IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 26 February 2024, accepted 9 May 2024, date of publication 14 May 2024, date of current version 22 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3400768

APPLIED RESEARCH

A Proactive–Reactive Methodology for Cyber-Resilient Inverter Control System

MATEO D. ROIG GREIDANUS[1], (Graduate Student Member, IEEE), GAB-SU SEO[2], (Senior Member, IEEE), AND SUDIP K. MAZUMDER[1], (Fellow, IEEE)

[1]Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, IL 60607, USA
[2]Power Systems Engineering Center, National Renewable Energy Laboratory, Golden, CO 80401, USA

Corresponding author: Sudip K. Mazumder (mazumder@uic.edu)

The work was supported in part by the U.S. Department of Energy under Grant numbers DE-EE0009026 and DE-CR0000019, and in part by the U. S. National Science Foundation under Grant 2219734. This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308.

ABSTRACT This paper presents a unified multi-timescale control approach for a power system with distributed energy resources to achieve cyber-resilient operation. The proposed concept combines two cyber-resilient control methods: proactive and reactive methods. The proactive method uses a blockchain that ensures measurement and control data can be securely exchanged among grid assets and also derives control set points as a load-sharing supervisory control, with an embedded logic called *chaincode*. The proactive method ensures data integrity, but it inherits stochastic latency with significant standard deviation due to the nature of the distributed ledgers and security measures, leading to challenges in control. To overcome this trade-off, the reactive approach uses event-driven communication. For this approach, rather than communicating the complete data, a lightweight data packet is communicated in a peer-to-peer fashion. Therefore, it guarantees driving the system into a stable operation in case the proactive operation degrades with insufficient latency. To validate the concept, Hyperleger Fabric blockchain 2.2 is used to characterize the latency and is customized for an inverter control system in this study. Based on the use case, a stability analysis is presented to evaluate the impact of the variable delay and to identify the need for a reactive approach to mitigate the effects of a prolonged delay in the proactive method. A test bed with two hardware inverter prototypes and a custom blockchain programmed with the unified method is developed for validation. A set of hardware experimental results validates the methodology and demonstrates the inverter system operations achieving frequency recovery and load-sharing restoration based on the unified control method.

INDEX TERMS Cyber-resilient control, blockchain, event-triggered, supervisory control, load-sharing, frequency recovery.

I. INTRODUCTION

Electric grids are transforming with increasing numbers of distributed energy resources (DERs), usually interfaced by power electronics converters, raising a multitude of technical challenges resulting from their fundamental differences from conventional rotating generators [1]. Two of the fundamental differences between traditional and modern DERs are i) the significantly increased number of control assets, which, in general, are scaled at relatively low power levels, and ii) the control system is communication-dependent for coordination between assets. The latter causes not only scalability issues—how to effectively control a large system with an increased number of assets—but also security issues—how to operate

The associate editor coordinating the review of this manuscript and approving it for publication was Snehal Gawande.

such a communication-dependent system in a cyber-secure manner [2]. To effectively manage and control various DERs, along with local distribution and transmission networks, it is deemed critical to establish extensive real-time data connectivity through wide-area networks (WANs), protocol standards, and real-time monitoring devices [3].

Enhancing the cybersecurity measures to the DER control communication networks comes at the cost of increased communication latency due to data processing, supplementary router/switch hops, fire-walling, cryptography techniques, certificate binding, encryption, and system reconfiguration [4]. These procedures have the possibility of compromising real-time network operations if the delays are significant [5]. Depending on the variables sent and the bandwidth of the controller receiving them, the effect of the delay on the communication can be substantial or minimal. For instance, a controller with a bandwidth in seconds might not be highly affected by a communication latency increase of tens of milliseconds. Conversely, a controller with a higher working bandwidth might experience a compromised transient response when dealing with such latency [6].

Given that these DER systems are required to carry out an increasing number of grid support tasks, many of which require communication, such as set point updates for frequency and voltage recovery, addressing the DER cyber vulnerability is of paramount importance. A communication mechanism that is by default cyber-secure, such as the blockchain [7], [8], could be required to solve DER cyber-related problems fully. One of the main advantages of blockchain-permissioned data control systems is that the data becomes immutable due to the distributed data storage, verification, and validation properties of the blockchain, which can be used to preserve the integrity, privacy, and availability of the smart grid data [9]. The proactive role of blockchain in securing exchanged data against cyberattacks in grid-connected and power-sharing inverters was investigated in [10] and [11]; however, the literature has not yet sufficiently addressed the practical application of blockchain for inverter-level control. The majority of blockchain-based smart grid applications concentrate on managing economic dispatch among DERs and energy transactions [12]. As such, the viability of using blockchain for the control of inverter-based resource (IBR)-dominated power systems is still an open research topic because the control requires high communication performance to support low-inertia system operations—In addition to the blockchain capacity to manage numerous assets [11].

Blockchain-aided networks have the drawback of not ensuring consistent, predictable latency [13], which adds to data processing and inter-control asset communication latency. In practice, during the transient, an excessive delay can lead to the suboptimal operation of the IBR-dominated system with unequal load-sharing conditions. Note that the latency can increase with system scale, depending on the blockchain network architecture, leading to more unpredictable latency. A solution to limit the degradation of the performance of the physical layer due to excessive delays while ensuring effective communication network capacity is to ensure another communication route between the control agents [14]. Peer-to-peer (p2p), event-triggered communication can be auxiliary in maintaining temporary system stability, e.g., in restoring the steady-state load-sharing ratio in the face of transients or sudden changes [15], [16]. In summary, future IBR-dominated power systems must incorporate multilayered proactive and reactive cybersecurity measures that guarantee communication and control security under steady-state conditions and ensure stable performance in the face of unforeseen events, such as unscheduled load transients.

This paper proposes a method to deal with these cyber issues while providing a cybersecurity framework that guarantees a networked IBR system's steady-state and transient performance even when facing excessive unexpected latency. Proactive, blockchain-permissioned, secure supervisory controller and reactive p2p event-triggered communication methods are combined in a novel unifying approach to achieve cyber-resilient inverter-level control. As a test bed, single-phase, three-level, half-bridge, neutral-point-clamped (3L-NPC) architecture of networked IBRs were used for the experimental results. The multilevel IBR topology was chosen due to its popularity as the most used topology for medium- and high-voltage industrial applications [17], [18]. The key contributions of this work are as follows:

- The proposed approach provides a complete multi-timescale suite of cyber-resilient system control approaches, including power electronics local control (primary control), proactive cyber-secure supervisory control (blockchain-permissioned), and reactive control (event-triggered communication) to ensure critical stable performance.
- The stringent characterization and evaluation of the blockchain use case for inverter system control is presented considering the effect of variable and abnormal latency on the blockchain supervisory data computation.
- The stability analysis of inverter systems with blockchain delay delineates the need for a reactive method design considering system performance.
- The demonstration of the complete concept in a real hardware test bed with typical microcontroller platforms and a microcomputer with web access to the blockchain server interface is presented.

This paper is outlined as follows. Section II introduces the unified proactive and reactive cyber-resilient communication and control approaches proposed in this study. Next, Section III provides the latency characterization of the proactive method, highlighting the stochastic latency nature, and discusses the impact of the stochastic latency of the proactive control method on the system performance. Finally, in Section IV, the efficacy of the unified proactive-reactive methodology is verified by experiments using the following three case illustrations: i) the proactive scheme for the

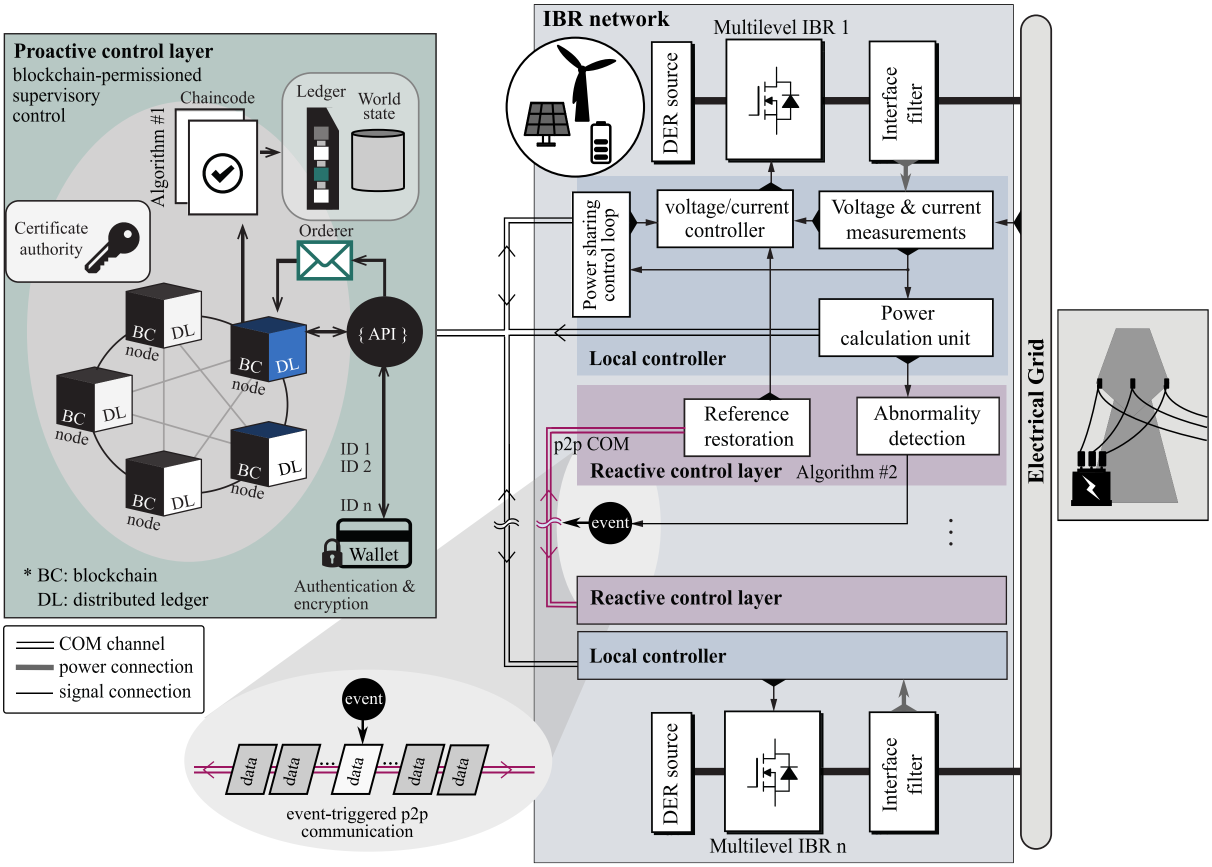


FIGURE 1. Concept diagram of the unified proactive and reactive resilience communication strategy. The proactive approach using a blockchain is used to secure the data exchange and control for the supervisory control. The reactive approach, with event-triggered peer-to-peer (p2p) communication between networked IBRs, operates to retain the reliable control performance under the stochastic latency of the blockchain.

load-sharing strategy of one grid-forming (GFM) and one grid-following (GFL) IBR during the load transient; ii) the proactive scheme for the load-sharing strategy of two GFM IBRs during the load transient; and iii) the play-role of the reactive approach to restoring the system operation in the face of abnormal latency. In Section IV, amidst the results and discussion on the proactive method, the scalability of the blockchain for an extended number of networked IBR devices is demonstrated.

II. UNIFIED CYBER-RESILIENT COMMUNICATION AND CONTROL

This section introduces the concept of the unified proactive and reactive cyber-resilient communication and control approaches proposed in this study. Fig. 1 illustrates a generic system operating multiple DERs with the unified control concept. As shown, each DER operates under a local controller block based on the local measurements, which is GFM (e.g., for battery storage to form a microgrid) or GFL (e.g., for photovoltaics to extract maximum power), depending on the type of the prime source and the control behavior needed. This is the fastest timescale in the system, requiring reliable local measurements. The primary control strategy is outlined in Appendix A.

Residing above the local control at a slower timescale, the supervisory control is implemented using the proactive measure with a blockchain. Using the distributed ledger technology and the authentication and encryption methods integrated in the network, the blockchain network serves as a secure medium for the supervisory control. The concept envisions the blockchain-permissioned supervisory control recording the measurement data from the field devices and providing set points to the local control assets, e.g., the system frequency recovery and load sharing investigated in this study. We consider that the blockchain system allows access only from the devices registered beforehand through certificate authority, securing the data integrity [19], [20]; however, as further discussed in Section III, the stochastic nature of its latency causes challenges that necessitate a reactive measure to avoid performance degradation under the variable latency. To illustrate the proposed reactive solution, Fig. 1 also provides a graphical description of the reactive control layer envisioned in this work. It uses event-triggered p2p communication among DERs. If the latency of the blockchain becomes high, leading to a suboptimal

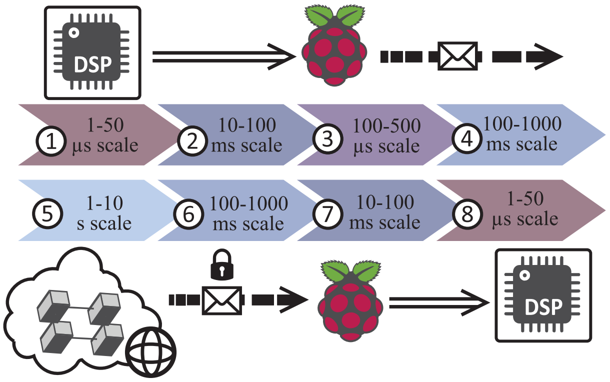


FIGURE 2. Proactive cyber-resilient control system illustrated with different control and communication timescales: i) 1–50μs, data acquisition, sampling, and control; ii) 10–100 ms, the digital signal processor (DSP) writes measurements to Raspberry Pi; iii) measurement data are acknowledged and processed on Raspberry Pi; iv) the blockchain supervisory control is invoked on a remote server; v) blockchain data are authenticated; vi) the Raspberry Pi queries inputs from the blockchain; vii) the Raspberry Pi writes new references to the DSP; and viii) the local control (in the DSP) receives the supervisory control updates.

load-sharing IBR network operation, by exchanging the local measurements and load-sharing ratios, DERs can adjust their set points to reach an acceptable operating point.

Fig. 2 displays an example system using the proactive scheme with different timescales from measurements to a local controller and to a supervisory control going through the blockchain network with update set points returning. The illustration has an Internet of Things (IoT) device, serving as an application programming interface (API), which connects to the server in case the field devices do not have this capability, but it is unnecessary in case the control asset has internet connectivity, such as state-of-the-art solar inverters. The following sections provide further details and insights to complete the concept.

A. PROACTIVE CYBER-SECURE COMMUNICATION AND SUPERVISORY CONTROL USING BLOCKCHAIN

The details on supervisory control using the proactive approach are provided herein. To protect the authenticity, integrity, and availability of information in transit between the supervisory power control layer and the local DER controller, the permissioned blockchain envisioned in this work uses a distributed ledger technology that provides the control system with the intelligence and autonomy via a smart contract [21]. The conceptualization of the blockchain is described next.

In general, a blockchain is a transaction ledger with blocks with a hash that binds each block to the preceding block. Since it is maintained by a distributed network of peer nodes that have a copy of the ledger practicing a consensus protocol to maintain the same ledger, it is considered secure, which is the ground of use for the proactive approach. To provide more context and intuition, the blockchain can be categorized into two types: permissionless and permissioned. A permissionless blockchain is publicly accessible and requires costly mining as proof of work, e.g., Bitcoin. In contrast, a permissioned blockchain is maintained by private entities and provides high privacy and reduced maintenance costs, which result in high security and throughput; therefore, it is considered promising for use in enterprise networks and power system controls [11], [20]. Hyperledger Fabric is a representative open-source permissioned blockchain, supported by the Linux Foundation, providing modular architecture, smart contract (called chaincode), and configurable consensus and membership services [22]. Considering its modularity and flexibility, it is used for this study.

Fig. 1 illustrates the key security components of the blockchain. First, using the permissioned blockchain, the system can control accessibility with high security. Authentication can be executed by the certificate authority to allow only the field devices registered beforehand to access the network. Encryption can be added using Transport Layer Security for peer and orderer node access. To implement the supervisory control, the chaincode of the Hyperledger Fabric is used. It allows a logic to be automatically executed as a result of an event, defined in the blockchain. For DER control, the logic can be programmed and run to derive new set points when a new measurement comes, or as programmed, based on the latest measurements, which is demonstrated in Section IV. Interested readers are referred to [20] because this paper focuses on the concept validation using a customized fabric.

Due to the decentralized ledgers' architecture, which removes the dependence on a central authority, database breaches are no longer a significant threat to identity systems. On top of that, permissioned blockchains are only accessible to restricted users who have been issued certificated identities. The blockchain certificate authority boosts the security and privacy of authentication systems by combining identity verification mechanisms with the distributed ledger technology. Fig. 3 illustrates the authentication mechanism by depicting two scenarios in which the blockchain recognizes differently the identity of 2-byte data packages sending the same encoded message. One bit distinguishes the user in scenario one from scenario two, raising a flag to the blockchain certificate authority to block the nonauthorized attempt to access the chaincode.

The data in the blockchain cannot be changed, i.e., immutable, even if the attacker is within the system [23]. However, spurious data sent from local controllers caused by attacks such as electromagnetic interference (EMI) [24] or side-channel noise intrusion [25] on local sensors can still pose a threat, given that the vulnerability exists outside of the secured blockchain-permission control layer. To add to the proactive cyber-secure characteristics of the blockchain, a transaction filter can be employed in the blockchain's API. Such a filter runs on established criteria assessing whether a transaction is legitimate by looking at the transaction's inputs and metadata. Based on operating boundaries and stochastic information, the distributed ledger nodes will independently reject any transaction that does not pass this filter. Fig. 4

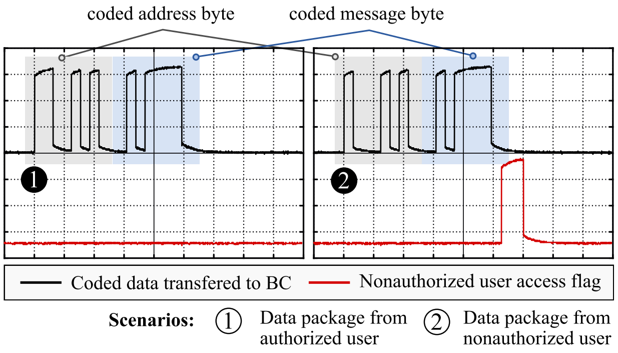


FIGURE 3. Depiction of the blockchain certificate authority authentication mechanism blocking a nonauthorized user from accessing the chaincode.

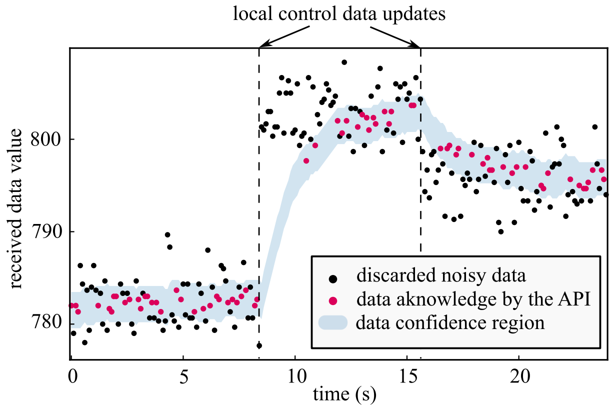


FIGURE 4. Illustration of the smart filtering characteristics for the blockchain transactions blocking tampered input data out of the predefined confidence region.

demonstrates the blockchain's filtering capabilities; random noise is added to the data that the API receives, which is then filtered using a moving average filter with data confidence limits based on allowable standard deviation predefined limits. Based on the filtering, only the acknowledged data is permitted for the transaction.

Critical to this study, the blockchain-based, cyber-resilient communication among the inverter control agents through the blockchain network trades off with increased and stochastic latency because of the nature of the blockchain. The sequential mechanism maintaining the blockchain with security—including authentication, blockchain creation, and synchronization—results in the stochastic nature of latency, causing a challenge for a control system. This latency could be significant in some cases and could affect system performance if not properly designed, as further discussed in Section III.

To provide more clarity on the supervisory control, Algorithm 1 captures key functionalities with an example that can be embedded in the smart contract concept in a blockchain under the proactive communication concept. First, the validity of the data received at the API will be evaluated by authentication and decryption, which ensures data integrity. Once a new measurement arrives, the chaincode

Algorithm 1 Proactive Cyber-Secure Supervisory Control Embedded in Hyperledger Fabric Chaincode

```
Require: Chaincode logic activated from an authorized field device to record local measurements and states, which have been validated by the certificate authority and decryption in the blockchain.
if $\sum_{i=1}^{\text{length}(GFM)} \left| \left( P^*_{GFM,i} - P_{o,i} \right) \right| \geq \epsilon$ then
    $P_{load,tot} := \sum_{i=1}^{\text{length}(loads)} P_{load,i}$
    $P_{GFL,tot} := \sum_{i=1}^{\text{length}(GFL)} P_{GFL,i}$
    for $k = 1;\ k \leq \text{length}(GFM);\ k++$ do
        $P^*_{GFM,i} := \frac{P_{load,tot} - P_{GFL,tot}}{P_{GFM,tot}} P_{GFM,rated,i}$
    for $k = 1;\ k \leq \text{length}(GFL);\ k++$ do
        if type$(GFL,k)$ = Load following then
            $P^*_{GFL,k} := \alpha_k \frac{P_{load,tot}}{P_{system,rated}} P_{GFL,rated,i}$
else
    Notify field devices with return value of no action.
Execute the blockchain chaincode to reflect the new set points to all controllable assets.
```

derives system-level parameters, e.g., system loading and power injection from GFL DERs, $P_{load,tot}$ and $P_{load,GFL}$, respectively. With the updated system parameters, it derives the new active power set points for the GFM inverters, which would recover the grid frequency, if the system has a transient, e.g., if the deviation from the set points is greater than a certain value, ϵ, in Algorithm 1. Note that the same mechanism can be implemented for voltage recovery, referring to the reactive power flow. The chaincode can have an additional logic to accommodate other types of assets. For instance, the system can have a GFL DER(s) that supports balancing supply and demand, similar to a GFM DER but in a passive way. This is applicable to a storage DER with closed-loop grid support functions, such as frequency-watt control, that can exploit the secondary control layer to tune the operation according to the grid conditions, such as the amount of support, e.g., using α_k. Algorithm 1 shows an example of load sharing of GFL inverters, aligned with the experiments discussed in Section IV. In addition to updating the set points, other control actions can be embedded, including load-shedding and relay switch control to form networked microgrids or for system restoration [26], [27].

B. REACTIVE EVENT-TRIGGERED COMMUNICATION AND CONTROL

The resilient communication link for secure data exchange via the permissioned blockchain comes at the cost of increasing latency with a higher number of power electronics nodes. Higher latency, even if it does not cause instability in the IBR network system, can deteriorate the transient response [28], for example, resulting in deficient load sharing

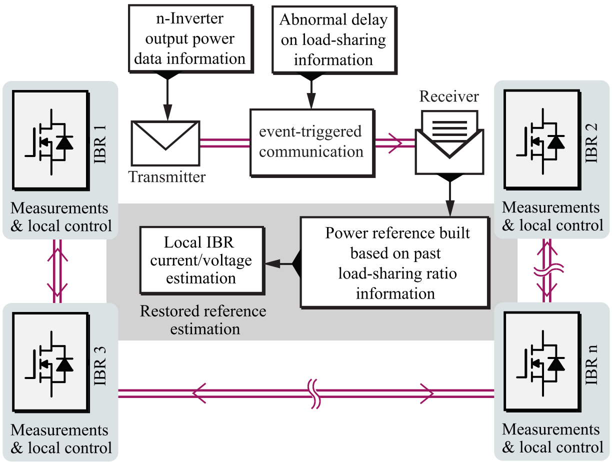

n-Inverter output power data information
Abnormal delay on load-sharing information
IBR 1
Transmitter
event-triggered communication
Receiver
IBR 2
Measurements & local control
Measurements & local control
Local IBR current/voltage estimation
Power reference built based on past load-sharing ratio information
Restored reference estimation
IBR 3
IBR n
Measurements & local control
Measurements & local control

FIGURE 5. Pictorial representation of event-triggered p2p communication between local controllers to restore load sharing between inverters.

Algorithm 2 Event-Triggered Reactive Control and Communication Decision Making

```
Input: Local state update from sensors; power
       references from permissioned blockchain
       supervisory controller
Data: Testing $P_i^*$ updates
Instantaneous output power calculation;
while $\tau_{flag} = 0$ do
    Normal local (current/voltage) control operation
      using supervisory control load-sharing updates
if $\sum_{i=1}^{N} \left(P_i^* - P_{o_i}\right) \neq 0$ then
    for $l = 0; l \leq \infty; l++$ do
        if $l \geq \eta$ then
            $\tau_{flag} := 1$;
            $l := 0$
        else
            Do otherwise
    Store $P_{st_i}$
else
    $P_{st_i} := P_{o_i}$;
    $\tau_{flag} := 0$
if $\tau_{flag} = 1$ then
    Communicate stored $P_{st_i}$ to peer IBR;
    Acknowledge data from peer IBR;
    Update load-sharing ratio $\rho = \frac{P_{st_i}}{P_{st_j}}, \forall i \neq j$
while $\tau_{flag} = 1$ do
    Local (current/voltage) control operation using
      restored power reference from prior load-sharing
      ratio N
```

or exceeding the transient processing power requirements of IBRs. Such performance degradation can lead to damage in power electronics devices and reduced long-term system reliability. The exchange of data from the local controller with the blockchain follows a traditional communication pattern that includes periodic data transfer. Alternatively, need-based and control-centric event-triggered communication can be a valid option, especially when communication and system performance are compromised due to abnormal delays in the blockchain response. This approach can operate with a decreased baud rate by communicating need-based data packages for reliability [29], [30].

In view of an alternative data exchange link, without bypassing the use of the security provided by the blockchain, a second layer of resilience is proposed in this study. The reactive strategy consists of p2p, reduced data packages exchanged between IBRs to retain load-sharing information in the face of a transient and unexpected delay in the control reference update from the local node perspective. In this reactive event-triggered methodology, data transmission between IBR nodes is only established if predefined output-dependent triggering criteria are not met. Consider the power reference update error $\varepsilon(t)$ defined as

$$\varepsilon(t) = P_{o_i}(t) - P_i^*(t_k), \quad t \in [t_k, t_{k+1}] \tag{1}$$

In (1), t_k is the latest instant when the blockchain transmits updated reference data to the controller, and $P_{oi}(t)$ and $P_i^*(t_k)$ are the instantaneous power measured and the reference updated at the latest transmitted sampling instant, respectively. Note that $\varepsilon(t)$ can be computed online, limited by the processing time of DSP sampling $(1 - 50\mu s)$. The event-triggered communication uses the error and its time dependency to determine whether a lightweight package should be transmitted to the next IBR peer, such that

$$t_{k+1} = t_k + \min\left\{t | f\left(\varepsilon(t), t_k\right) > \eta\right\} \tag{2}$$

where $f(\cdot)$, is a running counter function of the error and time of the last update at instant t_k, which is compared to a predefined threshold η. It should be noted that in contrast to availability-triggered data transmission facilitated by blockchain-permissioned reference updates, the p2p event-triggered alternative communication route described herein is based on need. The controller's restored-reference undergoes updates based on past load-sharing data, albeit sub-optimally, due to the stochastic latency associated with blockchain reference feedback.

Fig. 5 shows a pictorial representation of the proposed event-triggered communication between IBR peers in load-sharing mode. The power delivered from each IBR is communicated among its peers before load-sharing ratio information is used to partially restore the power balance between IBRs after a load transient in the case of a prolonged delay observed in the set point update. The p2p communication is called after an event-triggered decision is taken according to Algorithm 2.

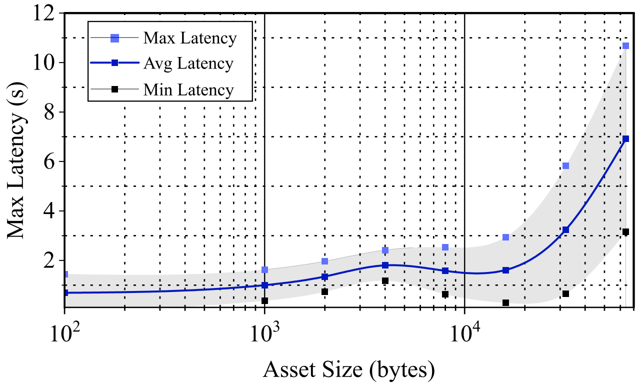


FIGURE 6. Latency benchmark of a Hyperledger Fabric 2.1 for different data sizes [31]. The minimum latency is extrapolated from the difference between the maximum and average for visualization. Here, read and write latency values are summed.

In Algorithm 2, P_i^*, P_{o_i} and P_{st_i} refer to the reference power commanded by the blockchain-permissioned supervisory controller, the instantaneous active output power for the i^{th} IBR up to the length N of the networked IBRs, and the averaged power in steady state condition, respectively; τ_{flag} refers to a binary flag signal that is in the up-logic condition when the local inverter acknowledges a prolonged delay exceeding the threshold, η.

III. ANALYSIS OF SECURITY-ENHANCED CONTROL METHOD ON SYSTEM PERFORMANCE

This section analyzes the impact of the proactive control method on the system performance, i.e., long and stochastic latency due to the distributed ledgers and multiple cyber-security measures used. The impacts of different sizes of data are examined, referring to a benchmark for Hyperledger Fabric, and the impact of device numbers is rigorously analyzed with a custom blockchain developed and tested in this work to study the blockchain's scalability. Based on the characterization, a stability analysis is presented to evaluate the inverter system stability with the primary inverter controller with a varying latency. It leads to insights into the design of the proposed system, including the mode transition between the proactive and reactive methods.

A. STOCHASTIC LATENCY OF BLOCKCHAIN

Although the proactive control approach can secure the measurement and control data distribution, compared to those without security measures, latency degradation is inevitable. Herein the blockchain latency referring to a benchmark and the customized permissioned blockchain for the supervisory control of the inverter system are investigated. The analysis provides insights into the amount of latency expected in the inverter control system and, more importantly, derives a practical control system design.

Fig. 6 displays latency data from a benchmark of a permissioned blockchain, Hyperledger Fabric 2.1, found in [31]. The benchmark data shown is for the fabric using the Couch database and the 2-of-any endorser policy with latency values of Create and Get transactions averaged, using Intel E-2174G-Quadcore and 32-GB RAM running Redhat EL 7.7-64. The full details of the benchmarking condition can be found in [31]. It displays statistical system latency as a function of data size, ranging from 10 Bytes to 64 kBytes. As shown, the Hyperledger Fabric blockchain has two distinctive features notable for control system applications: i) significant latency within a range of seconds and ii) stochastic latency. First, the significant latency should be given attention since its use can be restricted in systems that might require shorter latency to warrant its operation. The relatively long latency in the blockchain is attributed to the distributed ledger creation and the addition of the maintenance mechanisms and security measures, such as encryption and authentication, [32], [33]. Second, the stochastic nature of the blockchain latency is notable. As illustrated in Fig. 6, the latency deviation is significant, and it features the non-monotonic trend of the latency, leading to potential challenges in control and implying the need for a complementary communication and/or control method to alleviate the unpredictable latency.

B. SMALL-SIGNAL STABILITY ANALYSIS OF INVERTER SYSTEM WITH DELAYS

The following stability condition assumes that the IBR network is a delay-dependent system of incommensurate variable communication delays. The stability analysis considers that the blockchain undesirably introduces delay-dependent references to the inverter network, as discussed in Section III-A.

Consider the closed-loop, linear time-invariant model of the n-module load-sharing IBR network, which the following time-domain zero-input state-space model describes:

$$\dot{y}\left(t\right) = \varphi_0 y\left(t\right) + \sum_{m=1}^{n} \varphi_m y\left(t - \tau_m\right) \tag{3}$$

where φ_m is the continuous representation of the optimal control law $(\Phi(\cdot) - \Lambda(\cdot)K_D)$, introduced in Appendix A, that governs the m^{th} IBR, to the top number of n load-sharing inverters, with distributed variable delays, τ_m, affecting the dynamic states $(y(t))$ of the controlled linear time-invariant system. In this representation, the delays, τ_m, are assumed to be independent of each other.

Consider the following delay-dependent model transformation for:

$$y\left(t - \tau_i\right) = y(t) - \int_{t-\tau_i}^{t} \left(\sum_{m=0}^{n} \varphi_m y\left(u - \tau_m\right) \right) du \tag{4}$$

and i is an auxiliary index for the model transformation. The global n-module IBR state-space model from (3) can be rewritten without loss of generality as:

$$\dot{y}(t) = \left(\sum_{i=0}^{n} \varphi_i\right) y(t) - \sum_{i=1}^{n} \varphi_i \int_{t-\tau_i}^{t} \left(\sum_{m=0}^{n} \varphi_m y\left(u - \tau_m\right)\right) du. \quad (5)$$

Applying a Laplace transformation to the integral term of (5), the time-domain delays can be converter to their frequency domain equivalence given by:

$$\mathcal{L}\left\{\int_{t-\tau_i}^{t} \left(\sum_{m=0}^{n} \varphi_m y\left(u - \tau_m\right)\right) du\right\} \hookrightarrow = \frac{1 - e^{-\tau_m s}}{s} \sum_{m=0}^{n} \varphi_m e^{-\tau_m s}, \quad \text{for } \forall s \in \mathbb{C}_+ \quad (6)$$

where $\mathcal{L}$ refers to the Laplace transform operator, and s is a complex frequency domain parameter.

Hence, granted that the n-module closed-loop system model, φ_m, is stable, for any τ_m, $m = 0 \cdots n$, the delay-dependent IBR network can be considered boundedly stable if and only if $\sum_{m=1}^{n} \varphi_m$ is stable, and if the following determinant condition, characterized by the structured singular value, can be met [34]:

$$\det\left[sI - \left(\sum_{i=0}^{n} \varphi_i\right) - \sum_{i=1}^{n} \varphi_i \frac{e^{-\tau_i s} - 1}{s} \left(\sum_{m=0}^{n} \varphi_m e^{-\tau_m s}\right)\right] \neq 0 \quad (7)$$

Alternatively, the delay-dependent stability can be assured if the homogeneous response of all state variables decays to zero in the absence of any input to the system $\left(\text{i.e.} \lim_{t\to\infty} y(t) = 0\right)$. That is, the poles of the homogeneous response of (3) must be contained in the left half of the complex frequency domain plane to affirm stability. For illustration purposes, Fig. 7 shows the poles and zeros map of (7) for three IBRs with parameters described in Section IV considering variations in the average delay of the reference variable sent by the blockchain to the local controller. In the map, a latency sweep is performed from a zero-delay condition to an average delay of 10 s, referring to the Hyperledger Fabrics tested and discussed in Fig. 6—also in agreement with the stochastic latency of the blockchain after IBR network scalability later examined in Section IV-A3 (vide Fig. 15). Regarding the inverter model, three IBRs operating in parallel in GFL mode are considered with constant output voltage. The analysis considers the distributed τ_m delay of each IBR to be of random value, with a standard deviation of 0.82 s around the average latency. The root locus sweep is performed for 10 transfer-function data points of average latency, providing enough resolution to get insights on the stability of the system as the average latency is increased.

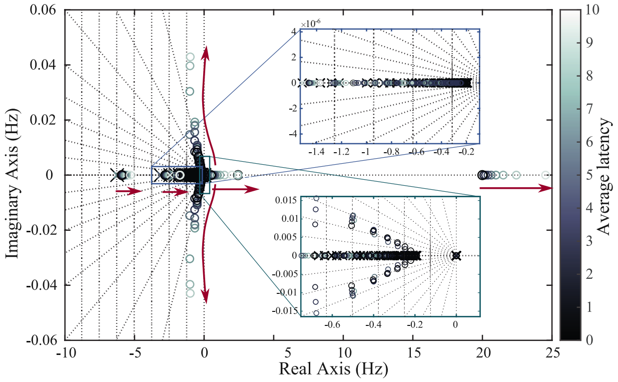


FIGURE 7. Pole-zero map of the output current for three load-sharing current-controlled IBRs for increased average latency coordinated communicated load-sharing information.

Note that the incremental delay does not cause system instability. Despite the single pole at the origin, the other poles of the system are all placed in the left half plane of the imaginary axis, indicating a stable mode of operation and remaining stationary as the latency increases. Conversely, the system zeros change with increasing latency, moving toward the left half plane of the axis. In particular, the non-minimum phase zeros indicate a slower transient response for the system, which is also confirmed by the experimental results obtained in Section IV. In essence, from this analysis, we can conclude that the coordinated distributed delay might degrade the overall performance, typically affecting the transient response of the networked system but not yielding an unsteady solution in either a short or prolonged time span.

IV. EXPERIMENTAL RESULTS

This section presents experimental results from the hardware inverter system tested with the unified cyber-resilient communication and control, including the proactive scheme and reactive countermeasure scenarios. The following results report the dynamic response of two inverters operating with different load-sharing strategies. First, the transient behavior of the blockchain-aided, load-sharing converters is investigated when the two single-phase IBRs, one GFM inverter and one GFL inverter, maintain the electric grid. Next, the dynamic response of two inverters, both in GFM mode, is shown with the supervisory control based on the customized blockchain executing the smart contract.

To validate these strategies, an experimental prototype was used. The inverter local control is implemented using a TMS320F28335 digital signal processor (DSP) from Texas Instruments (TI). In the experimental setup, two single-phase 3L-NPC inverters share a single voltage source, feeding the grid in parallel, as shown in Fig. 9. The proactive control discussed in Algorithm 1 is programmed in a custom Hyperledger Fabric blockchain using the same computer as in Section II-B. The supervisory control embedded in the proactive controller is accessed through a Raspberry Pi 4 IoT device that interfaces the local controller (in the TI DSP) and the blockchain server. The Raspberry Pi 4 primarily operates as an aggregator, filtering and updating the instantaneous power information processed by the IBRs. The IoT device serves as a software intermediary that allows the information

TABLE 1. Single-phase 3L-NPC inverter parameters.

<table>
<tr><th>Input Voltage (V_{DC})</th><th colspan="2">Output Voltage (V_{rms})</th><th>Rated Power (P_o)</th></tr>
<tr><td>400 V</td><td colspan="2">120 V_{rms}</td><td>1 kW</td></tr>
<tr><th>LCL Filter Capacitance (C)</th><th>Inverter-Side LCL Filter Inductance (L_1)</th><th>Grid-Side LCL Filter Inductance (L_2)</th><th>Switching Frequency</th></tr>
<tr><td>500 μH</td><td>3.9 μF</td><td>4.5 mH</td><td>20 kHz</td></tr>
</table>

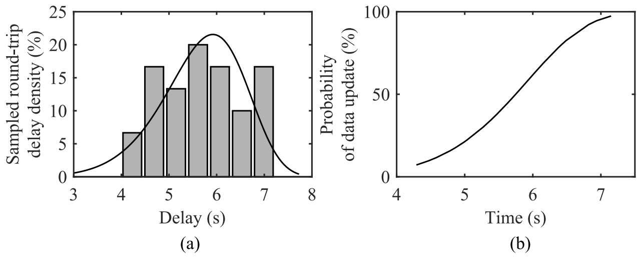


FIGURE 8. Weibull distribution probability plots of the measured round-trip delay between the DSP and the blockchain server after two sequential invocations of the blockchain where (a) presents a 7-bin of a 30 data sample histogram and the probability density function (PDF) of the delay (continuous line), and (b) depicts the cumulative distribution function for the same data set.

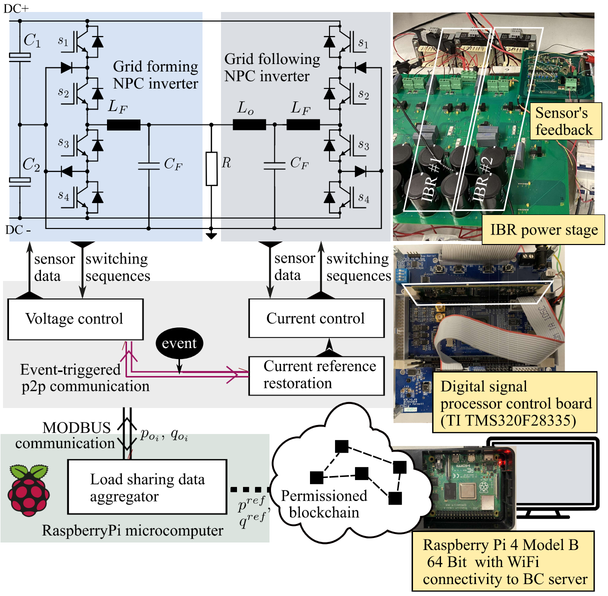

DC+
DC -
C_1
C_2
s_1
s_2
s_3
s_4
Grid forming NPC inverter
Grid following NPC inverter
L_F
L_o
L_F
C_F
R
C_F
Sensor's feedback
IBR #1
IBR #2
IBR power stage
sensor data
switching sequences
sensor data
switching sequences
Voltage control
Current control
event
Event-triggered p2p communication
Current reference restoration
Digital signal processor control board (TI TMS320F28335)
MODBUS communication
p_{o_i}, q_{o_i}
Load sharing data aggregator
p^{ref}, q^{ref}
RaspberryPi microcomputer
Permissioned blockchain
Raspberry Pi 4 Model B 64 Bit with WiFi connectivity to BC server

FIGURE 9. Schematic of one GFM and one GFL IBR with proactive-reactive communication-resilient load-sharing control. The IBR symbols are described in Appendix B.

to be communicated to the blockchain server and processed by Fig. 1 embedded in the Hyperledger Fabric chaincode. The reactive resilient method uses an event-driven p2p communication so that if high latency is perceived in the local controller, the average instantaneous power of each IBR is transmitted between IBRs to restore the power balance, as described in Fig. 2. The rated values and parameters of the single-phase 3L-NPC inverter are specified in Table 1 for a power-scaled prototype of a topology usually employed in Medium-Voltage (MV) IBR networks.

A. THE BLOCKCHAIN-AIDED PROACTIVE CONTROL

Initially, the impact of the delay on the experimental setup is briefly described. The histogram and probability functions of a 30-sample acquisition of the total round-trip delay per data transmission occurrence between the DSP and the blockchain, which the server accesses via the IoT device, for two IBRs are illustrated in Fig. 8. The delay comprises the sum of the MODBUS communication propagation times, the Raspberry Pi 4 data acknowledgment, and two serial invocations and queries of a remotely accessed blockchain server. The case emulates a worst-case scenario regarding typical blockchain latency, given that the sequential invocation of the blockchain causes twice the latency in an interleaving approach. The total latency stochastically varied around an average of 5.67 s. The cumulative distribution function (CDF), in Fig. 8(b), can be interpreted as the probability of sequential updates from the blockchain. It results in a maximum of 7 s to ascertain a 100% chance for the DSP to receive reference data updates from the blockchain. The varying delay agrees with the test and discussion in Section III.

1) SCENARIO 1: PROACTIVE APPROACH FOR ONE GFM AND ONE GFL IBR

First, the proactive communication and control for a grid comprising a network of GFM and GFL IBRs is investigated. This scenario represents a common microgrid operation consisting of different types of power sources with different control schemes, including GFM DERs to regulate the grid voltage and GFL DERs to synchronize to the GFM-formed grid and to inject power as programmed based on the regulated voltage, e.g., by maximum power point tracking control for solar or wind or constant power control for GFL storage. The concept can also be applied to a system with conventional power sources. This scenario involves two local control strategies, voltage regulation and current control, as illustrated in Fig. 9, depending on the type of IBR controls. In this scenario, the supervisory controller, implemented in the blockchain smart contract, responds to load transients to re-balance the load sharing among DERs by communicating new power set points to the local controllers. To demonstrate the supervisory control capability, the test case has two inverters, one for the GFM DERs and one for the GFL DERs. The GFL inverter is assumed to be a storage DER, and it is programmed to share the system load with the GFM DERs based on the supervisory control.

Fig. 10 illustrates the transient behavior of the load-sharing inverters under a load transient, 500-W step-up in the experiment. Upon the transient, as shown in Fig. 10(a), the GFM inverter, Inverter #1, instantaneously reacts to the transient to regulate the grid voltage by supplying the additional power while the GFL inverter, Inverter #2, continues to provide the constant power according to the set point that has not yet

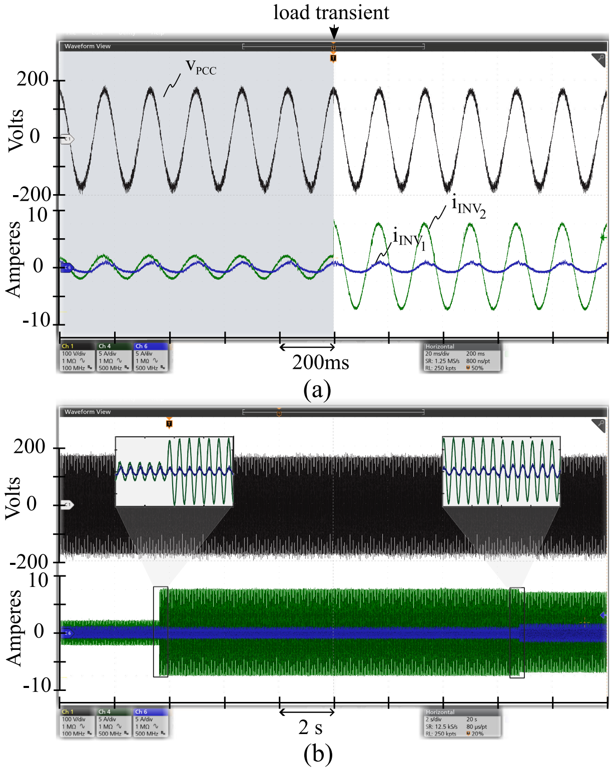


FIGURE 10. Experimental results of the two-inverter system for Scenario 1 (one GFM (IBR #1) and one GFL (IBR #2)) after a load transient (500-W step-up): (a) shows a close-up of the voltage and current waveforms in the transient, and (b) exhibits a longer-time span performance of the inverters actively sharing the load per the command of the supervisory controller based on the blockchain.

been updated. The data aggregator acknowledges the power delivered by the IBRs and invokes the blockchain to adjust the power reference balance between the IBRs. Note that the blockchain response is slow compared to the local control dynamics.

Figs. 10(b) display the longer-timescale dynamics of the system. As the increase of the system load is reported to the supervisory controller in the blockchain, the system starts to reshape the load sharing among the DERs from around 8 s. As the power contribution from the GFL DERs increases, to retain their power contribution to the system load (1:3 set in this experiment), the GFM DERs adjust their power provision, maintaining the grid voltage. With iterations against the transient, the supervisory control leads the system to a new steady state as designed. To avoid potential oscillatory operation and to reduce the sensitivity to erroneous measurements due to a mismatch between the dynamic response and the data acknowledgment, the aggregator applies a moving average filter to the instantaneous power data received by the DSP prior to invoking the blockchain, as shown in Fig. 11; thus, because the blockchain takes time to process the new inputs and update the API with the new power sets, the data aggregator has already averaged the instantaneous power measurements to communicate to the local controller.

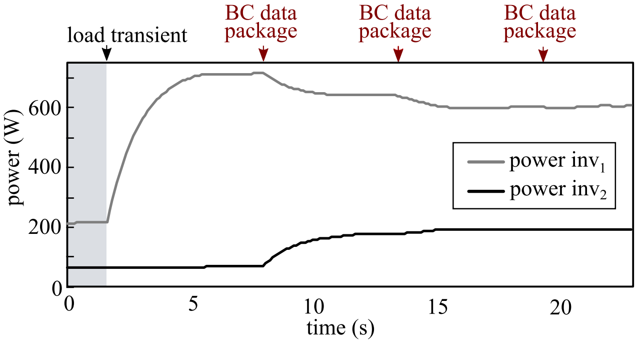
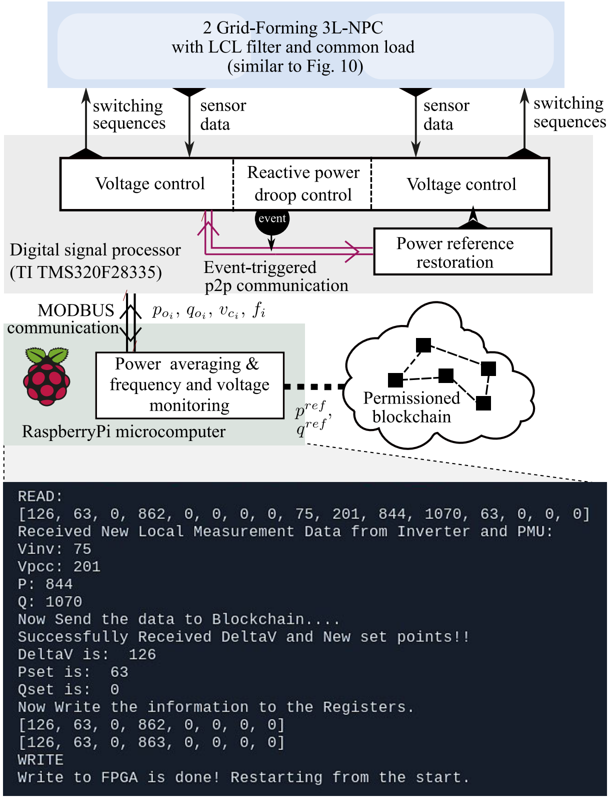


FIGURE 11. Power-sharing data acknowledged and filtered (moving averaged) at the aggregator (Raspberry Pi 4) as a function of the time and blockchain (BC) data packages update.

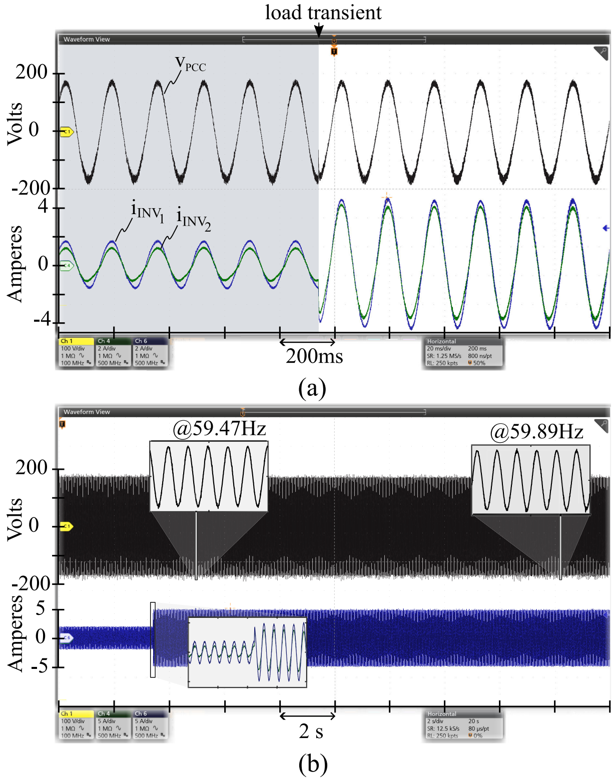


```
READ:
[126, 63, 0, 862, 0, 0, 0, 0, 75, 201, 844, 1070, 63, 0, 0, 0]
Received New Local Measurement Data from Inverter and PMU:
Vinv: 75
Vpcc: 201
P: 844
Q: 1070
Now Send the data to Blockchain....
Successfully Received DeltaV and New set points!!
DeltaV is:  126
Pset is:  63
Qset is:  0
Now Write the information to the Registers.
[126, 63, 0, 862, 0, 0, 0, 0]
[126, 63, 0, 863, 0, 0, 0, 0]
WRITE
Write to FPGA is done! Restarting from the start.
```

FIGURE 12. Schematic of two GFM IBRs with resistive load sharing.

2) SCENARIO 2: PROACTIVE APPROACH FOR TWO GFM IBRs

In Scenario 2, a test case with two GFM IBRs maintaining the electric grid is evaluated under the same generic control concept discussed in Scenario 1. The droop control strategy commonly used is employed to ensure instantaneous grid regulation and load sharing of multiple GFM IBRs according to their power ratings. The supervisory control based on the blockchain can be used to retain the system parameters around the nominal values, e.g., to recover the system frequency (shown in this paper) or to account for possible differences in the grid connection line impedances. Although power sharing can be achieved through the



(a)

(b)

FIGURE 13. Experimental results of the two-inverter system for Scenario 2 (two GFMs with droop primary control) after a load transient (500-W step-up): (a) shows a close-up of the voltage and current waveforms in the transient, and (b) exhibits a longer-time span performance of the inverters with the supervisory control for frequency recovery.

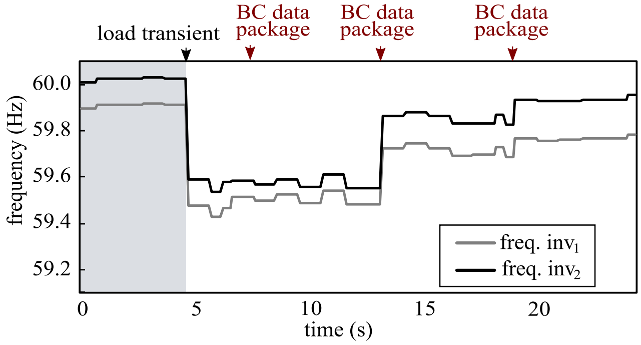


FIGURE 14. Frequency measurements data of the two inverters logged at the secondary control aggregator (Raspberry Pi 4).

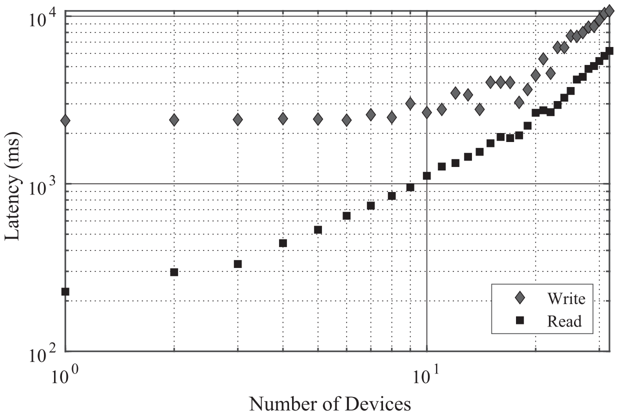


FIGURE 15. Latency measurements of a Hyperledger Fabric 2.2 running with different numbers of devices invoking and querying the blockchain. This setup represents a use case where measurement devices invoke and DERs query to obtain set points.

droop, frequency deviation can inevitably occur as the system loading varies. By the linear droop control law, a frequency droop (frequency decay in the case of a load step-up) is expected whenever an active power load transient occurs. In such an event, the supervisory control built into the blockchain compensates for the frequency change by updating the expected power reference. In the experimental setup, the two GFM IBRs report their local measurements to the Raspberry Pi 4, which invokes the blockchain and queries new set points for frequency recovery, as illustrated in Fig. 12.

The experimental results presented in Fig. 13 show that the droop GFM IBRs immediately recognize the load transient, imposing a system frequency drop (the frequency discrepancy between the two IBRs is a result of the measurement errors). Although the load-sharing ratio between the two GFM IBRs after the transient is maintained due to the frequency droop in this test case, a power deviation from the set points, $\sum_{i=1}^{\text{length}(GFM)} | \left(P^*_{GFM,i} - P_{o,i}\right) |$, occurs. To compensate for this, the supervisory controller updates the power references with the blockchain smart contract to restore the frequency deviation, as shown in Fig. 14. The frequency deviation is compensated in steps until the nominal frequency is fully recovered. Note that the impact of the delay in the frequency restoration is prominent, whereas it does not seem to be as hazardous as in Scenario 1, where the impact degraded the system dynamics. In comparison, the results also indicate that, because of different control objectives, the network-controlled system can have different tolerances for high delays in data processing between the external and internal control agents.

3) SCALABILITY OF THE BLOCKCHAIN

The scalability of the proactive control method, using the Hyperledger Fabric blockchain, is scrutinized in Fig. 15. It displays a set of experimental measurements of blockchain latency customized for the inverter control system use case discussed in this study. In this test, one monitoring device emulates distributing the measurement information through blockchain, e.g., a phasor measurement unit. Based on the measurement data, the blockchain can derive set points for DERs using a smart contract. This test uses the Hyperledge Fabric 2.2 running on Ubuntu 18.04 with i3-10110U and 16 GB RAM. The field devices are emulated by another laptop computer running multiple Linux terminals on Ubuntu 18.04. In the setup, we assume that one monitoring device invokes (writes) the blockchain to record the measurements, and the DERs, up to 32 devices in this test, as shown in Fig. 15, query (read) the blockchain to obtain their set points,

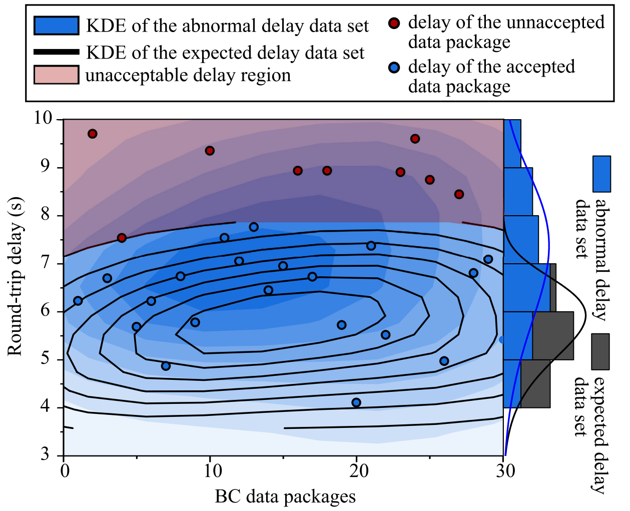


FIGURE 16. Kernel density estimation (KDE) and probability density distributions for BC data packages received by the DSP with expected delay and with extra randomly injected reference update latency.

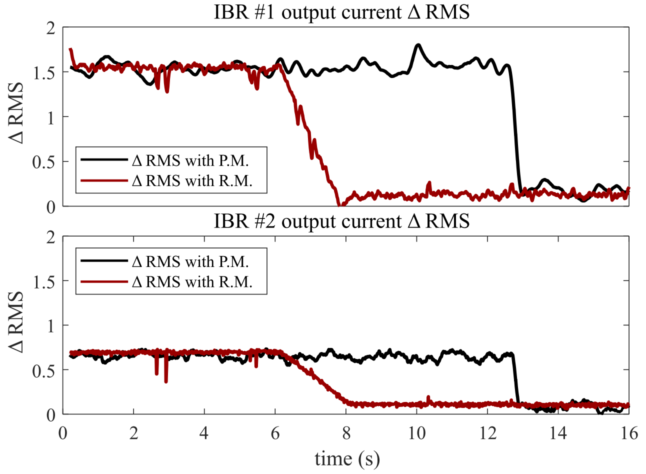


FIGURE 18. Comparison of the moving RMS (Δ*RMS*) between the current output and reference amplitudes after a load step. In the legend, P.M. refers to the "Proactive Method," and the "Reactive Method" is abbreviated by R.M.

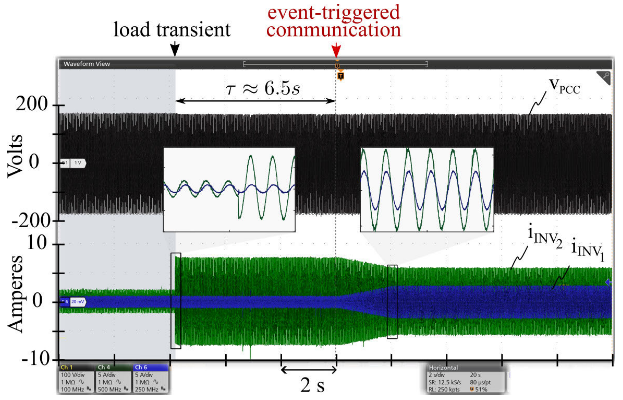


FIGURE 17. Experimental results of the two-inverter system for Scenario 3: one GFM and one GFL IBR with excessive latency in the primary communication inducing the reactive event-triggered communication after a 500-W load step-up.

derived from the blockchain chaincode, for the supervisory control.

As shown, the system latency significantly varies with different numbers of devices, ranging from 200 ms to more than 10 s. It is also notable that the write transaction, involving the Orderer operation to create a new ledger, yields significantly longer latencies than the read (get) transactions [22]. This indicates that the system designer needs to strategize the communication topology, considering a longer latency in write actions by nature. To confirm the reliability and validity of this test, two Beaglebone Black devices were used in addition to the laptop emulating multiple devices. They have shown a minimal difference in latency from the emulated devices.

B. REACTIVE METHODOLOGY FOR ABNORMAL LATENCY COMPENSATION

It is evident from these results that substantial blockchain latency momentarily degrades the dynamic power balance in the system (Scenario 1) and frequency deviation (Scenario 2). Power reference updates from the supervisory controller to the IBR local controller are sparsely distributed while the power balance or frequency is restored. To remedy the inevitable slow dynamics of the data update, especially when the system observes severe performance degradation from prolonged latency, the reactive approach described in Section II-B is carried out on the inverters described in Scenario 1. Because blockchain latency is a stochastic variable, the event-triggered threshold is defined in the experiment based on an upper limit of the expected delay dataset, as the worst condition for system operation previously described in Fig. 8, when the probability of data update was near its maximum. The experimental data from Fig. 16, illustrates, by comparison, a condition of unexpected delay distribution was found. In this portrait, the blockchain data package updates in red are above the pre-defined acceptable region and would invariably trigger the p2p reactive communication and control methodology. Such conditions may happen due to congestion of the blockchain server or purposely induced delays on the communication channel between the local controller and the proactive control layer.

Fig. 17 displays the result of a test case of a power system with one GFM and one GFL IBR experiencing excessive latency, which induces the event-triggered reactive method to become operational. Identical to Scenario 1, the GFM IBR recovers the power imbalance right after the transient. Subsequently, once the local inverter controller detects the prolonged latency anomaly, the p2p communication is activated to communicate critical data on both IBRs and, therefore, to restore the balance of power sharing as outlined in Algorithm 2. Here, the control is conditioned to recover in a ramp based on the previous information on the steady-state condition before the transient. Even though the communication bandwidth is limited for reliability purposes, such an approach is designed to transmit only the essential data, thus guaranteeing system stability and mitigating the suboptimal condition caused by the excessive delay.

The main difference between proactive and reactive approaches manifests in the rate of convergence between the regulated variable and the reference. This deviation convergence is illustrated in Fig. 18, which shows the moving root mean square of the error $\Delta\text{RMS}[k] = \sqrt{\frac{1}{N}\sum_{i}^{k=i-N+1}\left(i^{*} - i_{L_o}\right)}$ between the output current (i_{L_o}) and the reference (i^{*}) for the blockchain-based and event-triggered methods after a load perturbation, considering a regulated output voltage condition.

V. CONCLUSION

This work has provided a unified control approach for power systems with high penetrations of DERs, allowing for cyber-resilient operations against cyberattacks and associated issues. A proactive framework using a permissioned blockchain can guarantee data security in communication and provides supervisory control using the blockchain smart contract. The work characterized a custom Hyperledger Fabric blockchain and demonstrated its integration into the inverter control systems. The paper also recognized, by testing the custom blockchain, that the proactive method trades off the security improvement with increased and stochastic latency, which can affect the system performance and therefore cause challenges in system control. To mitigate the impact of the unpredictable blockchain latency on the system performance, a reactive method using p2p communication and control, complementary to the proactive method, has been proposed to complete the concept. The event-triggered control that is activated when excessive latency is encountered can mitigate the performance degradation from the stochastic nature of the blockchain. This work has experimentally validated the unified control methodology using a hardware test bed with two hardware inverters, a custom blockchain developed for the supervisory control, and p2p communication-based control. Three test cases in the experiments demonstrated that the concept can ensure power system controls, including power sharing among IBRs with different primary control types, and system frequency recovery against load transients, implying its high potential for other control purposes.

APPENDIX A
IBR PRIMARY CONTROL STRATEGY

A description of the primary control used in this study is herein provided. The applied primary controller is based on the switching sequence-based optimal control used in [35]. Here, the optimal control strategy is disclosed in a generic form for voltage or current regulation depending on the control objectives of the individual IBR. Appendix B provides the specifics on the control-oriented analytical model of the inverter.

The 3L-NPC inverter model can be represented as a nonlinear composition of the inverter characteristics and its switching sequences. For computing purposes, assume that the aforementioned model can be described as a piecewise-linear discrete set of dynamical equations as a function of the inputs and internal states such that the discrete map of the inverter's dynamics can be described by:

$$\begin{aligned} x_{j+1} &= f_1\left(x_k, t_{1k}, t_{2k}, \cdots, t_{nk}, i_{DC}, v_{PCC}\right) \\ &= \Phi(\cdot)x_j + \Lambda(\cdot)u_j \end{aligned} \tag{8}$$

where x_j and u_j represent the IBR states and inputs (i_{DC} and v_{PCC}), respectively, at the discrete instant j. $\Phi(\cdot)$ and $\Lambda(\cdot)$ are the discrete state-transition matrices that correlate the inverter states and the IBR inputs, respectively, to the next-step prediction of the system, which is described as:

$$\Phi(t_{nk}) = \prod_{i=1}^{n} e^{A_i t_{k(n-i+1)}} x_k \tag{9}$$

$$\begin{aligned} \Lambda(t_{nk}) = \Bigg[&\left(\prod_{i\neq 1}^{n} e^{A_{k(n-i+1)} t_i}\right)\left(e^{A_{k1}t_{k1}} - \mathrm{I}\right) A_{k1}^{-1} B_{k1} \\ &+ \left(\prod_{i\neq 1,2}^{n} e^{A_{k(n-i+1)} t_{ki}}\right)\left(e^{A_{k2}t_{k2}} - \mathrm{I}\right) A_{k2}^{-1} B_{k2} \\ &+ \cdots + \left(e^{A_{kn}t_{kn}} - \mathrm{I}\right) A_{kn}^{-1} B_{kn} \Bigg], \end{aligned} \tag{10}$$

where t_{nk} is the time allocation of the n^{th} switching state for the k^{th} switching sequence spread over a switching period, T_s, satisfying $0 \leq t_{nk} \leq 1$, $\sum_{n=1}^{h} t_{nk} = T_s$. A_{kn} is a state matrix of a subset of controllable switching states of the inverter switching model, and B_{kn} is the input matrix, outlined in Appendix B.

We consider the local optimal control strategy with the following cost function:

$$J(t_{kn}, T_s) = (x^{*} - x_{j+1})^{\mathsf{T}} P (x^{*} - x_{j+1}) \tag{11}$$

where P refers to the positive-definite weighting matrix, x_{j+1} refers to the individual inverter states in the next-step predictions, and x^{*} resembles the desired objective control reference, provided by the power-sharing control loop, after updates from the supervisory controller. For instance, a GFL controller targets the minimization of the current-regulation error to inject a constant power. In contrast, the control objective of a GFM controller is to regulate the inverter output voltage utterly defined by its primary control, e.g., a droop control, to ensure instantaneous balance of supply and demand and maintain the grid voltage and frequency within an acceptable range.

Suppose an alternative cost function representation is presented in (11). The same cost function can be linearly represented while maintaining its small-signal properties [36], without loss of generalization, giving a positive-definite matrix, Ω, such that:

$$\begin{aligned} J\left(e_j, u_j\right) &= e_{j+1}^{\mathsf{T}} \Omega e_{j+1} \\ &= e_j^{\mathsf{T}} \Phi^{\mathsf{T}} \Omega \Phi e_j + u_j^{\mathsf{T}} \Lambda^{\mathsf{T}} \Omega \Lambda u_j \\ &\quad + 2u_j^{\mathsf{T}} \Lambda^{\mathsf{T}} \Omega \Phi e_j \end{aligned} \tag{12}$$

where $e_j = x^* - x_j$ represents the state tracking errors of system (11). The solution to the equation can then obtain the unconstrained minimization of this cost function as such:

$$\frac{\partial J\left(e_j, u_j\right)}{\partial u_j} = 2\Lambda^{\intercal}\Omega\Lambda u_j + 2\Lambda^{\intercal}\Omega\Phi e_j = 0 \qquad (13)$$

which, by definition, results in a linear state feedback control law, such as $u_j = -K_D e_j = -K_D\left(x^* - x_j\right)$, where $K_D = \left(\Lambda^{\intercal}\Omega\Lambda\right)^{-1}\Lambda^{\intercal}\Omega\Phi$. The closed-loop linear state feedback control model is later used for the stability analysis of the delay-dependent networked system in Section III-B.

APPENDIX B
SINGLE-PHASE 3L-NPC IBR DYNAMIC MODEL

The following matrix defines the active dynamic open-loop model of a single-phase 3L-NPC inverter with output LCL filter, detailed in Fig. 9, in the state space:

$$\kappa \begin{bmatrix} \frac{\mathrm{d}v_{C_1}}{\mathrm{d}t} \\ \frac{\mathrm{d}v_{C_2}}{\mathrm{d}t} \\ \frac{\mathrm{d}i_{L_F}}{\mathrm{d}t} \\ \frac{\mathrm{d}i_{L_o}}{\mathrm{d}t} \\ \frac{\mathrm{d}v_{C_F}}{\mathrm{d}t} \end{bmatrix} = \underbrace{\begin{bmatrix} \sigma_1 & & \mathbf{0}_{2\times4} & & \\ \sigma_2 & & & & \\ \sigma_3 & \sigma_3 & -r_{L_F} & 0 & 1 \\ & & 0 & -r_{L_o} & 1 \\ \multicolumn{2}{c}{\mathbf{0}_{2\times2}} & 1 & -1 & 0 \end{bmatrix}}_{A_{kn}} \begin{bmatrix} v_{C_1} \\ v_{C_2} \\ i_{L_F} \\ i_{L_o} \\ v_{C_F} \end{bmatrix} + \underbrace{\begin{bmatrix} 1 & 1 & \mathbf{0}_{1\times3} \\ \mathbf{0}_{1\times3} & -1 & 0 \end{bmatrix}^{\intercal}}_{B_{kn}} \begin{bmatrix} i_{DC} \\ v_{PCC} \end{bmatrix} \qquad (14)$$

where $\kappa = \mathrm{diag}\left\{C_1, C_2, L_F, L_o, C_F\right\}$, and $\sigma_1 = \mathrm{s}_1 \times \mathrm{s}_2$, $\sigma_2 = -\mathrm{s}_3 \times \mathrm{s}_4$, $\sigma_3 = \frac{\sigma_1+\sigma_2}{2}$ are functions of the switching states and switching sequences of the single-phase half-bridge 3L-NPC converter described in [37]. The states i_{L_F}, i_{L_o}, v_{C_F}, v_{C_1} and v_{C_2} correspond to the inverter-side inductor current, the grid-side inductor current, the capacitor voltage, and the input-side split capacitor voltages, respectively. The state-space model inputs are the inverter DC current, i_{DC}, and the output voltage at the point of common coupling of the IBRs, v_{PCC}. Symbols L_F and r_{L_F} represent the inductance of the inverter-side LCL filter and its parasitic resistance. Similarly, L_o and r_{L_o} represent the grid-side filter inductance and its parasitic resistance, respectively, and C_F is the filter capacitance of the LCL filter. Symbols C_1 and C_2 are the capacitances of the split capacitors for the DC-link side of the inverter.

REFERENCES

[1] B. S. Hodge, H. Jain, C. Brancucci, G. Seo, M. Korps, J. Kiviluoma, H. Holttinen, J. C. Smith, A. Orths, A. Estanqueiro, L. Söder, D. Flynn, T. K. Vrana, R. W. Kenyon, and B. Kroposki, "Addressing technical challenges in 100% variable inverter-based renewable energy power systems," *WIREs Energy Environ.*, vol. 9, no. 5, p. e376, Sep. 2020.

[2] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo, W. Song, M. D. R. Greidanus, S. Sahoo, F. Blaabjerg, J. Zhang, L. Guo, B. Ahn, M. B. Shadmand, N. R. Gajanur, and M. A. Abbaszada, "A review of cyber–physical security for photovoltaic systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 4, pp. 4879–4901, Aug. 2022.

[3] V. Budhraja, C. Martinez, J. Dyer, and M. Kondragunta, "Interconnection and controls for reliable, large scale integration of distributed energy resources," Lawrence Berkeley Nat. Lab., Berkeley, CA, USA, White Paper, Dec. 1999.

[4] A. Kondoro, I. Dhaou, H. Tenhunen, and N. Mvungi, "A low latency secure communication architecture for microgrid control," *Energies*, vol. 14, no. 19, p. 6262, Oct. 2021.

[5] J. Johnson, I. Onunkwo, P. Cordeiro, B. J. Wright, N. Jacobs, and C. Lai, "Assessing DER network cybersecurity defences in a power-communication co-simulation environment," *IET Cyber-Phys. Syst. Theory Appl.*, vol. 5, no. 3, pp. 274–282, Sep. 2020.

[6] X. Chen, J. Zhou, M. Shi, Y. Chen, and J. Wen, "Distributed resilient control against denial of service attacks in DC microgrids with constant power load," *Renew. Sustain. Energy Rev.*, vol. 153, Jan. 2022, Art. no. 111792.

[7] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Hyperledger fabric blockchain for securing the edge Internet of Things," *Sensors*, vol. 21, no. 2, p. 359, Jan. 2021.

[8] S. Rathore and J. H. Park, "A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5522–5532, Aug. 2021.

[9] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 3–19, Jan. 2021.

[10] N. Gajanur, M. Greidanus, G.-S. Seo, S. K. Mazumder, and M. Ali Abbaszada, "Impact of blockchain delay on grid-tied solar inverter performance," in *Proc. IEEE 12th Int. Symp. Power Electron. Distrib. Gener. Syst. (PEDG)*, Jun. 2021, pp. 1–7.

[11] R. Mahmud and G.-S. Seo, "Blockchain-enabled cyber-secure microgrid control using consensus algorithm," in *Proc. IEEE 22nd Workshop Control Model. Power Electron. (COMPEL)*, Nov. 2021, pp. 1–7.

[12] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[13] L. Wan, D. Eyers, and H. Zhang, "Evaluating the impact of network latency on the safety of blockchain transactions," in *Proc. IEEE Int. Conf. Blockchain*, Jul. 2019, pp. 194–201.

[14] M. Chen, X. Xiao, and J. M. Guerrero, "Secondary restoration control of islanded microgrids with a decentralized event-triggered strategy," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3870–3880, Sep. 2018.

[15] J. Zhang, B. Sun, and D. Zhao, "A novel event-triggered secondary control strategy for distributed generalized droop control in microgrid considering time delay," *IEEE Trans. Power Electron.*, vol. 38, no. 5, pp. 5963–5978, May 2023.

[16] Y. Li, H. Zhang, X. Liang, and B. Huang, "Event-triggered-based distributed cooperative energy management for multienergy systems," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2008–2022, Apr. 2019.

[17] D. Floricau, G. Gateau, M. Dumitrescu, and R. Teodorescu, "A new stacked NPC converter: 3L-topology and control," in *Proc. Eur. Conf. Power Electron. Appl.*, 2007, pp. 1–10.

[18] J. Rodriguez, S. Bernet, B. Wu, J. O. Pontt, and S. Kouro, "Multilevel voltage-source-converter topologies for industrial medium-voltage drives," *IEEE Trans. Ind. Electron.*, vol. 54, no. 6, pp. 2930–2945, Dec. 2007.

[19] U. Satapathy, B. Ku. Mohanta, S. S. Panda, S. Sobhanayak, and D. Jena, "A secure framework for communication in Internet of Things application using hyperledger based blockchain," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–7.

[20] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.

[21] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–4.

[22] (2023). *A Blockchain Platform for the Enterprise*. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/orderer/ordering_service.html

[23] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for IoT," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–6.

[24] J. Selvaraj, "Intentional electromagnetic interference attack on sensors and actuators," Ph.D. dissertation, Dept. Elect. Comput. Eng., Iowa State Univ., Ames, IA, USA, 2018.

[25] N. Gajanur, M. D. R. Greidanus, S. K. Mazumder, and M. A. Abbaszada, "Impact and mitigation of high-frequency side-channel noise intrusion on the low-frequency performance of an inverter," *IEEE Trans. Power Electron.*, vol. 37, no. 10, pp. 11481–11485, Oct. 2022.

[26] A. Banerjee, V. U. Pawaskar, G.-S. Seo, A. Pandey, U. R. Pailla, X. Wu, and U. Muenz, "Autonomous restoration of networked microgrids using communication-free smart sensing and protection units," *IEEE Trans. Sustain. Energy*, vol. 14, no. 2, pp. 1076–1087, Apr. 2023.

[27] J. Sawant, G.-S. Seo, and F. Ding, "Resilient inverter-driven black start with collective parallel grid-forming operation," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Jan. 2023, pp. 1–5.

[28] S. Anand, B. G. Fernandes, and J. Guerrero, "Distributed control to ensure proportional load sharing and improve voltage regulation in low-voltage DC microgrids," *IEEE Trans. Power Electron.*, vol. 28, no. 4, pp. 1900–1913, Apr. 2013.

[29] J. Liu, Y. Gu, L. Zha, Y. Liu, and J. Cao, "Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 49, no. 8, pp. 1665–1678, Aug. 2019.

[30] C. Peng, D. Yue, and Q.-L. Han, *Communication and Control for Networked Complex Systems*. Cham, Switzerland: Springer, 2015.

[31] *Hyperledger Blockchain Performance Reports*. Accessed: Mar. 6, 2023. [Online]. Available: https://hyperledger.ithub.io/caliper-benchmarks/fabric/performance/2.1.0/nodeContract/gnodeSDK/submit/create-asset/

[32] X. Xu, G. Sun, L. Luo, H. Cao, H. Yu, and A. V. Vasilakos, "Latency performance modeling and analysis for hyperledger fabric blockchain network," *Inf. Process. Manage.*, vol. 58, no. 1, Jan. 2021, Art. no. 102436.

[33] M. Kuzlu, M. Pipattanasomporn, L. Gurses, and S. Rahman, "Performance analysis of a hyperledger fabric blockchain framework: Throughput, latency and scalability," in *Proc. IEEE Int. Conf. Blockchain*, Jul. 2019, pp. 536–540.

[34] K. Gu, J. Chen, and V. L. Kharitonov, *Stability of Time-delay Systems*. Cham, Switzerland: Springer, 2003.

[35] S. K. Mazumder and K. Acharya, "Multiple Lyapunov function based reaching condition for orbital existence of switching power converters," *IEEE Trans. Power Electron.*, vol. 23, no. 3, pp. 1449–1471, May 2008.

[36] S. Di Cairano and A. Bemporad, "Model predictive controller matching: Can MPC enjoy small signal properties of my favorite linear controller?" in *Proc. Eur. Control Conf. (ECC)*, Aug. 2009, pp. 2217–2222.

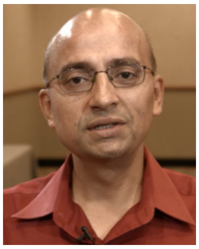
[37] B.-R. Lin and T.-L. Hung, "Development of a single-phase half-bridge neutral point clamped converter and its applications," in *Proc. IEEE Int. Symp. Circuits Systems.*, Jul. 2002, pp. 1–13.

MATEO D. ROIG GREIDANUS (Graduate Student Member, IEEE) received the B.E. and M.S. degrees in electrical engineering from the Federal University of Santa Catarina (UFSC), Florianópolis, Brazil, in 2018 and 2020, respectively. He is currently pursuing the Ph.D. degree in electrical and computer engineering with the Laboratory for Energy and Switching-Electronic Systems (LESES), University of Illinois Chicago (UIC), Chicago, IL, USA. His research interests include the ac stability of power electronics systems, renewable energy integration, and cyber-physical security of power electronic-dominated grids.

GAB-SU SEO (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Seoul National University, Seoul, South Korea, in 2015.

From 2016 to 2017, he was a Research Associate with the Colorado Power Electronics Center, University of Colorado, Boulder, CO, USA. Since 2018, he has been with the Power Systems Engineering Center, National Renewable Energy Laboratory (NREL), Golden, CO, USA, where he is currently a Senior Electrical Engineer and leads research projects focused on power electronics and power systems applications for electric grids with high integrations of inverter-based resources. He has coauthored more than 80 IEEE journal and peer-reviewed conference papers. He coauthored the Research Roadmap on Grid-Forming Inverters (NREL, 2020). His current research interests include power electronics for renewable energy systems and microgrids and power systems engineering for grid modernization, including grid-forming inverter control and inverter-driven power systems black start for low- or zero-inertia grids to improve grid resilience and stability.

Dr. Seo is won one Best Paper Award. He is an IEEE Roadmap Working Group Chair of the International Technology Roadmap of Power Electronics for Distributed Energy Resources (ITRD)—WG3 Integration and Control of DERs. He is an Associate Editor of the IEEE Transactions on Power Electronics, the IEEE Journal of Emerging and Selected Topics in Power Electronics, the IEEE Transactions on Industry Applications, the IEEE Open Journal of Power Electronics, and the *Journal of Power Electronics*. He is currently the Secretary of the IEEE Power Electronics Society Technical Committee on Sustainable Energy Systems (IEEE PELS TC5) and the Vice Chair of the IEEE PELS Denver Section.



SUDIP K. MAZUMDER (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from Virginia Tech, in 2001.

He has over 30 years of professional experience and has held research and development and design positions in leading industrial organizations. He was a Technical Consultant for several industries. He is currently a UIC Distinguished Professor and the Director of the Laboratory for Energy and Switching-Electronic Systems (LESES), Department of Electrical and Computer Engineering, University of Illinois Chicago (UIC). He is also the President of NextWatt LLC.

Dr. Mazumder was named a fellow of the American Association for the Advancement of Science (AAAS), in 2020, and Asia–Pacific Artificial Intelligence Association (AAIA), in 2022. He has been serving as an Administrative Committee Member for IEEE PELS, since 2015. He has also been serving as a Member-at-Large for IEEE PELS, since 2020. He was a recipient of the 2023 IEEE Power and Energy Society's Ramakumar Family Renewable Energy Excellence Award. He received several IEEE awards/honors, including IEEE Transactions on Power Electronics Prize Paper Awards, in 2002 and 2022, and Highlighted Papers, in 2018, 2022, and 2023, the Featured Article of IEEE Transactions on Biomedical Engineering, in 2023, the IEEE Conference Best Paper Award, in 2013, and the IEEE International Future Energy Challenge Award, in 2005. He has served as the Chair for the IEEE PELS Technical Committee on Sustainable Energy Systems, from 2015 to 2020. He served as the General Chair for IEEE PEDG Conference, in 2023. He serves as the General Co-Chair for the IEEE Energy Conversion Congress & Exposition (ECCE), in 2024. Since 2019, he has been serving as the Editor-in-Large for IEEE Transactions on Power Electronics. From 2016 to 2019, he was an IEEE Distinguished Lecturer.