A Secure Communication Architecture for Distributed Microgrid Control

Velin Kounev, *Student Member, IEEE*, David Tipper, *Senior Member, IEEE*, Attila Altay Yavuz, *Member, IEEE*, Brandon M. Grainger, *Member, IEEE*, and Gregory F. Reed, *Member, IEEE*

***Abstract*—Microgrids are a key component in the evolution of the power grid. Microgrids are required to operate in both grid connected and standalone island mode using local sources of power. A major challenge in implementing microgrids is the communications and control to support transition from grid connected mode and operation in island mode. Here, we propose a secure communication architecture to support microgrid operation and control. A security model, including network, data, and attack models, is defined and a security protocol to address the real-time communication needs of microgrids is proposed. The implementation of the proposed security scheme is discussed and its performance evaluated using theoretical and co-simulation analysis, which shows it to be superior to existing protocols.**

***Index Terms*—Microgrids, security, versatile communications.**

I. Introduction

MICROGRIDS have been proposed as a method to provide continuity of power to key societal and commercial locations (e.g., hospitals, military bases, etc.) and as a means to incorporate distributed energy generation such as wind and solar [1]–[3]. The basic building blocks of microgrids include the ability to connect to and from the power grid, electrical loads, and a back-up energy supply (e.g., renewables, fuel cells, etc.). A fundamental requirement of microgrids is operating in stand alone (i.e., island) and grid connected modes. In island mode, the microgrid control system provides frequency and voltage stability for optimal power flow, and ensures minimal load shedding and disruption during transition from grid connected to island mode. Furthermore, the microgrid should have the ability to move back from island to grid-connected mode, resulting in resynchronization with minimum impact to sensitive loads.

Providing reliable and secure communications among the microgrid components and between the microgrid and the larger grid is a requirement for the microgrid to function. Of particular concern is the communications supporting the microgrid control systems. References [4]–[7] provide overviews of the distributed hierarchical control layers within microgrids, namely: primary, secondary, and tertiary control layers. The primary control is responsible for maintaining voltage and frequency stability of the microgrid subsequent to changes in the system mode. The secondary control layer should compensate for the voltage and frequency deviations caused by the operation of the primary control layer. Finally, the tertiary control layer manages the power flow between the microgrid and the main grid, coordinates with adjacent microgrids, and facilitates optimal operation.

In general, each control layer is comprised of separate physical entities with differing computational resources. In implementing such a control architecture, the controllers at the top of the hierarchy take state input from lower layers and compute parameters that maybe passed to controllers at lower levels for their local control actions. Note that the control layers work on different time scales with real-time delay constraints for information exchange within and between layers. Hence, the communications between the control elements are time critical in nature implying the need for efficient algorithms that minimize the delay and computational resource requirements. Furthermore, the communication and security architectures must be versatile enough to support various communication patterns among control components, namely: unicast, multicast, and broadcast communications.

Here, we propose a secure communication architecture tailored to the microgrid control system. The main contributions of this paper include the following. We formally define a microgrid communication security model. We propose a security architecture that supports the hierarchical structure of microgrid control mechanisms and takes the resource constraints into account while respecting the real-time communication requirements. Moreover, we design a security protocol that supports broadcast, multicast, and unicast communications. The proposed solution provides data confidentiality and authentication while meeting the real-time communication needs within the microgrid. The implementation of the proposed scheme is discussed and compared with other approaches in this paper through theoretical comparison and a co-simulation analysis of a target microgrid. Our results indicate that the new security scheme outperforms its counterparts either in terms of computational efficiency or storage requirements. The rest of this paper is organized as follows. Section II presents background material on microgrids and the challenges they present. Section III provides an overview of

Manuscript received May 16, 2014; revised September 22, 2014 and January 19, 2015; accepted March 24, 2015. Date of publication May 11, 2015; date of current version August 19, 2015. Paper no. TSG-00464-2014.

V. Kounev and D. Tipper are with the Graduate Telecommunications and Networking Program, University of Pittsburgh, Pittsburgh, PA 15260 USA (e-mail: dtipper@pitt.edu).

A. A. Yavuz is with the School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR 97331 USA.

B. M. Grainger and G. F. Reed are with the Department of Electrical and Computer Engineering, University of Pittsburgh, Pittsburgh, PA 15260 USA.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2015.2424160

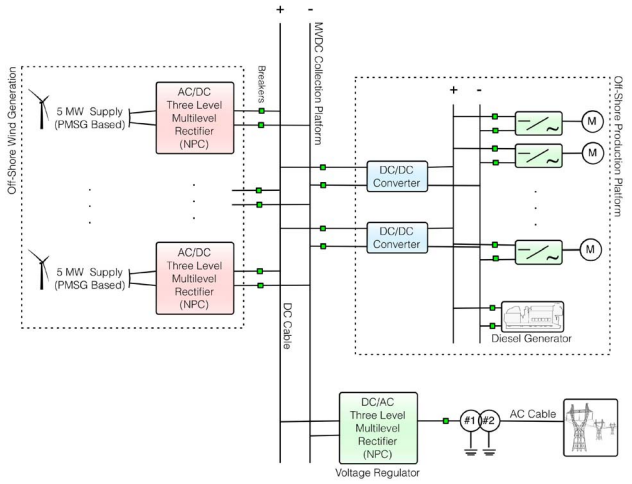


Fig. 1. Offshore production platform microgrid with offshore wind power.

related literature. Section IV presents the system, data, and attack models. Section V outlines the new security protocol, followed by Section VI, which provides performance results. Finally, we draw the conclusion in Section VII.

II. Background

As a motivating example, we draw on our recent work [8], [9] which proposed a medium voltage dc microgrid system to supply power to a set of offshore production platforms. The loads on an offshore platform include large motors used for propulsion, station keeping, drilling, and pumping product to the surface, as well as auxiliary on-site functions (e.g., lighting; heating, ventilating, and air conditioning; etc.). The microgrid power system architecture is shown in Fig. 1. The main local source of electricity is provided by a group of 5 MW wind-turbines that produce ac current. Also a backup diesel generator maybe incorporated on each platform. The ac from the wind-farm is converted to dc through a three-level neutral point clamped rectifier that establishes the 5 kV dc bus voltage. Interfacing the dc bus and offshore production platform are two bidirectional dc/dc converters. These converters transform dc voltages within the architecture and serve as channels for power to flow that are controller regulated. The major load on a platform is a set of megawatt class induction motor drives used to propel the drilling mechanism, propulsion, and station keeping, and these can be modeled as constant power loads. The primary controllers of the motors use a decoupled *dq*-axis control to regulate both machine flux and current. The primary controllers provide measurements to the secondary controller, which controls the power supply to the dc/dc converters. The details of the control algorithms are given in [8].

In general, a set of offshore platforms (e.g., an oil field) will be powered by a windfarm leading to a system of interconnected microgrids. Fig. 2 adapted from [9] illustrates the control and communication architectures of the system. Inside the microgrid for the purposes of power regulation and protection, the communication architecture provides a number of logical communication channels: primary controller to the secondary controller; secondary controller to the dc/dc

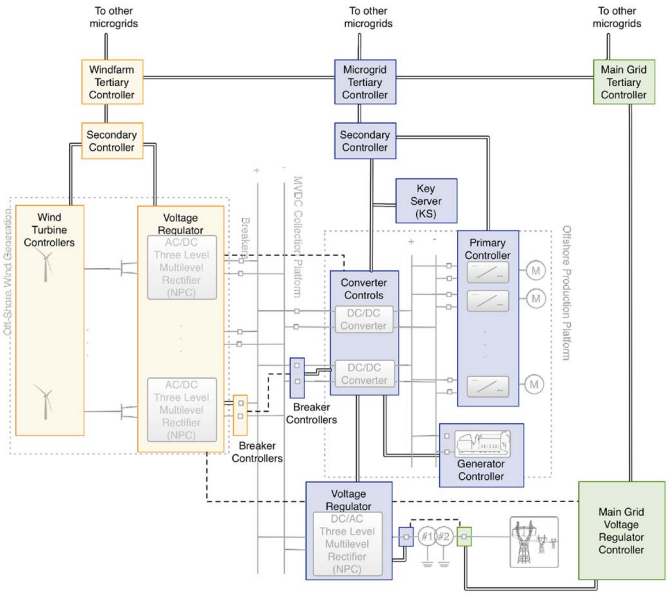


Fig. 2. Offshore platform microgrid control and communication architecture.

converters, backup generator, voltage regulator, and breakers. In order to facilitate power flow in and out of the microgrid, the secondary controller provides information and receives profiles from the tertiary controller. A tertiary controller communicates with the tertiary controllers of other microgrids and the main grid as shown in Fig. 2. Note that there may be a mix of organizations owning and operating the set of microgrids, the main grid and wind-farm.

The communication network provides the means for the microgrid control elements to signal among the components in order for the microgrids to operate, coexist, and connect to the main grid. The requirements of the communication network to support control signaling are: real-time performance guarantees, evaluated via worst case delay performance analysis; security, providing confidentiality and integrity guarantees while respecting the real-time delay boundaries; and high availability. Given the presence of high bandwidth communication networks, most of the delay in communication is introduced by the embedded control sub-systems that govern the flow of control messages and the execution of control logic. Many of the elements in the control systems are so called intelligent electrical devices (IED) such as voltage regulators, protective relays, and recloser controllers, that contain low-level microprocessors with small memories and have equipment lifetimes measured in decades. The execution cycles of such controllers must be considered in the design of a security architecture as they limit the type of confidentiality and integrity methods employed.

In the general microgrid context, the time scale of the primary control operation is in millisecond. Semi-independent primary control is needed with the controller taking into account commands from the secondary controller at a frequency in the range of tens of milliseconds or more [10]. For example, the secondary control would implement demand response as consumption in the microgrid increases, or supply from renewable energy decreases. The secondary controllers are expected to operate five to ten times slower or more than

the primary controllers. Finally, the tertiary control layer manages the power flow between the microgrid and main grid and between adjacent microgrids to facilitate optimal operation. High-level commands that involve the tertiary control are measured in seconds, or even minutes.

III. Related Work

The literature on cyber security for smart grid systems was recently surveyed in [11] and here we highlight relevant work. One major document addressing security for time-critical smart grid communication is IEC 62351 [12]. Released to build on top of IEC 61850 [13], it attempts to address the shortcomings of [13] in terms of cyber security for substation automation systems (SAS). The standard discusses data authentication via digital signatures, access control, security measures to prevent eavesdropping, prevention of playback and spoofing and intrusion detection. IEC 62351 specifies a variant of the Rivest, Shamir, and Adleman (RSA) algorithm, a public key infrastructure (PKI) cryptography algorithm for SAS communication. According to [12], the sender hashes the time-critical message using a secure hash algorithm (SHA-256) and then encrypts the hash with a private key via RSA in order to generate a signature. On the receiving end, the device hashes the message once again, decrypts the signed hash with the sender's public key, compares the received hash with the locally created one, and if the two hashed values match, it accepts the message as valid. However, the standard fails to meet the 3 ms end-to-end delivery requirement of IEC 61850 and thus far has little industry acceptance [14].

Recently, a number of publications [15]–[17] have focused on time-constrained secure communication. Three types of techniques have been proposed: 1) RSA-based approaches, similar to IEC 62351; 2) message authentication code (MAC) schemes, leveraging semantic security; and 3) one-time signature (OTS) protocols, making use of hash functions.

MAC-based schemes leverage a common semantic key between a sender and receiver pair. One popular MAC-based approach is timed efficient stream loss-tolerant authentication (TESLA) [15]. The TESLA protocol divides time into separate periods. The sender uses different keys to sign the messages in each epoch. Once the key has expired, the sender releases the key to the public, thus, allowing the receivers to verify any buffered messages. After the key is public, the sender needs to move onto the next key. The advantage of this protocol is the multicast, characteristic allowing a single message to be verified by multiple recipients. However, the buffering requirements make this protocol unsuitable for microgrid real-time communication. An alternative MAC principle-based approach uses the incomplete-set-scheme principle [18]. For every receiver, the transmitter has a separate short key. The sender signs a single message with all the private keys to all the recipients. To verify a message, each receiver uses the individual private key to create a local MAC and compares it to the received MAC. Since only the message sender has the full set of private keys, no other member of the communication cluster can fabricate the sender's identity. This protocol suffers from communication overhead, for n receivers we need n MACs in each message. However, it provides excellent computational performance due to its use of semantic cryptography.

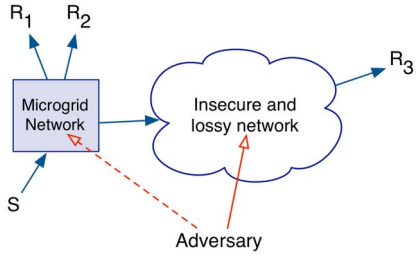


Fig. 3. Network model.

A number of OTS schemes have been proposed in the literature, such as [16] and [17]. At the core, they all try to address the issues of "one-timed-ness" and the large public key size. Wang *et al.* [19] have proposed TV-HORS which uses precomputed hash chains to authenticate data. The protocol creates a logical mapping between the data to the precomputed hash values. However, it requires a large number of precomputations resulting in long bootstrap times and large storage requirements. Furthermore, TV-HORS has a short key lifetime, which when coupled with the bootstrap time and storage requirements makes the protocol a poor fit for resource constrained applications.

The literature mentioned above focuses on either real-time systems security or general smart grid security. Currently, there is little microgrid specific security research [11] outside of [20]. This is especially true for industrial size microgrids such as studied here. In [20], a survey of microgrid protocols, architectures, equipment and security threats is given. The authors proposed an architecture defining interfaces and points for cyber security mechanisms by grouping microgrid equipment into enclaves based on their functionality. They note the crucial need to secure the microgrid control system communications. However, the real-time nature of the communications, the resource limitations of IEDs and the distributed hierarchical nature of the microgrid control systems are not addressed. Here, we note that the IEDs are the bottleneck of the electrical and communications co-system and as such develop a security solution that limits end-device computation and storage at the expense of communication overhead. We follow the principles laid out by the MAC-based incomplete-set-schemes, which make use of symmetric cryptography and provide computational efficiency.

IV. System and Attack Models

We adopt the system scenario illustrated in Fig. 3. The microgrid network is assumed to be behind the meter and may have a different owner than the other networks it interconnects with, which are assumed in worst case fashion to be insecure and lossy. As shown in Fig. 3, we consider a multicast communication scenario with a single sender S and multiple receivers R_i, $i = 1, 2, \ldots, n$ (note—unicast and broadcast are special cases of multicast). Table I summarizes the notation we adopt for the system model.

TABLE I
NOTATION TABLE

Parameter	Definition
S, R_i, n	sender, i-th receiver, and total number of receivers
t_d	Time to deliver a message by the network (including S and R transmission times, and intermediate network propagation times)
t_S	Sender's packetization (encryption + signing) delay
t_R	Receiver's processing (decryption + verification) delay
t_{ied}	Time to execute cycle of IED's control logic application
t_{aes}	IED's computation speed of encryption/decryption operation for the AES algorithm (in MiB/sec)
t_{cmac}	IED's computation speed for creating AES-CMAC signature (in MiB/sec)
d_{msg}	Size of message (in bits)
t_{max}	Maximum end-to-end delay bound
KS	Trusted microgrid key management server
k_{b_i}	Symmetric bootstrap key for IED_i know to KS and IED_i
k_{ks_i}	Symmetric confidentiality key known to KS and IED_i
k_c	Microgrid shared confidentiality key
N_i	Nonce generated by IED_i
N_i'	Nonce generated by IED_i to prevent replay attacks (different from N_i)
$v_{(i,j)}$	Authentication tag key between IED_i and IED_j
$H_{v_{(i,j)}}$	Function for creation of authentication tag

In Fig. 4, we show the end to end communication model. Controllers and IEDs communicate by making use of the UDP/IP protocol stack as is standard practice in real-time systems [21]. In such environments, TCP/IP is undesirable, since in the case of lost packet, by the time the retransmission reaches the intended receiver, the data is stale. Reliability is achieved via periodic transmission of data. In the model of Fig. 4, the network delivery delay is defined as t_d and includes the propagation and transmission delays. We use t_S to denote the time it takes a device to packetize and send a message after it has been passed down from the device's application. Additionally, we define t_R as the time it takes to process the incoming message and pass it to the receiver's application. We define $t_{\max}$, as the maximum end to end delay for all receivers of a message, where for successful delivery $t_S + t_d + t_R < t_{\max}$. In the event, the end to end delay of a message exceeds $t_{\max}$ it is discarded. In general, $t_{\max}$ is determined such that the microgrid power control can be designed to operate in a stable fashion. Note, that the end to end communication delay depends on many factors: the computational capability of the IEDs' hardware; the real-time operating systems; the application execution times; the speed of the communication links; and the topology and congestion status of the communication network.

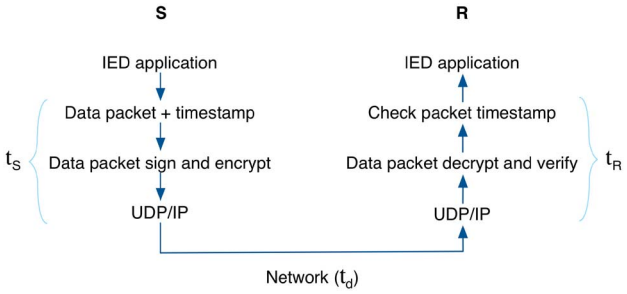


Fig. 4. End-to-end communications model within microgrid.

We classify the data in the microgrid network into three types: 1) messages carrying sampled data (e.g., current, etc.); 2) safety messages facilitating emergency power operations (e.g., opening a circuit breaker to prevent overload); and 3) control messages setting profiles for operation of the power network. We focus on the control messages as the data model since they pose the most demanding real-time delivery requirements. Each message has the following properties.

1) Sender S has no prior knowledge of the message contents before packet generation.
2) Each message is of broadcast or multicast nature.
3) All messages use UDP/IP and there are no retransmissions.
4) Each message is timestamped by the sender S.
5) R_i accepts the message if it is delivered and verified within $t_{\max}$ and rejects it otherwise.

It is assumed that all IEDs involved in electrical systems protection, operate in fail-safe mode. In the absence of communication, each protection IED would take independent protective actions. Lastly, we assume there exists a trusted third party that facilitates initial key exchange between devices that are not owned by the same entities, such as one microgrid to another, or between a microgrid and the main grid.

As an attack model, we assume an adversary has the following goals: 1) to inject a counterfeit message or to modify an existing message; 2) to intercept and to drop a legitimate message; and 3) to passively collect information from messages between S and R_i. To achieve those objectives, we assume that the adversary has the following capabilities: full access to the microgrid network, the adversary can capture, drop, delay, resend, or eavesdrop on some or all packets, the adversary can gain access to S or R_i and learn any key material.

V. MICROGRID SECURITY ARCHITECTURE

The goal of the proposed security architecture is to allow a sender S to send authenticated and confidential messages to one or more R_i over the microgrid and associated networks. This means, that within $t_{\max}$, each R_i can decrypt and verify every received message using the computational resources at its disposal. If an adversary injects, replays or modifies a message, each R_i should recognize the faulty message and discard it. The proposed architecture is simple by design as microgrid communications systems should be easily deployed and require little management. The architecture requires a standalone key management server (KS) in each microgrid. Since both confidentiality and authentication/integrity are provided

there are two types of keys used in communications. The confidentiality key is shared among a group, so that every group member can read the messages. The authentication keys are point-to-point between S and R_is. In order to achieve multicast communication S has a separate authentication key for each R_i. For purposes of clarity, any key used for a confidentiality encryption operation is referred to as k and any key used for creating an authentication tag is indicated by v.

A. Key Bootstrapping

For communication bootstrapping, the protocol adopts a modified version of the Needham–Schroeder protocol [22]. The modified version is safe against replay attacks, due to the use of an additional nonce N'. Each IED comes with factory printed bootstrap key k_{b_i} [e.g., 192-bit advanced encryption standard (AES) key]. At the time of installation, the technician enters the IEDs bootstrap key into the microgrid's KS. Once connected to the network, the IED_i sends a k_{b_i} encrypted join request to the microgrid's KS. In response, KS send back the microgrid's shared confidentiality communication key k_c and the IEDs individual confidentiality key k_{ks_i}. These steps are illustrated below

$$\text{IED}_i \rightarrow \text{KS} : \{\text{IED}_i, N_i\}_{k_{b_i}} \tag{1}$$

$$\text{KS} \rightarrow \text{IED}_i : \left\{\text{IED}_i, N_i, k_c, k_{\text{ks}_i}\right\}_{k_{b_i}}. \tag{2}$$

In order to communicate with other IEDs on the network, the IED_i sends a session bootstrap request to the IED_j. IED_j responds with a nonce encrypted under their personal confidentiality key k_{ks_j}

$$\text{IED}_i \rightarrow \text{IED}_j : \{\text{IED}_i\}_{k_c} \tag{3}$$

$$\text{IED}_j \rightarrow \text{IED}_i : \left\{\text{IED}_i, N'_j\right\}_{k_{\text{ks}_j}}. \tag{4}$$

The original IED forwards to the key server the two devices' IDs, a nonce and the token received from the other IED. The KS generates an authentication tag key $v_{(i,j)}$ for the new session, updates the token from IED_j to contain the key, and sends back to IED_i the encrypted message

$$\text{IED}_i \rightarrow \text{KS} : \left\{\text{IED}_i, \text{IED}_j, N_i, \left\{\text{IED}_i, N'_j\right\}_{k_{\text{ks}_j}}\right\}_{k_c} \tag{5}$$

$$\text{KS} \rightarrow \text{IED}_i : \left\{\text{IED}_j, N_i, v_{(i,j)}, \left\{\text{IED}_i, N'_j, v_{(i,j)}\right\}_{k_{\text{ks}_j}}\right\}_{k_{\text{ks}_i}}. \tag{6}$$

In the final step, the encrypted session information is forwarded back to IED_j. The authentication session key is confirmed by doing a simple arithmetic operation on the nonce between the two peers

$$\text{IED}_i \rightarrow \text{IED}_j : \left\{\left\{\text{IED}_i, N'_j, v_{(i,j)}\right\}_{k_{\text{ks}_j}}\right\}_{k_c} \tag{7}$$

$$\text{IED}_j \rightarrow \text{IED}_i : \left\{N_j, \left\{N_j\right\}_{v_{(i,j)}}\right\}_{k_c} \tag{8}$$

$$\text{IED}_i \rightarrow \text{IED}_j : \left\{N_j - 1, \left\{N_j - 1\right\}_{v_{(i,j)}}\right\}_{k_c}. \tag{9}$$

B. Communication

The communication protocol follows the principle of encrypt-then-MAC [23]. This is done for two reasons: there is no need to encrypt the authentication tag, thus, avoiding unnecessary encryption for S; and second, R_i can verify the message without decryption of the data and discard any fake messages. We present the steps for unicast and multicast communications in turn below.

1) Unicast Communications: Unicast communications is the normal mode for communications between IEDs and the primary controllers

IED_i encrypts the message with k_c (10)

$$\{m\}_{k_c} = E_{k_c}(m)$$

IED_i creates individual authentication tag (11)

$$\{m\}_{(i,j)} = H_{v_{(i,j)}}\left(\{m\}_{k_c}\right)$$

$$\text{IED}_i \rightarrow \text{IED}_j : \left[\{m\}_{k_c} || \{m\}_{(i,j)}\right] \tag{12}$$

IED_j creates digest from the received message (13)

$$\{m\}'_{(i,j)} = H_{v_{(i,j)}}\left(\{m\}_{k_c}\right)$$

IED_j compares the local and the received digest (14)

IF $\left(\{m\}_{(i,j)} = \{m\}'_{(i,j)}\right)$

IED_j accepts the message (15)

ELSE

IED_j rejects the message

END

2) Multicast/Broadcast Communication: As discussed earlier, some portion of the communication is multicast or broadcast in nature. Here, multicast communication is achieved at the expense of overhead. For multicast communication S emulates a multicast protocol by creating individual authentication digests for each IED_i within the microgrid. The creation of each authentication tag requires separate pair-wise keys. This is done for two primary reasons: first, each IED_i can verify the origin of a message; and second, in the event of an IED_i security breach, only the key material for that particular device is compromised and not for the entire microgrid. The protocol goes as follows:

Same as unicast communication (10) (16)

FOR EACH R_i (17)

IED_i creates message authentication tag

$$\{m\}_{(i,x)} = H_{v_{(i,x)}}\left(\{m\}_{k_c}\right)$$

END FOR

$$\text{IED}_i \rightarrow \text{Microgrid} : [\{m\}_{k_c} || \{m\}_{(i,j)} .. || \{m\}_{(i,n)}] \tag{18}$$

EACH R_i (19–21)

Same as unicast communication (13)–(15).

3) Communication Outside the Microgrid: There exist instances, when an IED within the microgrid needs to communicate with an outside IED. For example, when a breaker must inform another breaker on the other side of the power exchange bus. The outside breaker IED could be owned by different organization and as such the session set up would

involve two KSs. In order to meet the real-time communication requirement, the two KSs would be involved only in the key negotiation. Note, that a microgrid's internal confidentiality key k_c should not be shared with outside devices. As such, any IED that needs to communicate with the outside would have to maintain separate confidentiality keys and encrypt messages with both.

VI. Performance Analysis

In order to evaluate the proposed security protocol, we consider specific algorithms for its implementation and contrast it with RSA (PKI), the digital signature algorithm (DSA) (which is also used in PKI), and TV-HORS (OTS).

A. Bootstrapping and Key Size

The parameters used to calculate the performance are listed in Table II and are based on a 600 MHz microprocessor widely used in embedded systems such as power grid IEDs. We adopt the National Institut of Standards and Technology (NIST) recommendation to limit the key lifetime by requiring that at least 2^{48} message operations prior to a single message collision occurring. For the proposed scheme we use the AES algorithm for message confidentiality and the AES-based cipher-based message authentication code (CMAC) algorithm for message authentication [24]. A 192-bit AES key is recommended for data confidentiality and CMAC-based authentication, ensuring that the probability of forgery is quite low and the lifetime of the keys exceeds the lifetime of IED equipment. In the proposed algorithm, the bootstrap procedure is individual between each peer, thus, it is linear to the number of IEDs in the microgrid. In comparison for a PKI system to achieve the minimum required key lifetime, RSA needs at least 2048-bit key and DSA a 256-bit key [25]. Also, in PKI the sender bootstraps once for all receivers. The OTS protocol used for comparison is TV-HORS, due to its superior performance over other OTS algorithms [26]. In order to achieve the NIST specified key lifetime security level, TV-HORS requires a key of at least 500 KBytes [19]. In the target offshore platform microgrid system each primary controller sends one message every 80 ms, or 13 messages/s. Following [19], one can show the minimal time to bootstrap the key for TV-HORS is 120 s and the lifetime of the key is only 840 s. Thus, for every 14 min of operation each IED would have to pause sending data and bootstrap again the keys for 2 min. Of course, it is possible to increase the length of the key chains and therefore increase the lifetime of the keys, however, the storage requirements and bootstrap times increase as well. Lu *et al.* [27] stated similar findings in regards to using TV-HORS for substation communication security. Hence, TV-HORS is not a practical security solution for the target microgrid environment.

B. Theoretical Comparative Performance

While there is no benchmark standard for $t_{\max}$ in microgrids, we assume it to be 3 ms in accordance with IEC 61850. A comparative analysis is presented in Table III. The second column in Table III lists the number of keys an IED needs to store for the various security methods. If there are n devices in the microgrid, then for the proposed scheme each IED would be required to store k_c, two KS update keys, and $2(n-1)$ individual session keys (i.e., $(n-1)$ authentication keys and $(n-1)$ session keys). Note, that in the proposed scheme the KS needs to store one cluster k_c and $n(n-1)$ session keys.

TABLE II
Security Algorithms Time Performance Statistics [28]

OpenSSL performance statistics for VIA Eden 600Mhz	
Microgrid message payload (d_{msg}) [9]	42 bytes
Time for 192-AES encryption/decryption	0.008 msec
Time for 192-AES CMAC auth. tag	0.008 msec
Time for SHA-256 digest	0.007 msec
Time for RSA 2048 signature	312.5 msec
Time for RSA 2048 signature verification	9.1 msec
Time for DSA signature	91.7 msec
Time for DSA signature verification	111.1 msec

For the calculation of IEDs packetization latency t_S, we only consider encryption and authentication tag creation delays. On the receiver side, t_R, we only consider the time it takes to verify a message. For both metrics, TV-HORS has the fastest performance due to precomputation. In the proposed scheme, t_S increases linearly with the number of receivers, however, receiver verification consists of one authentication tag and one decryption operation. In the RSA and DSA cases, both the packetization and verification delays exceed the 3 ms end-to-end delay requirement. Hence, PKI algorithms are not be suitable candidates for microgrids.

The main drawback of the proposed scheme is the communication overhead introduced by the need to transmit separate point-to-point authentication tags in multicast communications. Toward minimizing the overhead, we make use of AES-CMAC-96 [29] with truncated 96-bit output authentication tags (while still using 192-bit keys for tag creation). Compared to the RSA approach, which has flat communication overhead of 2048-bit per message, our proposed protocol, has overhead that is linear to n in the broadcast case. However, for up to $n = 20$ the new scheme has less communication overhead than RSA. Finally, TV-HORS has flat overhead of a preconfigured number of SHA-256 messages digests per single authentication tag. For the data rates in question, the minimum feasible message digests per signature is 11 [17].

In the microgrid of Fig. 2, the communication network connects the following IEDs: ten primary controllers (assuming 4 MW drilling platform and 400 kW dc induction motors); secondary and tertiary controllers; the voltage regulator and the dc generator controllers; two dc/dc converters; 27 circuit breakers and a KS. This results in less than 50 IEDs. We define the application execution time of an IED as t_{ied}, the primary controller time as t_{pri}, the secondary controller as t_{sec}, the tertiary controller as t_{ter}, the dc/dc converter as t_{conv}, and the voltage regulator as t_{reg}. A control loop execution

TABLE III
COMPARISON OF MICROGRID SECURITY SCHEMES

Security Algorithm (type)	Storage per IED	t_S (msec)	t_R (msec)	Packet Size (bits)	Max R_is	Clock Sync Required
Proposed (Symmetric)	$(3+(2n-1))\cdot 192$ bits	$\approx n\cdot 0.008$	≈ 0.016	$d_{msg}+(n-1)\cdot 96$	>300	No
RSA (PKI)	2048 bits	≈ 312.5	≈ 9.1	$d_{msg}+2048$	0	No
DSA (PKI)	256 bits	≈ 91.7	≈ 111.1	$d_{msg}+160$	0	No
TV-HORS (OTS)	$>500KB$	≈ 0.0015	≈ 0.0015	$d_{msg}+11\cdot 256$	Unlimited	Yes (resolution in ms)

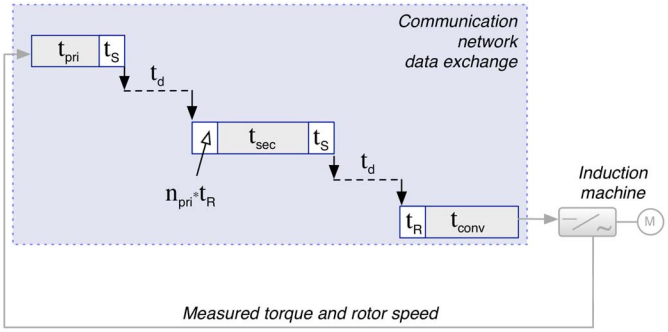


Fig. 5. Microgrid's primary–secondary distributed control loop.

time is defined as the time between when a measurement is emitted from the sensing IED until an adjustment command is delivered to the acting IED. Here, we focus on the primary–secondary and tertiary–secondary control loops. Since the data rates of IED equipment within the microgrid network are low (10–100 kb/s) in comparison to the link bandwidths (0.1–10 Gb/s), we assume the communication network is congestion free and ignore any intermediate router/switch buffering delays.

1) Primary–Secondary Control Loop: The primary controller at each motor provides torque and rotor speed measurements to the secondary controller every t_{pri} seconds. The secondary controller collects all the measured data, then calculates the appropriate duty cycles for each of the two dc/dc converters to alter the power flow to the machine loads. The latency between the measured torque and motor speed values and the adjustment of the power supplied by the dc/dc converters constitutes the primary–secondary control communication loop delay $T_{\text{pri}-\text{sec}}$. This is illustrated in Fig. 5. The primary controllers, as well as the two dc/dc converters, execute in parallel. However, the secondary controller has to process all the incoming data from the primary controllers before it can act, therefore, occurring an additional delay of $n_{\text{pri}}\cdot t_R$ (where n_{pri} is the number of primary controllers in the microgrid). Hence, the controller loop latency $T_{\text{pri}-\text{sec}}$ is

$$T_{\text{pri}-\text{sec}} = t_{\text{pri}} + t_{\text{sec}} + t_{\text{conv}} + 2\cdot t_S + 2\cdot t_d + (n_{\text{pri}}+1)\cdot t_R. \tag{22}$$

Utilizing Table II and assuming 100 Mb/s communication links, the one-hop propagation delay t_d is approximately equal to 0.05 ms. Further, taking values from the literature we set $t_{\text{sec}} = 500$ ms, $t_{\text{conv}} = 500$ ms [7], and $t_{\text{pri}} = 80$ ms [10]. For the proposed security architecture, the resulting control loop delay is $T_{\text{pri}-\text{sec}} \approx 1080$ ms. By comparison, if RSA (PKI) is used the control loop delay is $T_{\text{pri}-\text{sec}} \approx 1805$ ms, which is just under the 2 s latency threshold given in [30] to ensure stable operation of the microgrid's power network.

2) Tertiary–Secondary Control Loop: In a fashion similar to the above analysis, we evaluate the tertiary–secondary control loop delay $T_{\text{ter}-\text{sec}}$. The loop latency is expressed as

$$T_{\text{ter}-\text{sec}} = t_{\text{ter}} + t_{\text{sec}} + t_{\text{conv}} + 2\cdot t_S + 2\cdot t_d + 2\cdot t_R. \tag{23}$$

Assuming broadcast communications, with $t_{\text{ter}} = 500$ ms [10], the proposed protocol's delay is $T_{\text{ter}-\text{sec}} \approx 1580$ ms. However, if RSA is used instead, the loop delay is $T_{\text{ter}-\text{sec}} \approx 2144$ ms, which exceeds the stable operation threshold.

C. Microgrid Co-Simulation Performance

A co-simulation of the offshore platform microgrid was developed in order to more accurately evaluate the microgrid's power control and communication network interaction. The power system simulation [8] was developed in MATLAB and exported as generated code. The microgrid communication network was simulated using the Omnet++ simulation tool. The communication network was modeled as a UDP/IP/Ethernet network with 100 Mb/s links. The interface between the two simulators was developed using a custom adaptive scheduler in a discrete event system simulator framework [31]. Note, that the interaction between the two networks occurs due to the decision and action of the IEDs and controllers. Hence, the co-simulation scheduler takes into account each IEDs individual computation speed, execution cycle sub-routines, and internal/external events, in order to determine the co-simulation synchronization points.

The simulation results reported here were produced by running a power control test scenario and varying the number of multicast receivers. In the scenario each primary controller and induction motor starts at 1 s intervals. The secondary controller sends duty cycle commands to the dc converters in order to compensate for the disturbance introduced by the starting of the induction machines. After the microgrid power network is fully operational, the microgrid transitions from island to grid connected mode.

Fig. 6 shows the maximum observed end-to-end delay (i.e., $t_S + t_d + t_R$) during a simulation run versus the number of multicast receivers for the proposed security scheme (either using CMAC-192 or the truncated CMAC-96). Once can see that the end-to-end delay is consistent with the theoretical analysis and well below the 3 ms target.

Next we studied the primary–secondary control loop delay $T_{\text{pri}-\text{sec}}$ for the case of all of the IEDs active. The maximum

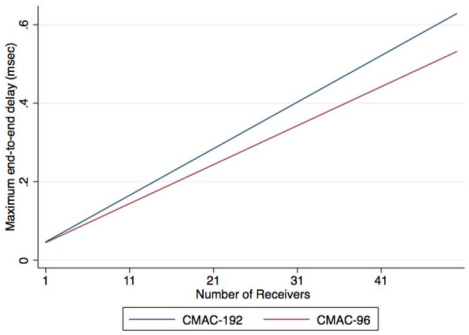


Fig. 6. Maximum end-to-end delay versus number of multicast receivers.

TABLE IV
MAXIMUM DISTRIBUTED CONTROL LOOP DELAY

Protocol	Distributed control loop delay [Theoretical / Simulation]
CMAC-192 & CMAC-96	1080 / 1128.5 msec
RSA	1805 / 2093.7 msec *unstable*
DSA	2485 / 4424.3 msec *unstable*

observed $T_{\text{pri}-\text{sec}}$ over the set of simulation runs is given in Table IV. The observed delay is larger than the theoretical model, due to the simulation incorporating the delay from intermediate nodes within the communication network, and the fact that the secondary controller has to process all the received primary controller messages prior to emitting any. We also include results for RSA and DSA, which are similar to the proposed scheme in that the simulation delay is larger than the delay predicted by the theoretical model. More importantly the RSA, DSA schemes result in unstable power system behavior, since the $T_{\text{pri}-\text{sec}}$ delay is too large. Note TV-HORS was not included as it results in the power system being unstable due to the long bootstrap time which must be repeated frequently given the limited key lifetime.

VII. CONCLUSION

This paper presented a security architecture for the communication network that is needed to facilitate microgrid power control operations. A security model, including network, data, and attack models, was formally defined. Based on the security model, we presented a new security protocol to address the real-time communication needs of microgrids. The implementation of the proposed security scheme was discussed and its performance was compared to well accepted security protocols. It was shown that existing schemes are either too slow or require too much memory for application in microgrids.

REFERENCES

[1] P. Piagi and R. Lasseter, "Autonomous control of microgrids," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Montreal, QC, Canada, 2006, pp. 1–8.

[2] M. Prodanovic and T. Green, "High-quality power generation through distributed control of a power park microgrid," *IEEE Trans. Ind. Electron.*, vol. 53, no. 5, pp. 1471–1482, Oct. 2006.

[3] S. Anand, B. G. Fernandes, and M. 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.

[4] R. Lasseter and P. Paigi, "Microgrid: A conceptual solution," in *Proc. IEEE 35th Annu. Power Electron. Spec. Conf.*, vol. 6. Aachen, Germany, Jun. 2004, pp. 4285–4290.

[5] K. De Brabandere, K. Vanthournout, J. Driesen, G. Deconinck, and R. Belmans, "Control of microgrids," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Tampa, FL, USA, 2007, pp. 1–7.

[6] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1963–1976, Dec. 2012.

[7] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuña, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 158–172, Jan. 2011.

[8] B. Grainger *et al.*, "Analysis of an offshore medium voltage DC microgrid environment—Part I: Power sharing controller design," in *Proc. IEEE PES T&D Conf. Expo.*, Chicago, IL, USA, 2014, pp. 1–5.

[9] V. Kounev, D. Tipper, B. Grainger, and G. Reed, "Analysis of an offshore medium voltage DC microgrid environment—Part II: Communication network architecture," in *Proc. IEEE PES T&D Conf. Expo.*, Chicago, IL, USA, 2014, pp. 1–5.

[10] J. M. Guerrero, J. C. Vasquez, J. Matas, M. Castilla, and L. G. de Vicuña, "Control strategy for flexible microgrid based on parallel line-interactive UPS systems," *IEEE Trans. Ind. Electron.*, vol. 56, no. 3, pp. 726–736, Mar. 2009.

[11] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, Dec. 2012.

[12] *International Electrotechnical Commission Technical Committee 57*, IEC Standard 62351, Jan. 2010.

[13] *International Electrotechnical Commission Technical Committee 57*, IEC Standard 61850, Jan. 2003.

[14] S. Fuloria, R. Anderson, K. McGrath, K. Hansen, and F. Alvarez, "The protection of substation communications," in *Proc. SCADA Security Sci. Symp.*, Miami, FL, USA, 2012, pp. 1–13.

[15] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proc. IEEE Symp. Security Privacy*, Berkeley, CA, USA, 2000, pp. 56–73.

[16] L. Reyzin and N. Reyzin, "Better than BiBa: Short one-time signatures with fast signing and verifying," in *Information Security and Privacy*. Berlin, Germany: Springer-Verlag, 2002.

[17] K. Cairns, C. Hauser, and T. Gamage, "Flexible data authentication evaluated for the smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Vancouver, BC, Canada, 2013, pp. 492–497.

[18] C. Szilagy and P. Koopman, "A flexible approach to embedded network multicast authentication," in *Proc. 2nd Workshop Embedded Syst. Security*, Atlanta, GA, USA, 2008, pp. 1–8.

[19] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, "Time valid one-time signature for time-critical multicast data authentication," in *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, 2009, pp. 1233–1241.

[20] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, "Microgrid cyber security reference architecture," Sandia Nat. Lab. (Hierarch. SNL-NM), Albuquerque, NM, USA, Tech. Rep. SAND2013-5472, 2013.

[21] W.-J. Kim, K. Ji, and A. Ambike, "Real-time operating environment for networked control systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 3, no. 3, pp. 287–296, Jul. 2006.

[22] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[23] N. Smart, "ECRYPT II yearly report on algorithms and keysizes," Dept. Inf. Technol. Commun., ECRYPT, Austin, TX, USA, Tech. Rep. ICT-2007-216676, 2010.

[24] M. J. Dworkin, "Recommendation for block cipher modes of operation: The CMAC mode for authentication," Inf. Technol. Lab., Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-38B, 2005.

[25] *Algorithms, Key Sizes and Parameters Report*, ENISA, Heraklion, Greece, 2013.

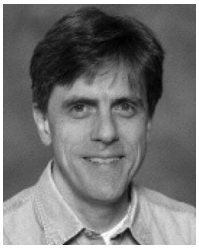
[26] Y. W. Law, Z. Gong, T. Luo, S. Marusic, and M. Palaniswami, "Comparative study of multicast authentication schemes with application to wide-area measurement system," in *Proc. 8th ACM SIGSAC Symp. Inf. Comput. Commun. Security*, Berlin, Germany, 2013, pp. 287–298.

[27] X. Lu, W. Wenye, and J. Ma, "Authentication and integrity in the smart grid: An empirical study in substation automation systems," *Int. J. Distrib. Sensor Netw.*, vol. 2012, Nov. 2012, Art. ID 175262.

[28] OpenWrt. (2014). *The OpenWrt Developer Team*. [Online]. Available: https://openwrt.org
[29] IETF. (May 2014). *The AES-CMAC-96 Algorithm and its Use With IPSEC*. [Online]. Available: http://tools.ietf.org/html/rfc4494
[30] Q. Shafiee, J. C. Vasquez, and J. M. Guerrero, "Distributed secondary control for islanded microgrids—A networked control systems approach," in *Proc. 38th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Montreal, QC, Canada, 2012, pp. 5637–5642.
[31] J. J. Nutaro, *Building Software for Simulation: Theory and Algorithms, With Applications in C++*. Hoboken, NJ, USA: Wiley, 2011.

Velin Kounev (S'12) received the B.S. degree in computer science from Goshen College, Goshen, IN, USA, in 2002, and the M.S. degree in telecommunications from the University of Pittsburgh, Pittsburgh, PA, USA, in 2007. He is currently pursuing the Ph.D. degree with the School of Information Sciences, University of Pittsburgh.

From 2007 to 2011, he was a Software Engineer and a Communication System Architect for driverless real-time train control systems. The cybersecurity aspect of his research focuses on efficient authentication and confidentiality schemes for low compute power embedded devices. His current research interests include secure real-time communication protocols, system simulations, performance and reliability for smart grids, Internet of things, scalability, and multipoint properties of such protocols.



David Tipper (M'80–SM'96) received the B.S. degree in electrical engineering from Virginia Tech, Blacksburg, VA, USA, in 1980, and the M.S. degree in systems engineering and the Ph.D. degree in electrical engineering from the University of Arizona, Tucson, AZ, USA, in 1984 and 1988, respectively.

He is the Director of the Graduate Telecommunications and Networking Program, and an Associate Professor with the School of Information Sciences, University of Pittsburgh, Pittsburgh, PA, USA. His current research interests include network design, network reliability performance analysis techniques, and information security. His research was supported by grants totaling over $8.8 million from various government and corporate sources such as the National Science Foundation, Defense Advanced Research Project Agency, the National Institute of Standards and Technology, the Army Research Office, IBM, and AT&T. He has co-authored the textbook *The Physical Layer of Communication Systems* (Artech House, 2006), and co-edited and contributed to *Information Assurance: Dependability and Security in Networked Systems* (Morgan Kaufmann, 2008).

Dr. Tipper serves as a Co-Guest Editor of a Special Issue on Advances in Network Planning, which appeared in IEEE COMMUNICATIONS MAGAZINE in 2014, and *Telecommunication Systems on Reliable Networks Design and Modeling* in 2013.

Attila Altay Yavuz (M'10) received the B.S. degree in computer engineering from Yildiz Technical University, Istanbul, Turkey, in 2004; the M.S. degree in computer science from Bogazici University, Istanbul, in 2006; and the Ph.D. degree in computer science from North Carolina State University, Raleigh, NC, USA, in 2011.

Since 2014, he has been an Assistant Professor with the School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR, USA. He has been an Adjunct Faculty Member with the School of Information Sciences, University of Pittsburgh, Pittsburgh, PA, USA, since 2013. From 2011 to 2014, he was a Security and Privacy Research Group Member with Robert Bosch Research and Technology Center North America, Palo Alto, CA, USA. His current research interests include design, analysis, and application of cryptographic tools, protocols to enhance the security of computer networks and systems, privacy enhancing technologies such as dynamic symmetric and public key based searchable encryption, security in cloud computing, authentication and integrity mechanisms for resource-constrained devices and large-distributed systems, and efficient cryptographic protocols for wireless sensor networks.

Brandon M. Grainger (S'06–M'14) received the Ph.D. degree in electrical engineering from the University of Pittsburgh, Pittsburgh, PA, USA, in 2014.

He is currently a Research Assistant Professor with the Department of Electrical and Computer Engineering, Swanson School of Engineering, University of Pittsburgh. From 2004 to 2006, he performed four work rotations with ANSYS, Canonsburg, PA, USA. He was with Mitsubishi Electric Power Products, Inc., Warrendale, PA, from 2008 to 2009; ABB Corporate Research Center, Raleigh, NC, USA, in 2010 and 2011; and Siemens-Robicon, New Kensington, PA, in 2012. His current research interests include power electronic technologies, specifically, semiconductor evaluation, power electronic topology design, advanced controller development, high voltage dc/flexible ac transmission systems, and grid integration concerns.

Dr. Grainger is a Member of the Power Electronics Society (PELS) and the Industrial Electronics Society, and a Co-Chair of the IEEE Pittsburgh PELS Chapter. He was one of the first Endowed R. K. Mellon Graduate Student Fellows with the University of Pittsburgh.

Gregory F. Reed (M'85) received the B.S. degree in electrical engineering from Gannon University, Erie, PA, USA, in 1985; the M.S. degree in electric power engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 1986; and the Ph.D. degree in electrical engineering from the University of Pittsburgh, Pittsburgh, PA, USA, in 2007.

He is the Director of the Electric Power Initiative with the Swanson School of Engineering, University of Pittsburgh; the University Center for Energy, Pittsburgh; and Grid Technologies Collaborative of the Department of Energy National Energy Technology Laboratory's Regional University Alliance, Pittsburgh, and a Professor of Electric Power Engineering with the Department of Swanson Schools Electrical and Computer Engineering, Pittsburgh. He is an Inaugural Member of the National Academies of Science and Engineering's Energy Ambassador Program. He has over 27 years of combined industry and academic experience in the electric power and energy arena, including engineering, research and development, and executive management positions throughout his career with the Consolidated Edison of New York, New York, NY; ABB Corporate Research Center, Raleigh, NC, USA; Mitsubishi Electric Power Products, Inc., Warrendale, PA; and DNV-KEMA, Arnhem, The Netherlands. His current research interests include teaching activities and related pursuits such as advanced electric power and energy generation, transmission, and distribution system technologies; power electronics and control technologies such as flexible ac transmission systems, high voltage dc, and medium voltage dc systems, renewable energy systems and integration, smart grid technologies and applications, and energy storage.

Dr. Reed is an Active Member of the IEEE Power and Energy Society and the American Society of Engineering Education.