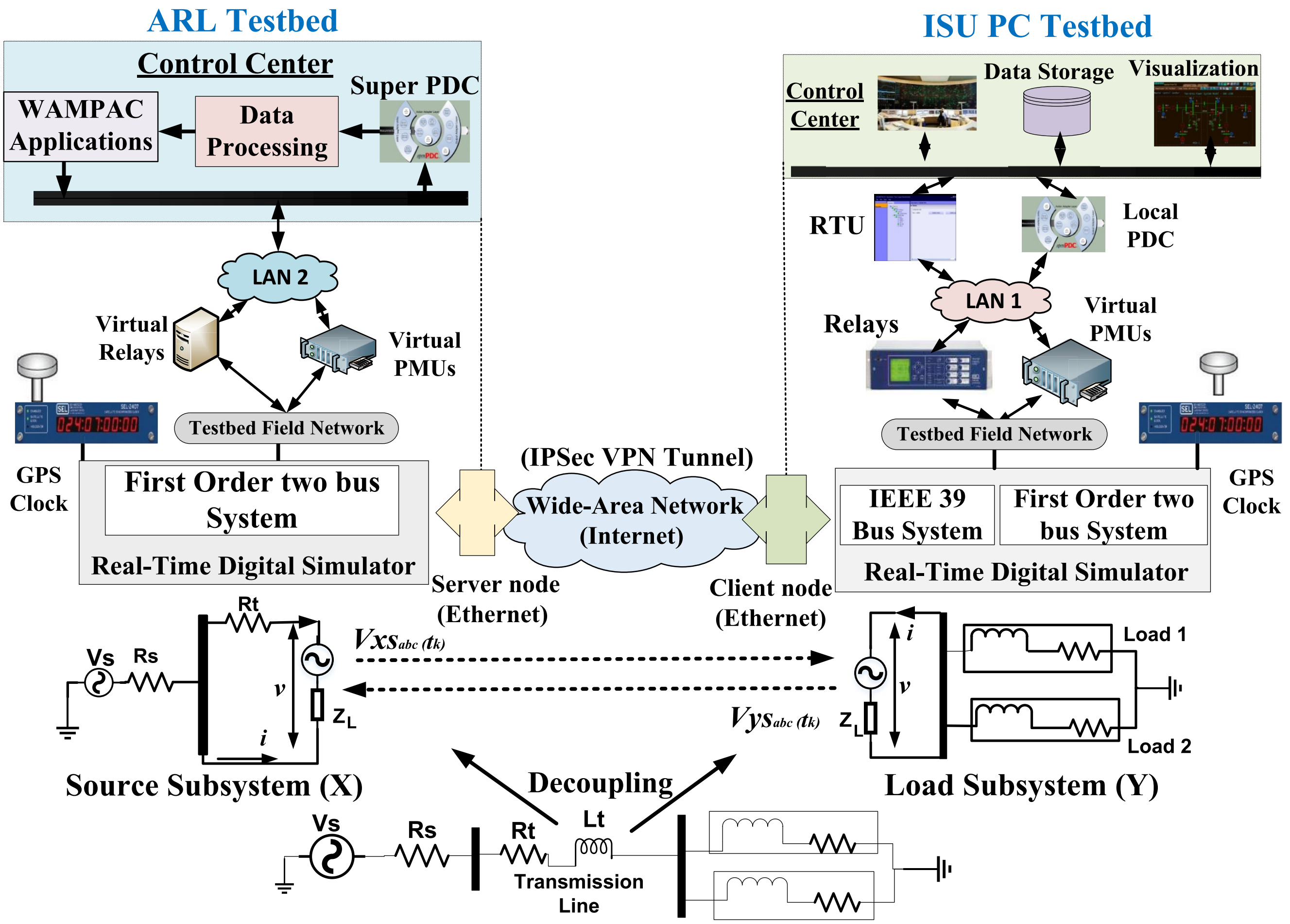


**FIGURE 6** Experimental setup using Iowa State University (ISU) PC and Army Research Laboratory (ARL) cybersecurity testbeds

## 6 | RESULTS AND DISCUSSIONS

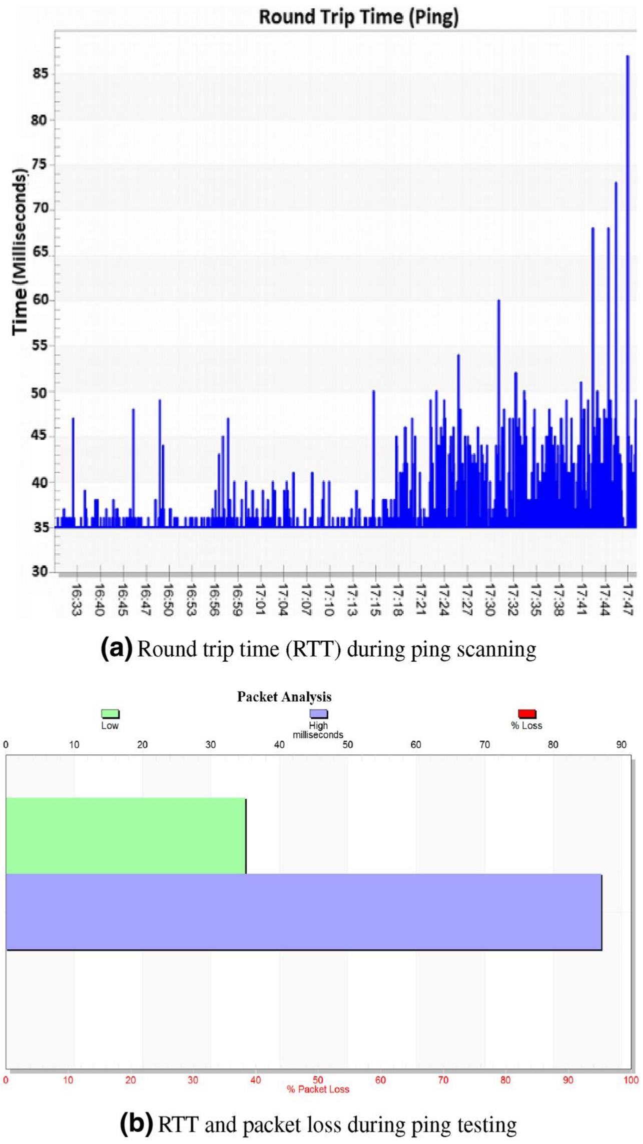
### 6.1 | Network packet analysis during CF

Since data latency and packet loss are two key challenges for performing CF-level experiments due to the internet-based communication medium, we have performed the network packet analysis in terms of network latency, packets drop, and communication bandwidth.

(a) **Communication Latency**: We have computed the wide-area communication latency in terms of round trip time (RTT) and communication delays. For computing the RTT delay, ping scanning is performed by pinging the ARL control centre every 0.5 *s*. Figure 7a shows the ping latency distribution, where the maximum RTT is computed around 87 *ms* and the minimum around 35 *ms*. Further, the experimental analysis reveals that there is a 0% packet loss during the ping testing in real time as shown in the red bar of bar graph in Figure 7b. It ensures a reliable communication network between two separate testbeds. We have also computed RTT of synchrophasor packets while varying the sampling rate from 60 to 20 frames/sec as shown in Table 2, and the average RTT has increased from 16.5 to 37 *ms*. Figure 8 shows the RTT of synchrophasor packets at a sampling rate of 60 frames/sec that has a minimum value of 6.15 *ms* and a maximum value of 25.9 *ms*.

(b) **Communication Bandwidth**: We have computed the PMU bandwidth requirements for different sampling rates, varying from 60 frames/sec to 20 frames/sec, also shown in Table 2. For a sampling rate of 60 frames/sec, the average value of computed bandwidth is approximately 15,250 byte/sec with a minimum value of 15,000 byte/sec and a maximum value of 15,300 byte/sec for the modelled phasors in the IEEE 39 bus system. Note that although the fast PMU measurements provide better grid visibility, the communication bandwidth also increases with an increase in the sampling rate.

(c) **PMU Communication Delay**: Since the communication between the ISU and ARL testbeds is a major latency factor, we have computed the communication latency for the incoming live-streaming PMU data. It is computed as the time delay from when the PMU measurements leave the local PDC of ISU substation and is received at the super PDC of ARL control centre. Figure 9 shows the variation in a data delay for different numbers of PMU packets. We have observed that the average value of computed delay is 16.6 ms with a minimum value of



**(a)** Round trip time (RTT) during ping scanning

**(b)** RTT and packet loss during ping testing

**FIGURE 7** Network packet analysis during ping scanning

**TABLE 2** Computed round trip time (RTT) and bandwidth of synchrophasor network packets

| RTT (ms) | | | |
|---|---|---|---|
| **Frames** | **Maximum** | **Minimum** | **Average** |
| 60 | 25.9 | 6.15 | 16.5 |
| 30 | 50.6 | 14.8 | 35.43 |
| 20 | 58.4 | 16.4 | 37 |
| **Bandwidth (Bytes/sec)** | | | |
| **Frames** | **Maximum** | **Minimum** | **Average** |
| 60 | 15,300 | 15,000 | 15248.873 |
| 30 | 7932 | 7422 | 7668.33 |
| 20 | 5650 | 5034 | 5240 |

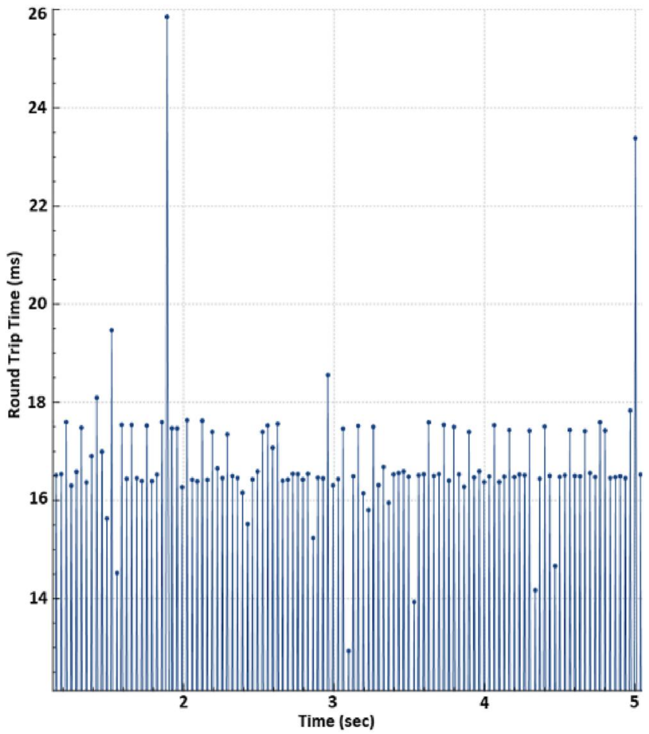


**FIGURE 8** Round trip time (RTT) for synchrophasors at 60 frames/sec

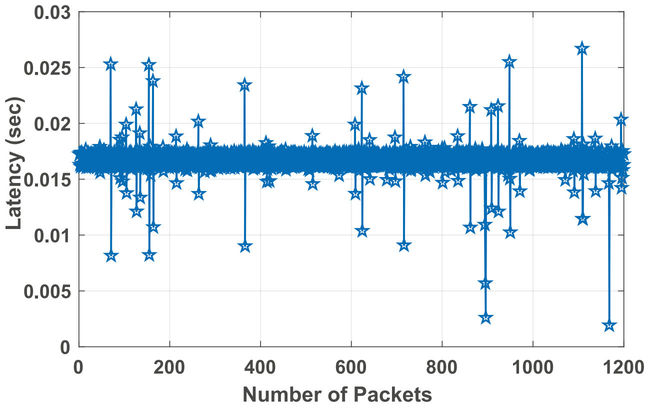


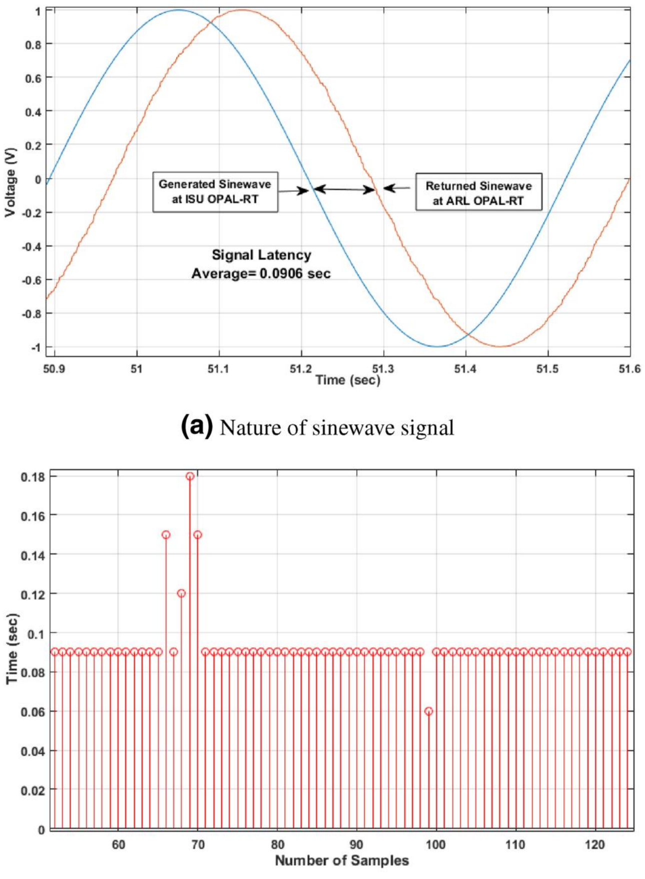
**FIGURE 9** Latency for phasor measurement unit (PMU) packets delay during live-streaming

1.9 ms and a maximum value of 26.7 ms. Note that the computed maximum PMU delay complies with the designated communication latency (38 *ms*) of WAPS in the Southern California Edison [28], 60–100 *ms* latency of wide-area voltage controller (WAVC) in the Bonneville Power Administration [29], and 100–200 ms latency of wide-area damping controller (WADC) in the Pacific DC Inter-tie (PDCI) in the North American Western Interconnection [30, 31]. Table 3 shows a list of different WAMPAC applications with their operational time (*sec*) that varies from 150 *ms* (WAVC) to 300 sec (Real-Time Contingency Analysis). Hence, this CF platform can be utilised to validate these applications in real time.

**TABLE 3** Operating time of different wide-area monitoring, protection, and control (WAMPAC) applications

| WAPAC Application | Operation Time (sec) |
|---|---|
| WAVC [29] | 0.15–0.3 |
| WAPS [28, 32] | 0.05–0.15 |
| WADC [30] | 1–10 |
| Real-time contingency analysis (RTCA) [32] | 60–300 |

Abbreviations: RTCA, Real-Time Contingency Analysis; WADC, wide-area damping control; WAPAC, wide-area protection and control; WAPS, wide-area protection scheme; WAVC, wide-area voltage controller.



**(a)** Nature of sinewave signal

**(b)** Round trip time (RTT) latency

**FIGURE 10** Generated and returned sinewaves at the Iowa State University (ISU) testbed's OPAL-RT simulator

## 6.2 | Experimental evaluation during DCPF

We have applied the proposed CIA by initially performing a closed-loop test to compute $T_c$, analyse the communication latency, and the nature of the incoming signal. Further, we have analysed the simulation fidelity of the GD-RTDS through the model validation.

### 6.2.1 | Close-loop testing

After the detailed investigation and rigorous testing, closed-loop testing is successfully performed using real-time simulators at the PowerCyber and ARL testbeds by sending a continuous sine wave of frequency $10/2\pi$ Hz from the ISU testbed's simulator to the ARL testbed's simulator using the ethernet-based communication interface with a Transmission Control Protocol/Internet Protocol end point connection at a time step of 30 ms. Figure 10 shows the comparison between generated continuous and returned discrete sine waves between two distant simulators with an average RTT latency of 90.6 ms, a maximum of 180 ms, and a minimum value of 60 ms with a zero packet loss.

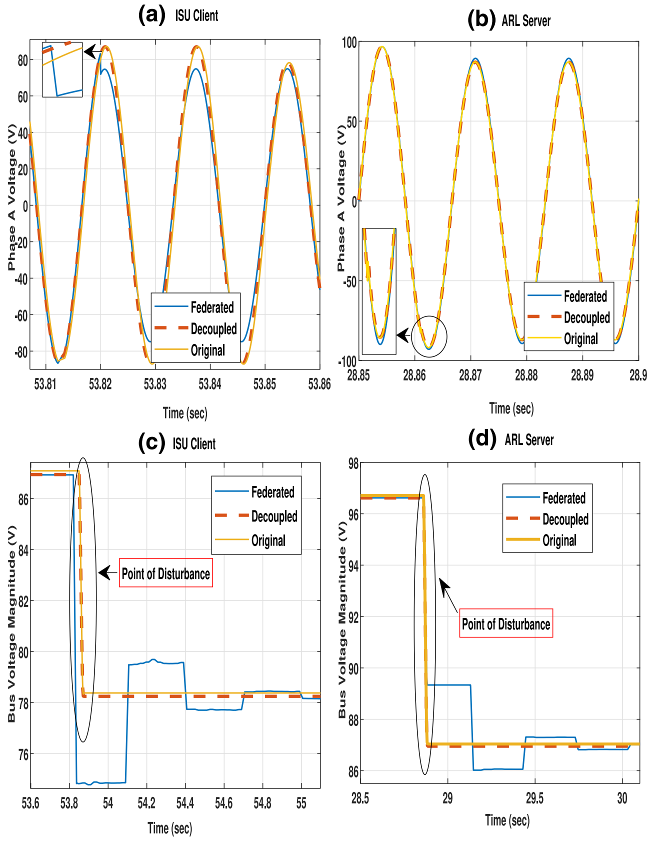


**FIGURE 11** Reconstructed voltage signals (a and b) and phasor magnitude values (c and d) during the voltage sag

### 6.2.2 | Simulation fidelity during DCPF

Previous experimental results reveal a reliable data exchange rate ($T_c$ = 30 ms) for operating client-server communication interfaces during the GD-RTDS using a first-order two-bus system. To assess the simulation fidelity while applying the proposed CIA, we have performed the model validation by considering three cases as original, decoupled, and federated (GD-RTDS) systems. We have first performed voltage sag, as a physical disturbance, by reducing the magnitude of source voltate (V) from 120 to 108 V. Second, a load tripping-based cyberattack is performed by maliciously tripping a relay directly connected to load 1.

Figure 11 presents the reconstructed voltage signals (a, b) and phasor voltage magnitudes (c, d) of all three cases during the voltage sag from the ISU client and ARL server sides.

**TABLE 4** Model validation error during the voltage sag

| Parameters | ISU client | ARL server |
|---|---|---|
| **Federated system** | | |
| MAE | 0.6792 | 0.3949 |
| MAPE (%) | 0.8587 | 0.4505 |
| MxAE | 5.327 | 2.2977 |
| **Decoupled system** | | |
| MAE | 0.1318 | 0.0883 |
| MAPE (%) | 0.1671 | 0.0983 |
| MxAE | 0.1821 | 0.0951 |

Abbreviations: ARL, Army Research Laboratory; ISU, Iowa State University.

Table 4 presents a quantitative performance measures in terms of mean absolute error (MAE), mean absolute percentage error (MAPE), and maximum absolute error (MxAE) of the voltage magnitude during 3 s of dynamic simulation. In this case, we observe a higher voltage magnitude error in the federated system compared to the decoupled system in both server and client sides. The computed signal errors are high at the point of disturbance during the transient simulation as highlighted through the zoomed portions in Figure 11a,b and ovals in Figure 11c,d with the MAE of 0.6792, MAPE of 0.8587%, and MxAE of 5.327 from the client side, and the MAE of 0.3949, MAPE of 0.4505%, and MxAE of 2.2977 from the server side in federated system.

Figure 12 presents voltage plots of all three cases during a load tripping attack from the ISU client and ARL server sides. We also observe a similar trend in this scenario where the federated system is relatively exhibiting a high signal error compared to the decoupled system. In this case, we observe an MAE of 0.3136, MAPE of 0.3434%, and MxAE of 6.787 from the ISU client side, and the MAE of 0.1227, MAPE of 0.1263%, and MxAE of 3.7364 from the ARL server side with respect to the original system (Table 5). Our experimental analysis reveals that the computed voltage error is dissimilar for different scenarios as the computed voltage error is higher during the voltage sag compared to the load tripping attack for decoupled and federated systems. Note that the proposed federated system shows negligible error during the steady state that is illustrated in the reconstructed voltage signals in Figure 11a,b and Figure 12a,b. It clearly illustrates that the proposed CIA algorithm ensures simulation fidelity by compensating time delays as the reconstructed phase A voltage compares closely with decoupled and original systems during the real-time simulation for the steady state. In both cases, the computed signal error gets amplified during transient states due to injected disturbances before restoring back to the normal steady state.

We have also computed the norm-2 error of phasor magnitudes as a simulation fidelity metric using (10) over a moving window of 10 samples to adequately characterise the error in federated and decoupled systems from client and server sides during the load tripping attack. In this equation, $v$ is the phasor voltage magnitude of decoupled/federated systems and $v_r$ represents the phasor voltage magnitude of original systems.

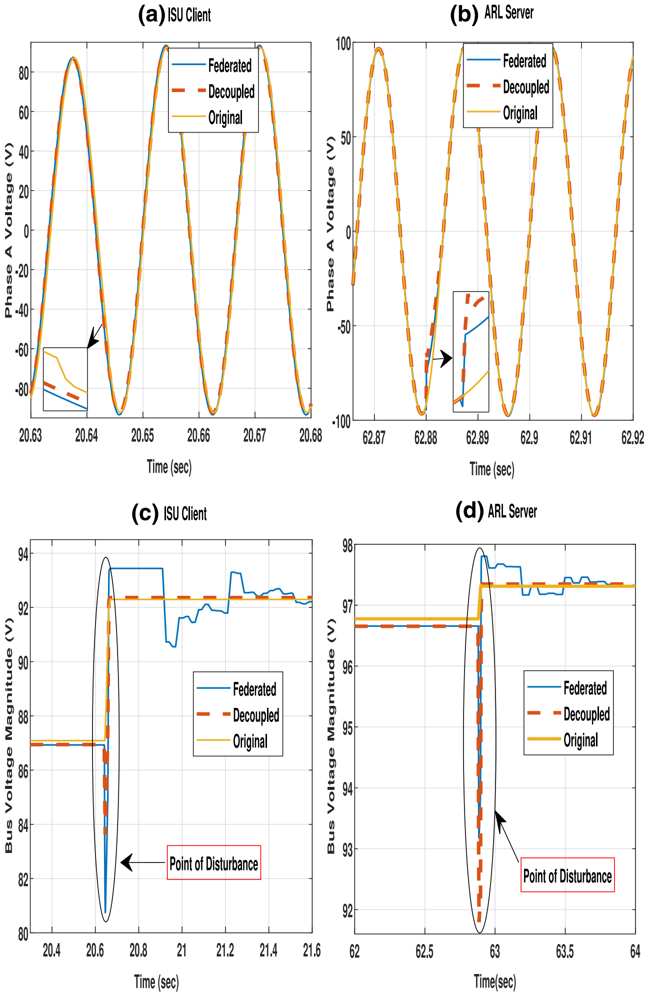


**FIGURE 12** Reconstructed voltage signals (a and b) and phasor magnitude values (c and d) during the load tripping attack

**TABLE 5** Model validation error during the load tripping attack

| Parameters | ISU client | ARL server |
|---|---|---|
| **Federated system** | | |
| MAE | 0.3136 | 0.1227 |
| MAPE (%) | 0.3434 | 0.1263 |
| MxAE | 6.787 | 3.7364 |
| **Decoupled system** | | |
| MAE | 0.1051 | 0.0894 |
| MAPE (%) | 0.1167 | 0.0667 |
| MxAE | 3.8913 | 5.1296 |

Abbreviation: ARL, Army Research Laboratory; ISU, Iowa State University; MAE, mean absolute error.

$$E_2 = \frac{v - v_{r2}}{v_{r2}} \tag{10}$$

Figure 13 indicates that the 2-norm error of the federated system from the ISU client side is relatively large with the

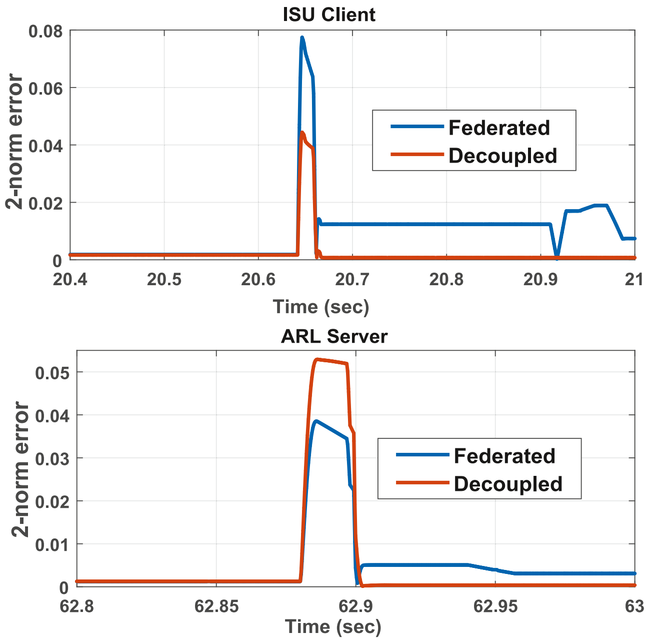


**FIGURE 13** 2-norm error of phasor magnitudes during the load tripping attack

**TABLE 6** Quantitative comparison of different federation architectures

| Parameters | CF | PCPF | DCPF |
|---|---|---|---|
| Overunning | 228 | 13 | 11 |
| Computation usage (%) | 36.97% | 31.96% | 9.54% |
| Average major computation ($\mu$s) | 13.69 | 11.39 | 6.8 |
| Average minor computation ($\mu$s) | 1.91 | 1.71 | 1.02 |
| Average execution cycle ($\mu$s) | 18.49 | 15.98 | 9.53 |

Abbreviations: DCPF, Distributed CPF; PCPF, Parallel CPF.

computed value of 0.077 compared to the ARL server side that shows the value of 0.0529 at the point of disturbance. We also observe a higher error of margin between the federated and decoupled systems at the ISU client side as compared to the ARL server side during disturbances. In both cases, the 2-norm errors eventually reduce to the initial minimum value after disturbances are removed.

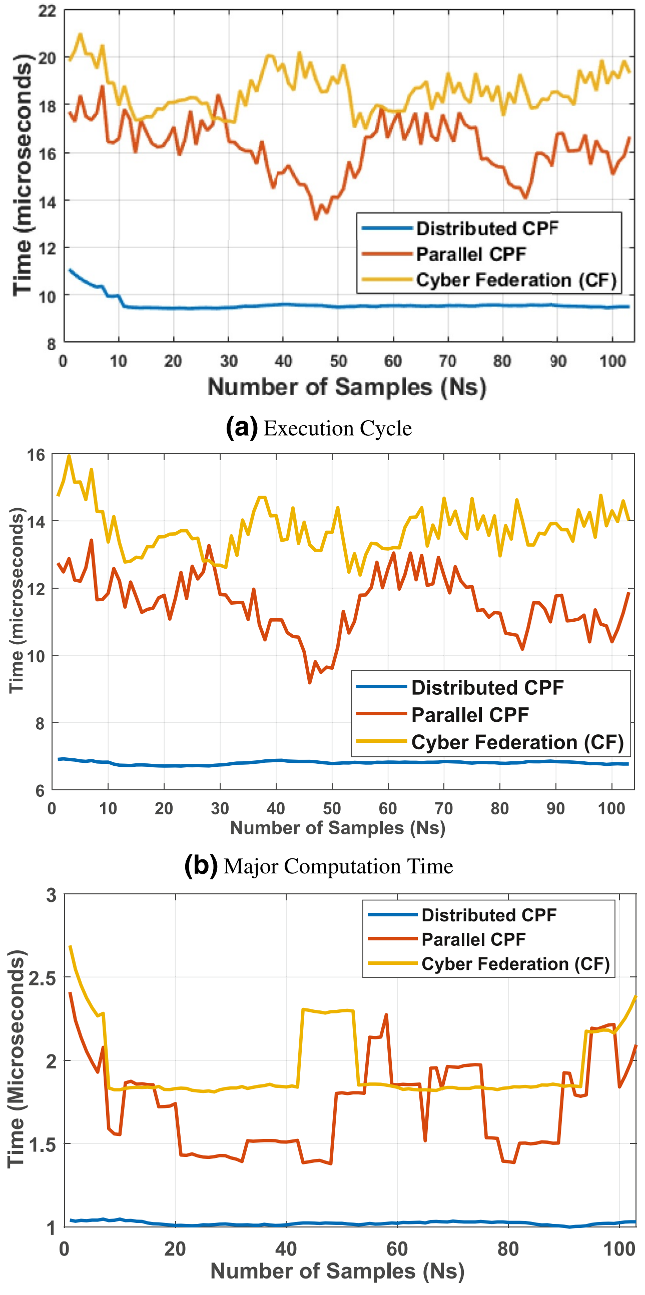
### 6.3 | Real-time simulation analysis

We have also performed the quantitative comparison of CF, PCPF, and DCPF architectures using simulation parameters, as shown in Table 6, during the real-time execution of the first-order two-bus system for 500 s. In this case, we observe 228 instances of overrunning during the CF, 13 instances of overrunning in the PCPF, and 11 instances of overrunning in the DCPF, where the given system did not simulate in the specified time step, that is, 50 $\mu$s. Higher overrunning during CF and PCPF simulations reveals higher computational power requirements compared to the DCPF simulation. Also, the computation usage during the simulation is low in DCPF compared to other federation architectures. We observe a similar trend in other performance parameters, including average major computation, minor computation, and average execution cycle where their values are high in CF and low in DCPF. Average computation time represents the average time taken by the model to perform block calculations that include discrete and continuous states' calculation and algebraic calculation for a major time step (average major computation) and minor time step (average minor computation). Average execution time includes the average time taken to compute all model tasks, such as major and minor computation, and simulator overhead and services.

Figure 14 shows the computed parameters (execution cycle (a) and major and minor computation times (b and c)) with respect to the number of samples where the DCPF shows the consistent performance for all parameters. Higher values of these parameters during the CF and PCPF put restrictions on the system size and indicate that a larger number of cores is required to perform real-time simulation compared to the DCPF while supporting HIL testing and communication data exchange.

## 7 | CONCLUSION AND FUTURE WORKS

In this paper, we presented the conceptual architecture, testbed design, and several applications of the networked federation testbed in the context of smart grid cybersecurity. We described the implementation of proposed federation architectures by integrating Iowa State University's PowerCyber Laboratory and the US ARL to conduct CF and DCPF experiments for different case studies. Further, we introduced the CIA to ensure simulation fidelity while performing the DCPF experiments by applying the TLM-based decoupling technique, estimating phasor values, and interchanging system variables at a down-sampled rate. For detailed case studies, we utilised the IEEE 39 bus system and performed a network packet analysis to validate the application of CF platform to support WAPS-related cybersecurity experiments. During the DCPF, we decoupled a first-order two-bus system to perform GD-RTDS and analysed the simulation fidelity using several performance measures while validating decoupled models during the load tripping attack. We observed that the proposed CIA efficiently preserves the simulation fidelity during the steady state; however, the model error gets amplified during the transient state that varies at client and server sides. We also performed the quantitative comparison of different federation architectures during the real-time simulation and observed that the DCPF exhibits lower overrunning and computation usage as compared to CF and PCPF. For future works, we plan to explore the efficacy and feasibility of federated testbeds for a broader case of wide-area monitoring, protection, and control applications of the smart grid. Further, this research opens up several avenues for further research, which include:



**(a)** Execution Cycle

**(b)** Major Computation Time

**(c)** Minor Computation Time

**FIGURE 14** Real-time simulation parameters during federation-level experiments for CF, parallel CPF (PCPF), and distributed CPF (DCPF)

(1) Development of CIA for the unbalanced three-phase system and performing the detailed analysis while also considering high-frequency components in the voltage profile.
(2) Design a real-time predictor model to improve model accuracy during the GD-RTDS at DCPF level and develop NASPI-inspired network interfaces to federate multiple CPS testbeds.

## ACKNOWLEDGEMENTS

This research is funded in part by US NSF Grant # CNS 1446831 and US DOE Grant # DE-EE0008773.

## CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

## DATA AVAILABILITY STATEMENT

The authors declare that all the data applied in this manuscript is open source and publicly available.

## ORCID

*Vivek Kumar Singh* https://orcid.org/0000-0002-5909-3454

## REFERENCES

1. Hahn, A., et al.: Cyber-physical security testbeds: architecture, application, and evaluation for smart grid. IEEE Trans. Smart Grid 4(2), 847–855 (2013). https://doi.org/10.1109/tsg.2012.2226919
2. Cintuglu, M.H., et al.: A survey on smart grid cyber-physical system testbeds. IEEE Commun. Surv. Tutorials 19(1), 446–464 (2017). https://doi.org/10.1109/comst.2016.2627399
3. NIST.: Cyber-Physical Systems for Testbed Design (2016)
4. North American SynchroPhasor Initiative.: Data Bus Technical Specifications for North American Synchro-Phasor Initiative Network (2009)
5. Bobba, R., et al.: Exploring a tiered architecture for NASPInet. In: 2010 Innovative Smart Grid Technologies (ISGT), pp. 1–8 (2010)
6. Singh, V.K., et al.: Evaluation of anomaly detection for wide-area protection using cyber federation testbed. In: 2019 IEEE Power Energy Society General Meeting (PESGM), pp. 1–5. Atlanta (2019)
7. Ricci, R., et al.: Designing a Federated Testbed as a Distributed System. TRIDENTCOM (2012)
8. Palmintier, B., et al.: A power-hardware-in-the-loop platform with-Remote distribution circuit Co-simulation. IEEE Trans. Ind. Electron. 62(4), 2236–2245 (2015). https://doi.org/10.1109/tie.2014.2367462
9. Lammers, H.: INL and NREL Demonstrate Power Grid Simulation at a Distance URL (2015)
10. Chakrabortty, A. et al.: A US-wide DETERWAMS-ExoGENI testbed for wide-area monitoring and control of power systems using distributed synchrophasors. Accessed 15 March 2016
11. Ashok, A., Wang, P., Govindarasu, M.: Cyber-physical-social system security testbeds for an attack-resilient smart grid energy engineering. In: Cyber-Physical-Social Systems and Constructs in Electric Power Engineering, vol. 16, pp. 433–449 (2016)
12. Cristaldi, L., et al.: A virtual environment for remote testing of complex systems. IEEE Trans. Instrum. Meas. 54(1), 123–133 (2005). https://doi.org/10.1109/TIM.2004.834067
13. Faruque, M.O., et al.: Thermo-electric co-simulation on geographically distributed real-time simulators. In: 2009 IEEE Power Energy Society General Meeting, pp. 1–7 (2009)
14. Monti, A., et al.: A global real-time superlab: enabling high penetration of power electronics in the electric grid. IEEE Power Electron. Mag. 5(3), 35–44 (2018). https://doi.org/10.1109/mpel.2018.2850698
15. Huang, Q., et al.: Power system decoupled simulation in MATLAB/SIMULINK. In: 2008 40th North American Power Symposium, pp. 1–8 Calgary (2008)
16. Ravikumar, K., Schulz, N., Srivastava, A.: Distributed simulation of power systems using real-time digital simulator. In: IEEE/PES Power Systems Conference and Exposition, pp. 1–6. PSCE '09 (2009)
17. Jalili-Marandi, V., et al.: Real-time Electromagnetic and Transient Stability Simulations for Active Distribution Networks (2013)
18. Stevic, M., et al.: A bilateral teleoperation approach for interface algorithms in distributed real-time simulations. In: 2018 IEEE Workshop on Complexity in Engineering (COMPENG), pp. 1–5. Florence (2018)
19. Stevic, M., et al.: Multi-site European framework for real-time co-simulation of power systems. IET Gener. Transm. Distrib. 11(17), 4126–4135 (2017). https://doi.org/10.1049/iet-gtd.2016.1576
20. Bharati, A.K., Ajjarapu, V.: SMTD Co-simulation framework with HELICS for future-grid analysis and synthetic measurement-data generation. IEEE Trans. Ind. Appl. 58(1), 131–141 (2022). https://doi.org/10.1109/TIA.2021.3123925

21. Huang, Q., Vittal, V.: Integrated transmission and distribution system power flow and dynamic simulation using mixed three-sequence/three-phase modeling. IEEE Trans. Power Syst. 32(5), 3704–3714 (2017). https://doi.org/10.1109/tpwrs.2016.2638910
22. Bharati, A.K., Ajjarapu, V.: Investigation of relevant distribution system representation with DG for voltage stability margin assessment. IEEE Trans. Power Syst. 35(3), 2072–2081 (2020). https://doi.org/10.1109/tpwrs.2019.2950132
23. Singh, V.K., et al.: Testbed-based evaluation of SIEM tool for cyber kill chain model in power grid SCADA system. In: 2019 North American Power Symposium (NAPS), pp. 1–6. Wichita (2019)
24. Singh, V.K., Govindarasu, M.: A cyber-physical anomaly detection for wide-area protection using machine learning. IEEE Trans. Smart Grid 12(4), 3514–3526 (2021). https://doi.org/10.1109/TSG.2021.3066316
25. Hui, S.Y.R., Christopoulos, C.: Numerical simulation of power circuits using transmission-line modelling. IEE Proc. 137(6), 379–384 (1990). https://doi.org/10.1049/ip-a-2.1990.0060
26. Karimi-Ghartema, M.: Synchronous reference frame PLL. In: Enhanced Phase-Locked Loop Structures for Power and Energy Applications, pp. 133–145. IEEE (2014)
27. Guillo-Sansano, E., et al.: Harmonic-by-harmonic Time Delay Compensation Method for PHIL Simulation of Low Impedance Power Systems, pp. 560–565. EDST, Vienna (2015)
28. Herbert Falk, SISCO: The Anatomy of a Centralized Remedial Action System: What Can Be Done in 50 Milliseconds? (2014). [Online]. Available:
29. Taylor, C.W., et al.: WACS-Wide-Area stability and voltage control system: R&D and online demonstration. Proc. IEEE 93(5), 892–906 (2005). https://doi.org/10.1109/jproc.2005.846338
30. Yao, W., et al.: Wide-area damping controller for power system interarea oscillations: a networked predictive control approach. IEEE Trans. Control Syst. Technol. 23(1), 27–36 (2015). https://doi.org/10.1109/tcst.2014.2311852
31. Trudnowski, D., et al.: Initial Closed-Loop Testing Results for the Pacific Dc Intertie WADC. IEEE PESGM (2017)
32. Ashok, A., Govindarasu, M., Wang, J.: Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. Proc. IEEE 105(7), 1389–1407 (2017). https://doi.org/10.1109/jproc.2017.2686394

**How to cite this article:** Singh, V.K., et al.: NEFTSec: Networked federation testbed for cyber-physical security of smart grid: Architecture, applications, and evaluation. IET Cyber-Phys. Syst., Theory Appl. 1–15 (2022). https://doi.org/10.1049/cps2.12033