SECURE REAL-TIME SMART GRID COMMUNICATIONS: A MICROGRID PERSPECTIVE

by

Velin Kounev

B.A. in Computer Science, Goshen College, 2003

M.S. in Telecommunications, University of Pittsburgh, 2007

Submitted to the Graduate Faculty of

the School of Information Science in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

University of Pittsburgh

2015

UNIVERSITY OF PITTSBURGH

SCHOOL OF INFORMATION SCIENCE

This dissertation was presented

by

Velin Kounev

It was defended on

April 22nd 2015

and approved by

Professor David Tipper, Ph.D., University of Pittsburgh

Assistant Professor Attila Yavuz, Ph.D., Oregon State University

Associate Professor Prashant Krishnamurthy, Ph.D., University of Pittsburgh

Professor Taieb Znati, Ph.D., University of Pittsburgh

Professor Gregory Reed, Ph.D., University of Pittsburgh

Dissertation Director: Professor David Tipper, Ph.D., University of Pittsburgh

SECURE REAL-TIME SMART GRID COMMUNICATIONS: A MICROGRID PERSPECTIVE

Velin Kounev, PhD

University of Pittsburgh, 2015

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. In this dissertation we propose a distributed control architecture to govern the operation of a microgrid. The functional communication requirements of primary, secondary and tertiary microgrid controls are considered. Communication technology media and protocols are laid out and a worst-case availability and latency analysis is provided. Cyber Security challenges to microgrids are examined and 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. We propose a novel security protocol that is custom tailored to meet those challenges. The chosen solution is discussed in the context of other security options available in the literature. We build and develop a microgrid co-simulation model of both the power system and communication networks, that is used to simulate the two fundamental microgrid power transition functions - transition from island to grid connected mode, and grid connected to island mode. The proposed distributed control and security architectures are analyzed in terms of performance. We further characterize the response of the power and communication subsystems in emergency situations: forced islanding and forced grid modes. Based on our findings, we generalize the results to the smart grid.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

PREFACE

I would like to thank my committee for their guidance and contribution. Special thank you to Dr. David Tipper for his mentorship and support.

This thesis is dedicated to the memory of my father, Professor Kountcho Velev Kunev, MD, Ph.D. Благодаря за всичко, ти си с нас всеки ден!

1.0 INTRODUCTION

1.1 MOTIVATION

The U.S. electric grid is an independently owned, complex network of power plants and transmission lines. By and large, the grid constitutes wires, substations, transformers and switches. The existing infrastructure is unidirectional in nature - power is carried from the plants where it is generated to the end-consumers, where it is consumed. The geographical distance between generation and consumption is often large. This leads to practical inefficiencies. Only a third of the originating fuel is converted to electricity. Close to 10% is lost during transmission, and another 20% is held in reserve - only to be use in case of emergencies, or 5% of the time [8]. Due to it's ad-hoc construction the grid is prone to cascading failures resulting in wide-area blackouts. All electrical transmission has to operate on the same frequency at all times, and supply and demand between power plants and end-customers, has to be balanced in real-time. Deviations in operating frequencies and unequal balance are the primary technical reasons for domino effect failures.

The next generation electric grid, commonly referred to as "smart grid", is expected to address issues of inefficiency and reliability. This would be made possible by the introduction of two main improvements: distributed power generation and power flow control systems. Distributed generation means that power is generated closer to where it is needed. This approach elevates the need for transporting electricity over large distances, eliminating issues of in-transit power loss. Since local supply would be custom tailored to local demand, different areas of the grid would have to be segregated. This would ensure that multiple areas of supply and demand do not interfere with each other. By only controlling local frequency and power balance, wide-spread blackout would be less prominent. Protection

would ensure that the domino effect is interrupted - failure in one grid would be locally contained, and a local grid would be able protect itself by disconnecting from the main. Additionally, a local grid would be able to supply power to nearby failed grids. In the literature this small smart grid is commonly referred to as a microgrid.

A power network of microgrids is immensely complex. The current generation of power flow control system has to be re-thought. The Supervisory Control And Data Acquisition, or SCADA, was introduced after the large blackout of 1965 [9]. Initially rolled out in critical sub-stations in order to help visualize the state of the grid, today, SCADA has a large penetration in the transmission network. Still, the system was build to support uni-directional power flow, and post-failure manual power restoration. Foremost, SCADA is a information gathering system, and not an automated control and protection agent. For smart grid level of pervasive control and monitoring, the new control system would have to integrate information technology, communication technology and power system engineering. Distributed generation would mean that bi-directional power flow and automated protection would require on-the-fly autonomous actions from the control system without human supervision.

The vision of this modern grid is grand. The dilemma most utilities face, however, is how to get to the future as soon as possible, while minimizing cost and not taking any risks. Utilities still see their primary concern as keeping the lights on, and investments into unproven technology is viewed as unsound business. The cost of this grid of microgrids is staggering compared to a single uni-directional infrastructure and there is a lack of a business model for return on the investment. Customers are mostly unaware or uninterested in smart grids - electricity is a commodity, and the only sales pitch is how cheap it can be sold and how quickly power can be restored after failure. Microgrids are not a product, but a solution to supply challenges that the current grid is not capable of meeting. One can theorize that the smart grid would not emerge within the business community, but instead from an organization with specific and particular power needs.

One such customer is the U.S.A. Military and the Department of Defense. A military base is similar to a city, with houses, shopping centers and entertainment venues. Power to such installation is brought by a number of feeder lines, representing a security risk. Interruption of power jeopardizes the security of the base. A microgrid can continue supplying power to

the area even in the absence of the main feed, absorbing and dampening any disturbance due to service interruption. Another potential application for microgrids are business operations located in remote or underdeveloped regions such as offshore oil drilling rigs, or data centers in third world countries.

Today, smart grid and microgrid are still simply concepts. They aim to meet specific needs, yet currently they are loosely defined due to our lack of clear understanding of what they are. The evolution into the grid of the future could start with an intermediate hybrid distribution network (Figure 1). The current grid would be at the core of this network, its simply too vast to be replaced. Equipment modernization would take place from within (substation automation, phasor measuring units and so forth). Edge connected microgrids would provide custom solutions to high demand customers, such as the US military. A natural evolution would then take place until the technical difference between the main grid and edge microgrids would dissolve. A smart grid would be finally realized.

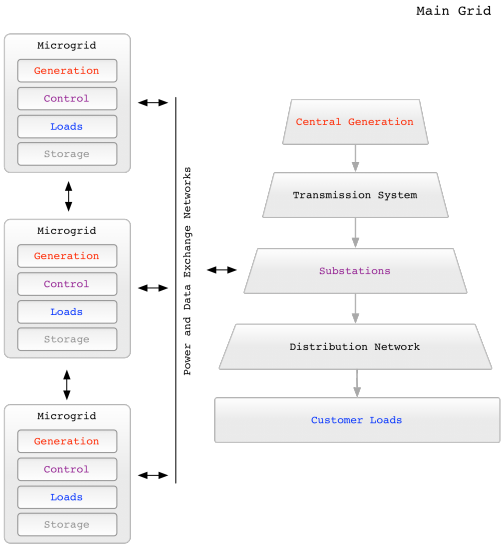

Figure 1: Network topology of intermediate hybrid distribution network.

1.2 CONTRIBUTION

This dissertation attempts to address the following question:

Can the current state-of-the-art telecommunication and security protocols provide the highly available secure communication required for real-time microgrid operations?

Key background concepts include microgrid operations, distributed control systems, network reliability and availability, network performance and cyber security. In this context, this dissertation makes the following contributions:

- We propose a distributed control architecture to govern the operation of a microgrid. The functional requirements of primary, secondary and tertiary microgrid controls are considered. Communication technology media and protocols are laid out and a worst-case availability and latency analysis is provided.
- Cyber Security challenges to microgrids are examined. We propose a novel security protocol that is custom tailored to meet those challenges. The chosen solution is discussed in the context of other security options available in the literature. Our approach is justified by comparing performance and scalability characteristics.
- Microgrids operate in two modes: grid connected, in which there is two-way power exchange between the microgrid and the main power grid (or possibly another microgrid), and island mode, in which the microgrid does not feed or draw power from its surroundings. We build and develop a microgrid model, that simulates the two fundamental microgrid power transition functions - transition from island to grid connected mode, and grid connected to island mode. The proposed distributed control and security architectures are analyzed in terms of performance. We further characterize the response of the power and communication subsystems in emergency situation - forced islanding and forced grid modes.
- Based on our findings, we generalize the results to the smart grid. Prevailing smart grid communication architectures and security standards are examined and discussed. We propose enhancements to those and justify our recommendations.

1.3 DISSERTATION OVERVIEW

This dissertation is organized as follows: we continue with a review of the related literature, each chapter of this work building upon the one preceding. Figure 2 lists the chapter layout and the background topics to be reviewed. Completed chapter are highlighted and future work is indicated with a dashed border.

Chapters I and II provide the Introduction, Motivation and Literature review of related background theory and concepts.

Chapter III presents a communication network and distributed control system architectures to provide signaling for the microgrid operations introduced in [10]. The different communication options are discussed and their performance in the context is characterized. Initial discussion regarding the embedded secondary and tertiary controllers is presented, including an overview of potential performance bottlenecks. The chapter presents the paper titled "Analysis of an Offshore Medium Voltage DC Microgrid Environment âĂŞ Part II: Communication Network Architecture" and presented at IEEE T&D PES 2014. I am the primary author of the paper and was written under the guidance of Dr. David Tipper. The paper is based on the work presented by Dr. Grainger et al. [11].

Chapter IV addresses the question of communication security of the distributed control architecture presented in the previous section. Security adds considerable performance strain to the system and limits some aspects of the communication flow. For that reason and the fact that microgrids and smart grids are critical infrastructure, the discussion of security protocol was important enough to be a separate topic by itself. We provide a solution that differs from the most research concepts found in the literature today. Our security protocol is discussed and compared to justify the decision. The chapter presents the paper "A Secure Communication Architecture for Distributed Microgrid Control" accepted in IEEE Transaction on Smart Grid 2015, special issue on âĂIJCyber Physical Systems and Security for Smart GridâĂİ. I am the primary author of the paper and was written under the guidance of Dr. David Tipper. Dr. Yavuz provided the expertise on encryption algorithms specifics

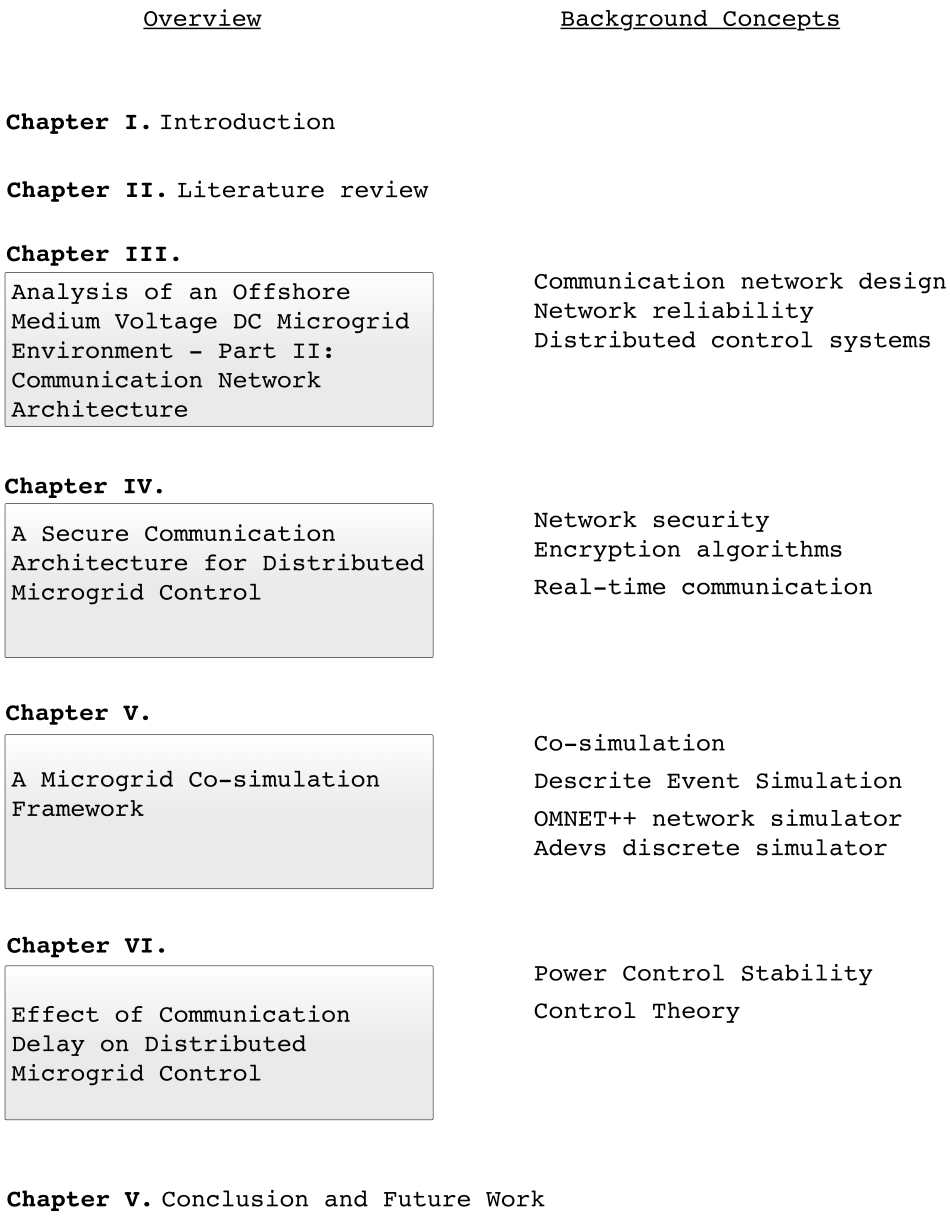

Figure 2: Thesis overview and related background topics.

and specifications. The paper is based on the work presented by Dr. Grainger et al. [11]. Chapter V aims to provide quantitative performance results of the solutions provided thus far in this dissertation. Microgrids still are in a research stage and real-world implementations

do not yet exist outside of a few small testbeds. The only possible approach is to build a simulation environment, while keeping in mind that it is only a simulation and as such it is an approximation. Co-simulation environment will be developed while taking advantage of some existing packages and creating new software where none is available. The co-simulator would incorporate the power and communication networks in one package. Each end-device would have to simulate simultaneous interaction with both environments and account for any possible cross influence between the networks. The test case scenarios would include normal microgrid transition modes, as well as emergency connect and disconnect events. The chapter presents the paper "A Microgrid Co-Simulation Framework" and presented at IEEE Cyber-Physical Week 2015. I am the primary author of the paper and was written under the guidance of Dr. David Tipper. Furthermore, I developed the co-simulator and the synchronization algorithm described in the paper. Dr. Martin Lévesque provided his expertise in the field of smart grid co-simulation and co-authored the paper. The paper is based on the work presented by Dr. Grainger et al. [11].

Chapter VI generalizes the finds from the previous chapters by the effect of communication and distributed system delays on the microgrid power control and stability. The paper is co-authored by myself and Dr. Grainger with an equal contribution.

Our conclusion and future work is discussed in Chapter VII.

2.0 RELATED LITERATURE

Smart grid and microgrid have different origins. Smart grid has its roots in government and business, and it is the umbrella term encompassing all possible modernization of the US power grid [12–15]. From improvement in automatic operations to real-time pricing for customers, the smart grid would enable a new business model for the power utility sector. In contrast, microgrid is a technical term put forth by the scientific community [16, 17]. It is a technical solution to the challenges facing today's aging power distribution network. Microgrid's definition is concrete and precise. It is, however, not possible without one enabling technology, telecommunications. The power community focuses on the improvements of power control algorithms, resulting in that most microgrid peer-review publications ignore the effects of the communication networks. Proposed concepts assume that control messages between distributed controllers flow securely and instantly, ignoring all questions of packet errors, network congestion and transmission delays and delay jitter. There publication neglect any performance degradations of the power flow due to the communication network's conduct. In contrast, the efforts of the computer, information science and telecommunication communities are directed at how to apply existing computation algorithms, protocols and concepts to power networks in the context of smart grid. Most publications from these groups marginalize power flow characteristics. As the NIST roadmap to smart grid [18] notes:

"When practices from one sector, such as the IT or communications sector, are applied directly to the power sector, care must be taken because such practices may degrade reliability and increase risk. This is because the requirements for the power sector, for timing of communications, for example, may be different from the IT and communications sectors."

The two communities lack a common language and terminologies. For solutions to have merit outside of pure scientific debate, it is important to have input from both sides. This work attempts to address this by providing communication network solutions to practical power flow problems that can be used in real-world applications. We choose microgrid operations for this investigation. The high level of maturity of microgrid theory governs this decision. The rest of this literature review aims to introduce all background concepts. We start by theoretically defining smart grid and microgrid, followed by an explanation of the relationship between the two. The discussion concludes with an overview of real-time and secure communication principles and practices.

2.1 SMART GRID DEFINITION

The smart grid emerged from the efforts of the US Government as the vision for the nation's future electrical network. The U.S. Department of Energy (DOE), in collaboration with the Federal Energy Regulatory Commission (FERC) and the National Institute of Standards and Technology (NIST), sets forth six key functionalities to be achieved by smart grid infrastructure: (1) Advanced Metering Infrastructure; (2) Demand Response; (3) Electric Vehicles; (4) Wide-area Situation Awareness; (5) Distributed Energy Resources and Storage; and, (6) Distributed Grid Management [19].

Each set of functions has its own requirements in terms of bandwidth, latency and availability for the communication systems. The communication infrastructure is divided into 3 parts: Home Area Network, Neighborhood Area Network and Wide Area Network. Summaries for each smart grid functionality is presented below.

- Advanced Metering Infrastructure (AMI): The primary connection between the customer and utilities provider. The function of the system is to collect and measure energy consumption for billing and statistical purposes. Future AMI evolutions are envisioned to allow automation modulation of energy loads during peak hours. This advanced two-way communication would require significant investment due to near real-time operational requirements. Operational requirements such as bandwidth, availability and latency are

expected to grow to significantly higher level.

- Demand Response (DR): One of the most significant advantages of smart grid is demand response (DR) functionality. Demand response is the reduction of the consumption of electric energy by customers due to increase of energy pricing or heavy burden on the system. Such operation can significantly reduce peak loads. The final most advance version of DR is automated DR, allowing on-premise smart appliances to respond to dynamic condition on the grid, and shift load consumption in a near-real-time manner.
- Wide Area Situational Awareness (WASA): A set of technologies designed to improve the monitoring of the power system across large geographical areas. Because of the inherently interconnected and interdependent nature of the grid operation, a disturbance in the power supply in one area can quickly spread and become a widespread problem, âĂIJwith cascading and deleterious consequencesâĂİ
- Distributed Energy Resources and Storage (DER): One of the main advantages of smart grid is more robust support for distributed energy resources into the grid. The energy flow will be multi-directional, from utility to home, home to utility, or even from home to home. For successful operation, real-time net metering is required in order to measure the electricity drawn from the grid minus the energy provided by energy sources on the premises. Finally, DER is suppose to provide more robust model for incorporating renewable energy sources into the grid.
- Electric Vehicles (EV): Mass-marketing of Electric Vehicles promises great reduction in emissions and energy independence. The current electrical grid is unlikely to provide the peak capacity required to charge a significant number of EV during peak hours. Further, EVs present a new opportunity as electric storage devices, that can balance load demands across the grid.
- Distribution Automation (DA): Would allow utilities to remotely monitor and control equipment in its distribution network through automated decision-making, providing more effective fault detection and power restoration. The primary function of DA is to reduce voltage to an appropriate level in order to isolate potential faults, and to ensure adverse effect do not spread to other portions of the grid.

2.2 MICROGRID DEFINITION

Microgrids have been proposed as a better way to implement the emerging potential of renewable energy generation [20]. The required building blocks of microgrids are the presence of an energy source, loads and back-up energy supply (traditionally energy storage or diesel generators). The fundamental operational requirements for microgrids are operation in island mode, requiring frequency and voltage stability for optimal power flow, grid connected to island mode, ensuring transition and stabilization for minimal load shedding and disruption, and island to grid connected mode transition, resulting in re-synchronization and minimum impact for sensitive loads during transient periods. From a control point of view, the microgrids can be summarized by three layers: primary, secondary and tertiary control. Each one of those layers is a separate physical entity, that may or may not be owned by the same operator.

Droop control for optimal power flow is the prevailing microgrid operation [21–24]. The primary controller(s) within the microgrid senses changes in the power network's frequency and adjusts the power output. No communication network signaling is present. The addition of a power source or removal of a load would be detected via changing power characteristics without the need for communication between controllers. Once the controller detects a change in the operating frequency, it adjusts the generator to produce more power in the event of a load addition, or less power in the event of a load removal. Droop control is a basic operation needed for the microgrid power balance and power flow operation.

Such concepts are not new to the power transportation community [9]. For decades, utilities have employed similar algorithms in substation automation. In the event of power line removal from the network, the bus downstream would be the first power equipment that detects voltage decline. The bus taps its transformer in order to restore distribution voltage to its target levels. If the transmission voltage decays under target minimum, the operator may insert additional capacitor banks. This would raise the voltage back to nominal levels requiring the transformer to tap back down as to avoid over-voltage at the bus. Each tap is mechanical operation and the opening and closing results in wear to the equipment. Furthermore, the detect-and-then-act mode of operation of the power network introduces

transient periods of power instability that can last tens of seconds.

The main idea behind the coupling of power and communication systems is that such unnecessary mechanical operations can be avoided. In the example above, the operator could select a sequence of events to take place, ensuring the additional voltage source is online prior to tripping of the power line. This would result in shortening the transient period and extending the life of the power equipment.

2.3 RELATIONSHIP BETWEEN SMART GRID AND MICROGRID

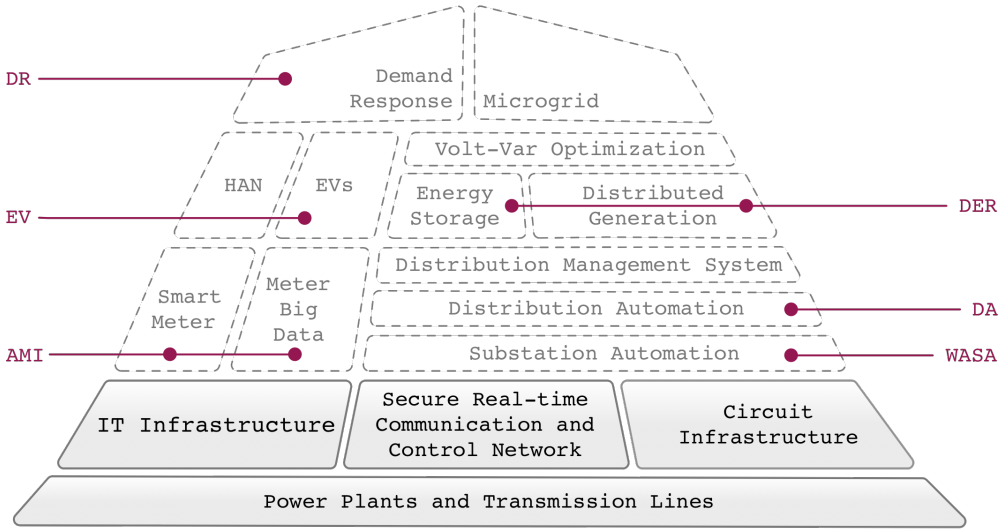

Figure 3: Building blocks of smart grid, and the relationship to microgrid. DOE's definition of smart grid functionality is indicated on both sides of the pyramid.

The smart grid definitions put forth by the Department of Energy are high-level applicational requirements. To be realized, a number of enabling technologies and intermediate steps must take place. Figure 3 depicts smart grid's architecture at a high level going from bottom to top [8]. At the bottom, the IT infrastructure, the secure real-time signaling

network and the circuit infrastructure would lay on top of the physical power plants and transmission lines. These two bottom layers are the foundations for all future applications. Each new layer that builds upon the previous one is more complex, requiring a higher level of performance and interoperability. The horizontal integration at each level is the basic building blocks of smart grid; nevertheless, functionality is only possible when the vertical blocks start working together. Smart meters and the data collected from them would make use of the IT infrastructure. Once in place, the advanced metering infrastructure (AMI) would enable utilities and customers to have near-real time pricing and service updates. At each customer premise, the home area network (HAN) would allow for the connection of customer electronics and electric vehicles (EV) to smart meters. Furthermore, HAN would allow for remote control of power electronics, eventually leading to demand response (DR). This is the most significant improvement envisioned in smart grid, enabling real-time load shedding control by the utilities. As such DR is among the most technically complex portions of smart grid. If DR is to be possible, utilities would have to invest in modernization of the core distribution network. The modernization would start in the distribution substations, giving operators up-to-date wide area situational awareness (WASA). Once substations not only provide monitoring data, but take automatic preventative actions, distribution automation (DA) would be possible. The distribution management system would be centrally controlling the two-way flow of electricity in the transportation network. The ability to balance two-way power flow would enable energy storage and distributed generation, or DER. These two items are fundamental features of microgrids and would have to be implemented in the core network before a microgrid could be connected. Until then, microgrids would have to operate in island mode or be used only for a backup in case of the main line failures (U.S.A. military application of choice). Finally, volt-var optimization would be possible since each bus in the network would provide real-time statistics, enabling the reduction of safety buffers and optimizing power flow.

2.4 REAL-TIME COMMUNICATION FOR POWER NETWORKS

A communication system would provide the fast, secure and reliable means for microgrids to operate and coexist. During normal operations, signaling would allow microgrids to synchronize with the main prior to connecting, extending equipment lifetime and minimizing transient periods in the electrical network. In emergencies, signaling would ensure that the power exchange would be disengaged prior to power equipment's detection of abnormal levels of voltage or frequency, thereby avoiding any potential damage.

In order to achieve those goals, the three main requirements of the communication network are: real-time performance guarantees, evaluated via worst case delay performance analysis; unquestionable security, providing tempering and confidentiality guarantees while respecting the real-time boundaries; and extremely high availability, needed to ensure the non-interrupted service. These are challenging due to the simple fact that both power and communication subsystems are electrical networks. The first, the power, is an analog electrical system, while the second, the communication, is a digital electrical system. Even in the presence of fibre-optic communication links, most of the delay in the communication network would be introduced by the embedded control sub-systems that govern the flow of control messages and the execution of control logic. These systems are digital electrical machines, and as such the challenge can be summarized as electricity chasing electricity.

To illustrate, let us consider the following sequence of events. After the detection of an emergency event in the power network, the protection equipment would send notification messages to neighboring equipment via the communication system, in order to prevent domino effect failures. However, these messages would only be relevant if they arrived prior to the arrival of any harmonics in the electrical network - digital electrical packets would be racing against transient analog voltage. Additionally, messages to protection equipment located further than one-hop away, would have to be processed by intermediate network devices. Such devices add nominal processing delay, due to the execution of internal routing protocols. Buffering delay would be added in case of network congestion, which in this example is very likely. All other power equipment would be also signaling at the same time. In a worst case scenario packet drops are possible if intermediate routing nodes reach their

internal buffer limits and they need to free up memory space. Communication packets carrying warning signals may not arrive at the destination prior to the power line's disturbance arrival. In such a scenario, the network packets are no longer of any use since the local protection equipment would have to take independent protective action. As a result of its own tripping, the machine would send additional warning messages, creating even more traffic in the already congested communication network. The problem would increase with each additional protection tripping. For a microgrid communication protocol to be a viable practical option, it must ensure that such scenarios would be handled properly.

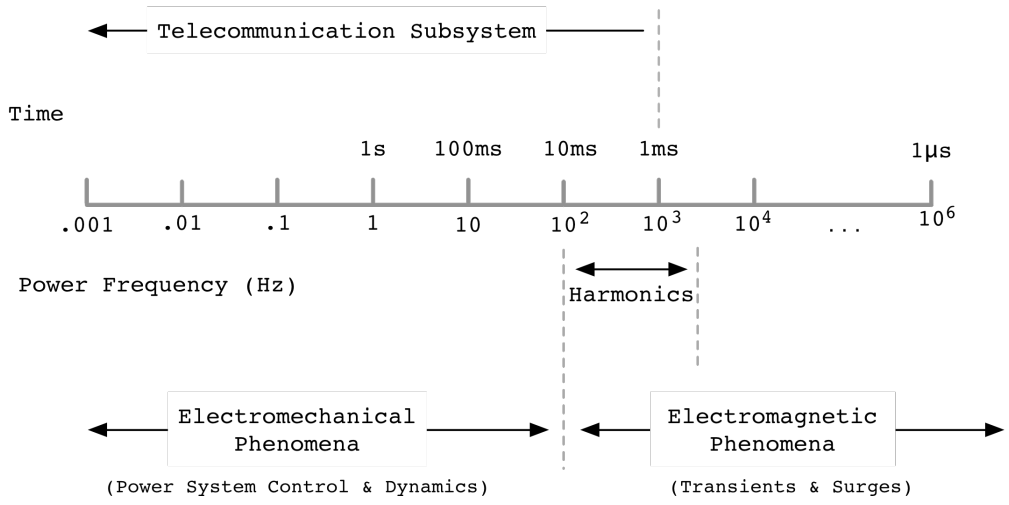

Figure 4: Power vs. Telecommunication subsystems timescale [3].

Figure 26 summarizes the different time-scales in the power and communication networks. The time unit of control signals traveling the telecommunication network is in milliseconds. Electrical phenomenon in the power network mostly last under tens of milliseconds. End-to-end packet delay would be close to the upper-time boundary of the power transient, meaning that any electrical power phenomenon would be hard to prevent from spreading via telecommunication signaling. The critical nature of operations further complicates the problem, by adding additional processing delay due to data encryption at each end point. Furthermore, most of the messages are broadcast/multicast in nature, resulting in multiple

packets for a single event notification. Reliability analysis of any communication protocol would have to include the proper delivery of all broadcast/multicast messages.

The power utilities have faced the problem of telecommunication enabled power distribution for decades. The major challenge faced by the substation automation system (SAS) is to provide interoperability between protection, control and monitoring services. In order to address this issue, in 2003, the international electro-technical commission published "Communication Networks and System in Substation" [25]. Today, the widely accepted IEC 61850 provides standards for telecommunication data exchange, data format definition (all the way up to level 7 of the OSI model), and XML based configuration. The main goal of the standard is to take away any ambiguity regarding the functionality of a subsystem, or Intelligent Electric Devices (IED). This document predefines all allowed power and network equipment, their functionality, their inputs and outputs, and all interfaces to be carried over the communication network. IEC 61850 uses a mixture of existing protocols in cases where those meet the stringent performance requirements, and define new customized ones where none exist, or performance is unsatisfactory.

The scientific community and industry has widely adopted a wide variety of protocols from organization such as IETF and IEEE [26–28]. By design principle, these clearly separate the communication network and the independent end-devices. In contrast, IEC 61850 views the power and communication networks, and all attached end-devices, as a holistic system designed for a specific task [25].

The IEC 61850 protocol's end-device model connects to the network via an unique network address. Within that physical device, there are one or more logical devices. Each logical device contains one or more logical nodes. A logical node contains named grouping of data, objects, and the implementation of the logic associated with particular power system function. In computer science terms, a logical node can be as simple as a single function or a class and the logical device can be viewed as a library of classes. IEC 61850 pre-defines all aspects from a single data field to a complete physical device. No new end-devices, functionaries, communication inputs and outputs, or modifications are possible. This is the only way to ensure that the performance specification are met. The protocol is a clear representation of the power system engineering design practices.

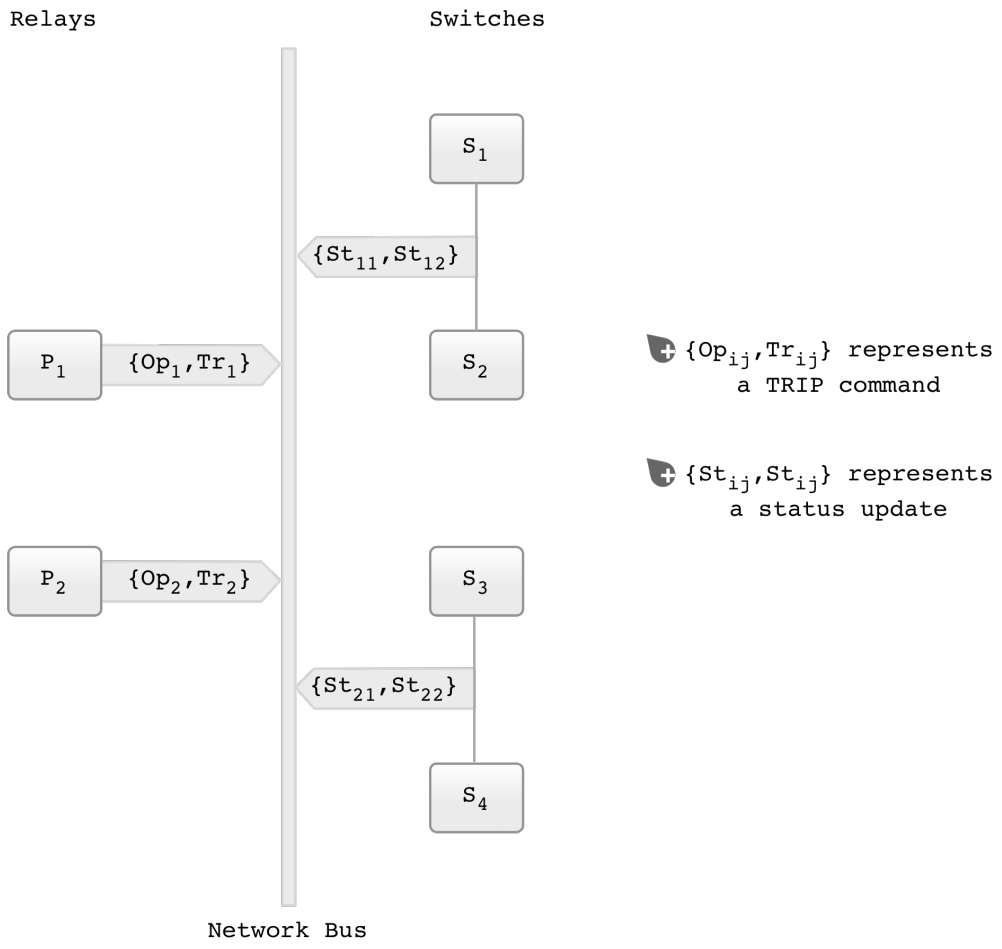

Figure 5: Substation network as per IEC61850 [4].

In the IEC 61850 protocol, the different logical devices communicate via publish and subscribe mechanisms. The protocol views the entire communication network as a single logical bus. Owners of data push updates "on the bus" and intermediate network devices route data to destinations, multiplexing any broadcast messages. For instance, a sample device configuration [4] may consist of two protective relays P_1 and P_2, and four switch gear S_1, S_2, S_3 and S_4 (Figure 5). Each relay maintains and publishes two data objects Op and Tr, indicating a TRIP command after fault detection. Additionally, P_1 and P_2 provide status updates onto the bus via two additional data objects $\{St_{11},St_{12}\}$ and $\{St_{21},St_{22}\}$. S_1 and S_2 subscribe and monitor $\{Op_1,Tr_1\}$, S_3 and S_4 monitor $\{Op_2,Tr_2\}$ for incoming TRIP commands. For redundancy purposes, S_1 and S_3 need to monitor the status of P_1 via

Table 1: Timing requirements of end-to-end message deliveries in IEC 61850 [1].

Message Type	**IEC61850 Protocol**	**Substation Interior**	**Substation Exterior**
Protection	GSSE & GOOSE	3ms	8-12ms
Monitoring & Control	TimeSync & ACSI	16ms	1s
Maintenance	ACSI	1s	10s
Data Sampling	SMV	3ms	10ms

$\{St_{11}$,$St_{12}\}$ data object, and S_2 and S_4 do the same for P_2 via $\{St_{21}$,$St_{22}\}$.

To meet the stringent power distribution delay requirements, IEC 61850 defines that interlocking TRIP messages and data sampling messages must be delivered to the destination within 3ms. The message delivery delay is the elapsed time from the instant the logical node in the detecting IED (relay in the example above) generates the message to delivery in the logical node of the protection IED (switches). Table 1 provides a summary of time requirements of IEC 61850. It is important to note that most messages are multicast, they have to be delivered to multiple IEDs, and the timing requirements apply to all subscribers.

Standard communication protocols were not designed to meet such delay constraints. For this reason, the IEC 61850 specifies new network protocols. For all sampled data, the protocol defines sample measured value (SMV) protocol (data objects $\{St_{11}$,$St_{12}\}$ and $\{St_{21}$,$St_{22}\}$ for example). Generic object oriented substation events (GOOSE) delivers all control commands, such as a TRIP command (data objects Op and Tr). A simple non-object oriented counterpart to GOOSE is generic sample measured state event (GSSE). The final two protocols are TimeSync for time synchronization and Abstract communication service interface (ACSI) for data queries and acquisition. Figure 6 presents the full IEC 61850 protocol stack.

In summary, IEC 61850 takes a drastically different approach to telecommunication. All end-devices and the communication network are not independent. The network would only carry specific data, and would only communicate to pre-defined devices. This is the way to ensure that the low latency and high availability requirements posed by the power network operations are met. Furthermore, the document establishes a standard for interoperability

between vendors, with predefined configuration and support for IED types. However, the main source of criticism of the standard is the complete omission of cyber security and the assumption of a single communication network. Such assumptions are valid in sub-station automation, however, microgrid operation would require communications between different substation communication networks. IEC 61850 is insufficient to meet those challenges and a new protocol definition is needed.

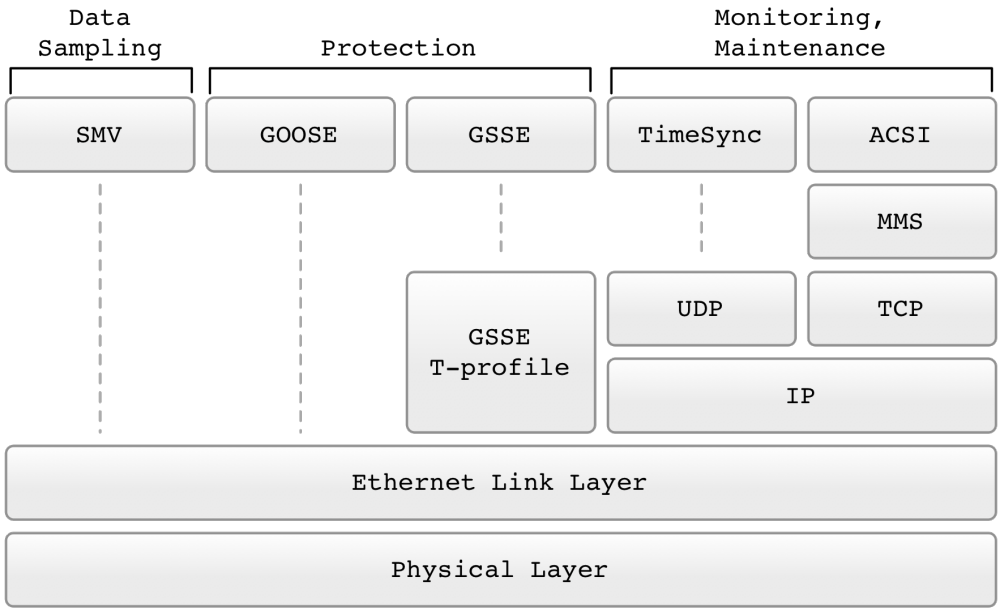

Figure 6: IEC61850 protocol stack. [1].

2.5 SECURE REAL-TIME COMMUNICATION FOR POWER NETWORKS

Microgrids have not yet received much attention outside the power distribution scientific community, resulting in the lack of microgrid related security communication research. The literature on smart grid, however, has identified a number of candidates to meet the security

needs of this new distribution system. Most of current publications mk are focusing on customer based non-critical application security [29–33]. An example of these applications is Advanced Metering Infrastructure (AMI), which is to provide customer with up-to-date energy consumption feedback. The primary concerns are customer privacy and the security of non-critical energy consumption feedback data.

The most noteworthy document addressing information security for time critical smart grid communication is IEC 62351 [34]. Released to build on top of IEC 61850, it attempts to address the shortcomings in terms of cyber security for substation automation communication. The document 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 RSA as the de-facto standard in substation automation communication. According to the specification, the sender hashes the time-critical message using SHA256 and then encrypts the hash with a private key via RSA in order to generate signature. The receiver 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.

The standard further specifies the conditions under which the protocols need to operate, as a processing power and memory limited equipment as well as narrowband communication channels. Defined is the threat model as disgruntled employees, industrial espionage, hackers, vandalism and terrorism. In order to address those threats in the specified environment, the document makes a number of suggestion. The aim is to secure the protocols already defined in IEC 61850. The authors payed special attention to the real-time data transmission suite - GOOSE and SMV that require response time of 3 ms. The solution provided, however, is very dubious. Sections of the documents seem to contradict each-other as to how to provide cyber security to those critical data transmissions. Originally, the authors suggest that since GOOSE and SMV communicate only on LAN, physical security and no data encryption, should be employed as to avoid any encumbrance to the already resource strained equipment. As a result, the standard instructs the device manufacturers to omit any implementation of data confidentiality, while data integrity should be still provided. Data confidentiality, via symmetric key cryptography is very efficient and given the small

data quantities it results in no noticeable performance degradation. On the other hand, the standard specifies RSA variant to be use for digital signatures. The algorithm based on public key cryptography is much more computation intensive then symmetric key counterparts, and current implementations cannot meet the stringent real-time delay delivery requirements [35].

Even further, it would appear that the authors of the standard became aware during the time of writing that the use of RSA signatures may take considerable time. As such, they made a rather strange suggestion that all end-devices should keep track of the current time, and any message received after 2 minutes of the transmission timestamp should be discarded. This suggestion is in direct contradiction with the timing requirements put forth in IEC 61850 (Table 1). Such requirement further complicates the security challenge by mandating devices to use current local times as security deterrent. In communication networks, synchronization of the drifting prone independent local clocks is notoriously difficult problem to solve. For that reason, most modern security protocol do not require synchronized clocks between the sender and the receiver. This is even more true regarding the problem at hand since power distribution operates on the millisecond timescale rather than seconds as in telecom networks.

More recently, a number of peer-review publications [35–40] have focused on time-constrained secure communication for the smart grid. There are three major branches of those: RSA based approaches, similar in approach to IEC 62351; message authentication code schemes (MAC), leveraging symmetric security; and one-time signature (OTS) protocols, making use of hash functions.

Message authentication code based protocols leverage a common symmetric key between a sender and receiver pair. There are two common protocols in the literature. First, there is Timed Efficient Stream Loss-tolerant Authentication (TESLA) [35]. 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 in public, thus allowing the receivers to verify any buffered messages. Further, once the key is public, the sender loses all it privacy leverage and needs to move on to the next key. The advantage of these protocols is the one-to-many, or multicast, characteristic allowing a single message to be verified by multiple recipients. However, the buffering requirements make this protocol unsuitable for

real-time communication.

The second MAC based variant uses the incomplete-set-scheme principle. For every receiver, the transmitter has a separate short key. The sender signs a single message with all the private keys of all the recipients. To verify a message, each receiver uses a 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 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 symmetric cryptography as opposed to the public key counterparts.

In the last decade, new authentication based schemes have received much attention. Originally designed for sensor networks, which are resource constrained, those protocols leverage the speed of one way hash functions without a trapdoor. A number of One-Time Signature (OTS) schemes have been proposed [36,37]. At the core, they all thrive to address the two main shortcoming of the approach - it's "one-timed-ness" and the large public key size.

Wang et al [41] have proposed TV-HORS, one of the most cited security protocols in the context of the smart grid. TV-HORS uses pre-computed hash chains to authenticate data. Since a sender cannot know in advance what data would be sent and specific hash chains cannot pre-computed, the protocol creates a mapping of what data parts maps to a what hash value. The sender divides the time into epochs. In each epoch, there are an active public and private keys. Once the private key has been used to the point of jeopardizing security, it is released to the public, and the epoch is advanced by one. The defunct private key becomes the public key for the new epoch. Every message is cut into predefined size chunks. More chunks per message result in higher security, but shorten the length of the epoch. Each message chunk maps to generic pre-computed hash value from the private key and the final hash vector becomes the signature for the data. The receiver cuts the message again and hashes the chunks locally. If the received hash vector matches the locally computed one, then the end-device accepts the message. Since each received hash vector can be mapped to old public key, the receiver can verify that the received hash vector has not been replaced in transit. The limitation of the protocol is the quite large public key, compared to MAC

based protocols, and the short epoch duration in the cases of a large number of messages per second. There are a number of variants [42, 43, 43], with some of them extending the length of epochs, but the basic approach is the same and none has gained more publicity then TV-HORS.

In [1], Xiang Lu el al. simulated IEC 61850 while varying the CPU speed of the sender and receiver. Their results confirmed that most of the security protocols have poor performance, under 40% delivery rate (Table 2), when the CPU speed is below 600 MHz. Today, such 600 MHz is the standard CPU speed for equipment for power distribution networks on sale by Eaton Corporation [44] and Schweitzer Engineering Laboratories [45]. For comparison, the Department of Energy has mandated that most message that would be exchanged in the communication network employed in the core of the power distribution network would have to guarantee reliability above 99.999% [46]. Reliability in the context of the smart grid should be understood as a variant of performability [47]. Messages should be delivered error free within the specified time limit above the required availability threshold.

Table 2: Delivery ratio of GOOSE and SMV messages within the 3ms substation interior limit, while considering different signature schemes and based on the sender and receiver's CPU clock speeds [1].

	CPU Frequency		
Algorithm	**600 MHz**	**1 GHz**	**1.6 GHz**
No Encryption	97%	98%	99%
RSA	36%	63%	85%
MAC	87%	98%	98%
HORS	90%	98%	95%

2.6 CONCLUSION

The chapter reviews literature publication regarding power operations and communication networks in the context of smart grid and microgrid. The review started by defining the two terms and defining the relationship between the two. Both concepts pose real-time and high-security requirements to the communication network. The chapter reviews aÂănumber of real-time protocols and options presented in the literature, followed by an overview of the security extension. Furthermore, the review discussed areas of omissions and drawback in the presented solutions that would be the main focus of the thesis. The next chapter proposes a communication architecture for a DC based microgrid.

3.0 MICROGRID COMMUNICATION NETWORK ARCHITECTURE

Microgrids have been proposed as a better way to implement the emerging potential of renewable energy generation. The required building blocks of microgrids are the presence of an energy source, loads and back-up energy supply (traditionally energy storage or diesel generators). The fundamental operational requirements for microgrids are operation in islanding mode, requiring frequency and voltage stability for optimal power flow, grid to islanding mode, ensuring transition and stabilization for minimal load shedding and distribution, and islanding to grid mode, resulting in re-synchronization and minimum impact for sensitive loads during transient periods. Each of those operations are substantially complex and require the harmonic operation of the number of different sub-systems. The electrical distribution system needs to work in tight synchronization with the signaling system. Fast co-operation of those systems is dependent upon scalable and intelligently designed co-existence architectures. From a control point of view, the microgrids can be summarized by three layers: primary, secondary and tertiary control. Each one of those layers is a separate physical entity, that may or may not be owned by the same operator. Each control layer must function in unison with each other in a scalable and highly efficient manner. Designing a communication network architecture to meet the stringent real-time operation requirements of the control layers is the focus of this article. As a potential application for a microgrid scenario we focus on offshore drilling platforms supplied by wind farm power generation. Today, domestic offshore oil drilling takes place in the Gulf of Mexico and Northern Alaska. The eastern seaboards, from North Carolina through Maine, are locations with the greatest potential for offshore oil and gas drilling [48].

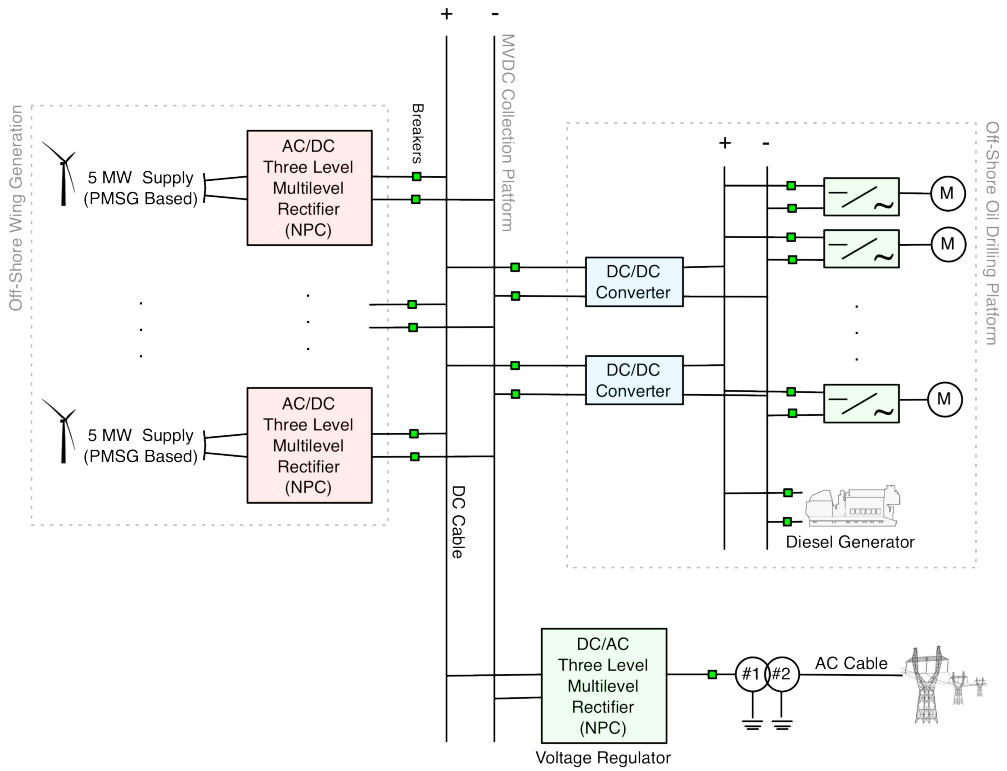

Figure 7: Local Offshore Wind Power Supplying Power to Offshore Oil Drilling Platform.

Drilling rigs and offshore oil platforms rely heavily on AC variable frequency drives for applications such as propulsion, station keeping, drilling, and pumping product to the surface. Supplying consistent and reliable power to those installations is a mandate with regards to system economics. Due to the ever increasing complexity of the oil drilling procedures, requiring newer techniques such as horizontal drilling at a greater depth, oil platforms require additional electricity to power the drills and auxiliary platform operations [49]. Currently, power is generated on site using diesel generators in a highly inefficient conversion process, resulting in tens of millions of dollars in operation expenses per platform [50, 51]. Using renewable energy, specifically wind generation at sea, is an appealing alternative. The potential generation capabilities of offshore wind power is much greater since offshore wind is stronger, less intermittent, and more consistent compared to traditional onshore wind generation.

In Part I, we propose a microgrid control architecture for supplying wind-turbine gen-

erated energy to the drilling platform. The architecture is distributed in nature (Figure 7). The correct operation of the power distribution network relies on reliable signaling provided by the telecommunication sub-system. The architectural details of the communication system for the power system architecture in Figure 7 is the focus of this article.

The remainder of this paper is organized as follows: Section II gives an overview of distributed control architecture, including the microgrid and wide-area communication networks. Section III presents telecommunication technological options, as well as security and addressing protocols for the proposed architecture. Finally, our conclusion is drawn in section IV.

3.1 COMMUNICATION NETWORKS

Communication network architectures are described in terms of the seven layer OSI Model [52]. For the purposes of the following discussion, the focus is on layers two and three - Media Access Level (MAC) and Internet Protocol (IP). Simply put, the MAC layer provides the functionality to send and receive data between a transmitter and a receiver, within the bounds of the same network. Basic transmission error checking is provided. The IP layer builds upon, adding intra-network addressing, substantially improved error checking, re-transmission capabilities for lost packets, congestion control, and session management (via Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)). In-depth discussion of the OSI Model and the above mentioned protocols is out of the scope of this paper, with additional resources listed [53].

Due to the real-time, and safety critical nature of the drilling operation, the communication network has to provide above all fast, reliable and secure service. The entire communication network can be envisioned as two separate networks: (1) microgrid network and (2) wide-area communication network. The microgrid network includes the secondary control, DC/DC converters, primary controllers, induction machines, and the diesel backup generator. For more details on the operation of the microgrid's energy control architecture please refer to Part I. The wide-area network, induces the tertiary control, wind turbine farm(s)

and the secondary control, with the secondary control functioning as a bridge between the two networks. The geographical distance between the elements of the wide area network can be quite high, in the tens of miles, depending on how far away the wind farms are installed from the offshore platform.

3.1.1 Microgrid Communication Network

The frequency of messages in the microgrid network is determined by the fastest cycle of a sub-system element in the network. There are three logical channels in the network (1) induction machine/primary controller to the secondary controller, (2) secondary controller to the DC/DC converters, (3) secondary controller to backup generator (Figure 8). There is no reverse logical channel between the secondary and primary controllers. The primary controller functions as independent local control. The channel between the induction machine and the secondary controller has the highest frequency of messages. The induction machine would provide torque and rotor speed measurements every 10 to 25 μs [54]. This high of a frequency is necessary in order to capture and address transient phenomenon due to grid islanding. The two measurements provided are float values, and the payload of every message is not extensive, however, the high update frequency means that the number of messages every second would be considerable. Each measurement value pair, is unique to the induction machine, and the number of measurements are proportional to the number of induction machines in the microgrid. Given the update cycle, the estimated number could be between 5,000 to 10,000 messages per induction machine per second. Once the secondary controller receives the measured values from each induction machine, it calculates the appropriate duty cycles for each of the two DC/DC converters, as to alter the demanded power flow to the machine loads. Those values are emitted with the same frequency of around 25 μs; however, there are only two sets of values transmitted, one to each converter, resulting potentially in around 10,000 messages per second (a message every 10 to 25 μs). The latency between a measured torque and motor speed values and the reception of the correlated control command by each of the DC/DC converters constitutes the distributed control loop delay experienced by the power system.

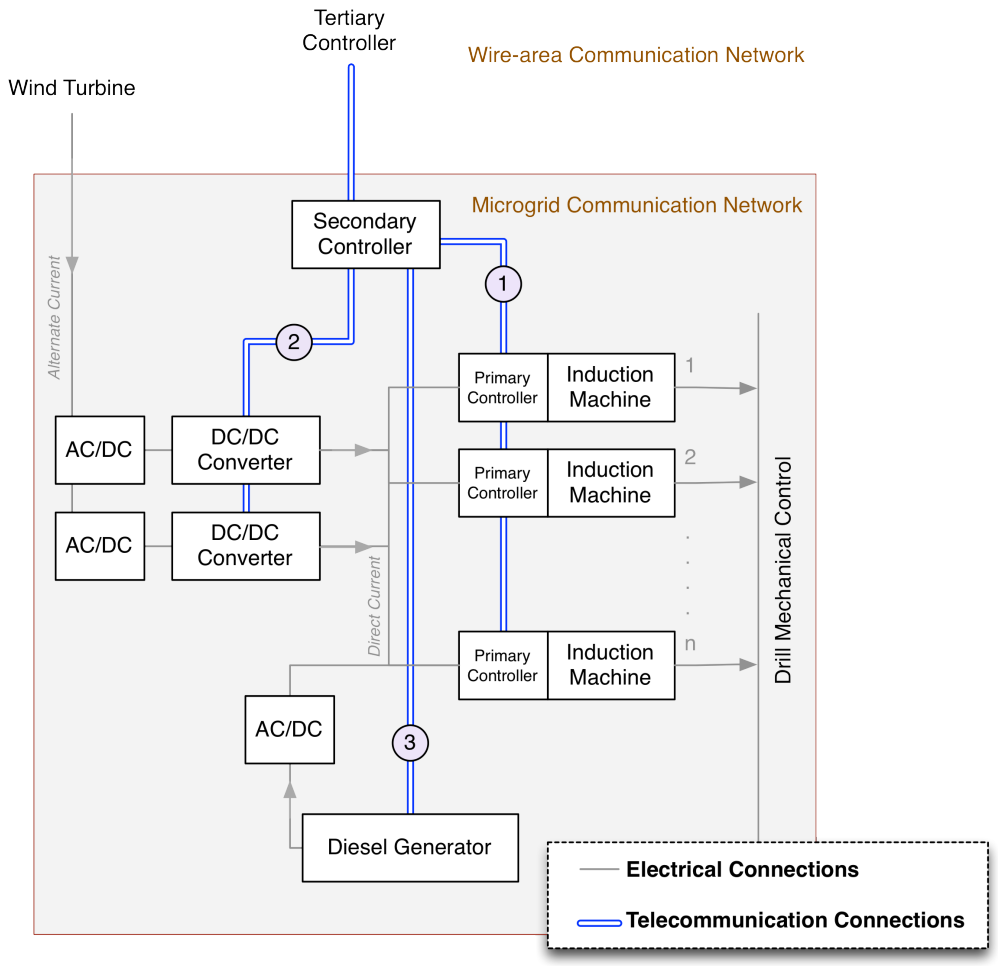

Figure 8: Architecture of microgrid communication networks.

The secondary controller would contribute significantly to the delay budget. The controller would have to interface with the wide-area control network via IP addressing, resulting in full IP stack included in the real-time operating system, and therefore, a slower runtime cycle. One possible way to avoid a slowdown in the cycle for the microgrid network interface is to have two execution cycles running in the embedded real-time operating systems of the controller. The processes should run on two physically separated processors communicating possibly via shared memory channels (Figure 9). This would allow the inside microgrid loop controller to operate on a much higher frequency, by only implementing MAC layer addressing and omitting encryption/decryption operations (steps (2) and (6) in Figure 9). On other hand, the outside network application would (1) query the outside interface (IP

Layer), (2) decrypt information, (3) read the logical channel for any message from inside the microgrid, (4) execute control logic, (5) write to the logical channel, (6) encrypt data and (7) write to the outside interface at the end of it's cycle. The inside loop controller would (1) receive network messages, (3) check the logical channel for any control instruction from the tertiary controller, (4) execute logic, (5) write messages to the tertiary controller, (7) and output messages to the appropriate local microgrid network port. Even by separating the controllers in order to gain performance, it is unlikely that the inside communication cycle would be able to keep up with the 10 to 20 μs message frequency. Without loss of generality, we assume that the inside communication execution cycle would be of at least 10 millisecond, and the outside communication cycle would be around 20 millisecond [55].

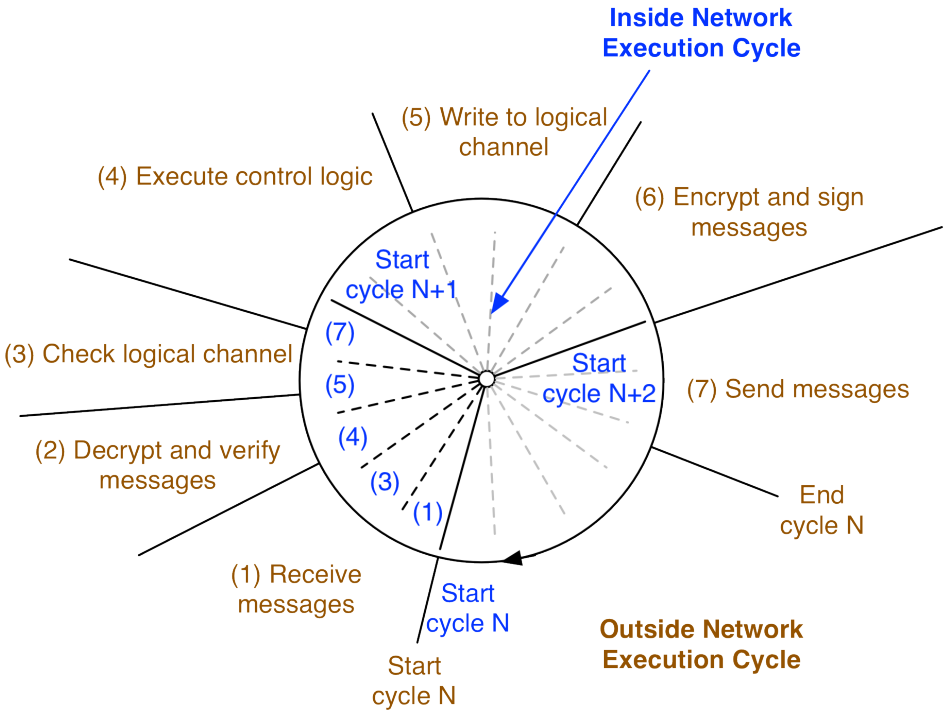

Figure 9: Secondary Controller's inside and outside communication cycles.

3.1.2 Wide-area Control Network

The tertiary controller would be in charge of balancing energy supply and demand between the onshore grid, wind farms, and one or more microgrids. In the event of insufficient wind generation, the tertiary control would initialize backup energy supply, via the diesel generator located in each microgrid, in order to continue non-interrupted drilling operations. The tertiary controller would be a distributed control system, with each microgrid having a dedicated top level controller (Figure 10). Due to the possibly large geographical area, resulting in a number of separate networks, the communication network would require IP addressing and significant security protocols. Contrary to the local microgrid control network, which creates messages with a deterministic high frequency, the wide-area control network would be of a non-deterministic nature. Two major types of messages would be present: keep alive between different sub-systems, and command/failure notifications. The keep alive message would be with a range between milliseconds and seconds. The control and failure messages are stochastic in nature as a result of changing wind directions and intensity or other natural phenomenon, as well as hardware and software failures.

Due to the size and the distributed architecture, security becomes an issue as well as interconnectivity and scalability. One wind farm may be connected to two or more oil platforms, and a tertiary control may communicate between multiple wind farms and platforms. Functionality provided by the IP layer would be needed here for session establishment and maintenance. Data encryption and authentication is vital for security protection. The network is assumed to be using UDP, and not TCP as transmission protocol. Retransmissions are not employed. In case of packet loss, the receiver would take into account the follow up packet. A retransmit packet will contain stale information, data too old to be acted upon, by the time it is received. Furthermore, in case of TCP it is possible to flood the network with retransmitted packets, creating congestion. This is due to the fact that TCP uses principle design to avoid loss in non-critical networks. The protocol tends to be over active and too aggressive in time-critical networks. Hence, the applications at the end points need to be robust enough in order to tolerate packet losses, up to a safe predefined number, and continue normal operation.

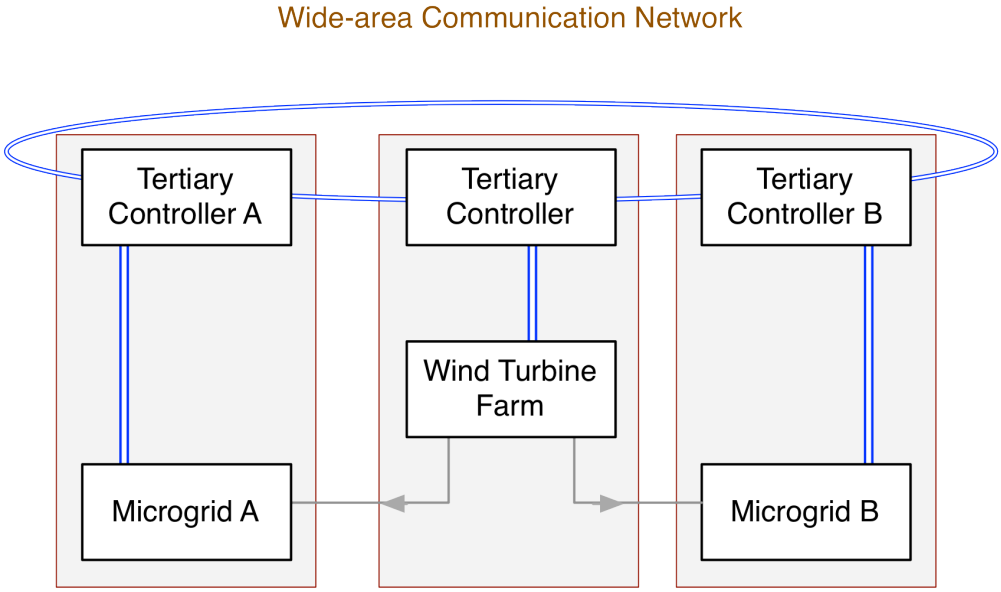

Figure 10: Architecture of wide-area communication network.

3.2 PERFORMANCE ANALYSIS OF THE DISTRIBUTED COMMUNICATION ARCHITECTURE

Communication networks are evaluated in terms of four factors - efficiency, latency, availability and reliability, and security. In the following section, we discuss each communication technology and evaluate the performance based on those parameters. Throughout the remainder of this section please refer to Table 6 for a summary of the information.

3.2.1 Availability and Reliability

Availability in communication networks is the percentage of time in which the network is in a specified operational state. The most simple representation, shown by (23), of availability is the product of all links and equipment availability A_i on the communication path assuming

a series arrangement.

$$A_{series} = \prod_{i=1}^{n} A_i \tag{3.1}$$

The above calculation is applied for a communication networks that do not have built in back-up paths. For networks with more then one path between source and destination pair, availability is determined by using (3.2).

$$A_{parallel} = 1 - \prod_{i=1}^{n} (1 - Ap_i) \tag{3.2}$$

where Ap_i is the availability of the i th path. In general, parallel networks are always more reliable, however they are much more expensive to implement. For the availability calculation in the microgrid and wide-area communication networks, we assume single path networks. Unlikely in reality, however it is important to analyze this base case in order to gain understanding of media options and their suitability.

3.2.2 Packet Size and Overhead

Efficiency is defined as the fraction of useful data bits out of the total bits transmitted. The extra bits are control information and they are referred to as overhead. There are two communication protocols employed in the network design (1) inside the microgrid (2) outside the microgrid/inside the wide-area. The goal of the former protocol is speed and reliability with minimal overhead. The goal of the latter is also speed and reliability, however some performance is sacrificed for the purposes of interoperability and security. In the communication protocol within the microgrid we assume that Ethernet is adopted and 42 bytes are used for the payload. This is the minimum allowed by the MAC protocol. There are an additional 42 bytes of mandatory MAC header. The overall efficiency is 50%, which is low, and a result of the small payload of every packet. This can be corrected by buffering some measurements and sending them in a single packet. This, however, goes against the real-time principle of the applications. Low efficiency is typical of such applications (real-time audio and video). In the wide-area network the payload would be 512 bytes (the minimum for UDP Packets), with additional 70 bytes of headers. The payload would also be encrypted,

however private key encryption does not expand the data it encrypts. The overall efficiency is much higher, around 90%. However, due to the larger packet size, there would be larger transmission delay.

Table 3: Summary of telecommunication protocols and media options for Microgrid and Wide-area networks.

	Microgrid Network	**Wide-area Grid Protocol**			
	Ethernet	Fiber	Wimax	Satellite	Microwave
Addressing	MAC	IP			
Message Packet Type	MAC	UDP			
Retransmissions	-	-			
Range (up to)	250 miles [56]	100's of miles [56]	10 miles [57]	100's of miles [58]	30 miles [59]
Security	Physical	Public and Private Key Encryption, Message Authentication			
Payload	42 bytes (minimum)	512 bytes (minimum)			
Overhead per Message	42 bytes (MAC)	42 bytes (MAC) + 20 bytes (IP) + 8 bytes (UDP)			
Transmission Rate (bits/sec)	1 Gbps	1 Gbps	40 Mbps	1 Mbps	45 Mbps
Message Transmission Delay (estimate)	0.6 μsec/link	4.6 μsec/link	120 μsec/link	>10 msec/link [58]	100 μsec/link
Link Availability (up to)	0.99999 [56]	0.9999 [56]	0.99	0.95 [60]	0.99 [59]
Oneway End-to-End Availability (up to)	0.99998 (2 links)	0.999 [1]	0.9 [1]	0.59 [1]	0.9 [1]
Protocols End-to-End Delay (estimate)	$\approx$ 10 msec (2 links)	$\approx$ 100 msec [1]	$\approx$ 100 msec [1]	$>$ 150 msec [1]	$\approx$ 100 msec [1]

3.2.3 Transmission Delays

There would be a number of sources of delay in the network - transmission delay, processing delay in the intermediate notes, and encryption/decryption delay (only for the wide-area network). Out of those, the transmission delay would be the least significant, and the processing delay the most. In the wide-area network there would be around 13 μs delay for private key encryption per message (assuming low level FPGA implementation of AES/Rijndael [61]), and another 4 ms [62] for authentication of the data. Assuming the real-time system can achieve, and that is a reasonable assumption [55], 10 ms per cycle for the inside interface, and 15 ms for the outside plus an additional 5 ms for encryption and authentication. This would result in around 10-11 ms delay for one hop end-to-end delay for the microgrid network, and 100 ms for the wide-area network.

1 All Wide-area availability and delay calculations assume that logical channels between two microgrids use the following path: two links inside the first Microgrid and pass through Secondary and Tertiary Controllers, one link between the two microgrids, pass through second microgrid's Secondary and Tertiary Controllers and two links inside the second microgrid (Figures 8 and 10).

3.2.4 Security

As stated previously, security results in too much overhead and delay and is unlikely to be used in the microgrid network. The assumption here is that the microgrid network would be contained in one physical location - the offshore platform. As such, the cyber security is replaced by physical security (e.g. locked cabinets for the equipment, and steel cable enclosures).

In the tertiary network, encryption is necessary due to the fact that the network has a large geographical span, possibly connecting multiple networks owned by different operators, and potential use of a wireless communication technology. Wireless signals are easily intercepted and fabricated, and they have to be encrypted to prevent malicious behavior.

There exist two encryption paradigms - public and private key encryption. The advantage of public key encryption is that two parties communicating with each other have their own separate keys. As such data encrypted by a party is also signed by that party, and cannot be later denied or produced by a third party. The downside of public key encryption is that it has quite slow decryption and especially slow encryption procedures. As such it is not used for large data streams. In comparison, private key cryptography is significantly faster, up to speeds of 3 Gbps [61], however both parties share the same key. Therefore, data is not signed and can be denied, or knowledge of the secret key allows a third party to join the communication undetected.

A common practice in security protocols is to use public key encryption in the initial communication setup, agree on a private key, and switch to private key encryption. Since public keys are individual, there is a need for key management intermediary, a Certificate Authority, that is in charge of distributing, renewing and retiring keys. The microgrid communication network would have to be protected by a firewall and a intrusion detection system (IDS). This is especially important, since inside the microgrid network there is no data encryption. Under no conditions, should an outside communication channel be allowed in those non-encrypted networks. The secondary controller should be the only channel of communication inside and outside the microgrid network. Deviation of this rule could result in adversary issuing plain text control commands to the DC/DC converters and damaging

the induction machines.

Private key set up delays, due to key negotiation and public key encryption, prior to switching over to private key encryption are out of the scope of this paper. The assumption here is that the session has been established.

3.3 CONCLUSION AND FUTURE WORK

This paper presented a communication network architecture for managing power supplied to an oil drilling platform through means of offshore wind generation. These system components can behave as a practical microgrid scenario. A number of different technology options with theoretical bounds were laid out. Future work would investigate those cases, as well as normal operation of the two networks, electrical and telecommunications, in co-simulated hybrid environments. The communication network performance would dictate functionality assignment between different sub-systems. For instance, certain function require delay unable to be provided by the communication system, and therefore the only possible assignment would be in the primary controller. The drawback of primary controller functions is that they operate in a non-collaborative fashion requiring higher safety margins in the overall system design. Functionality assigned to the secondary controller can take more accurate decisions and reduce overhead.

4.0 MICROGRID SECURE REAL-TIME COMMUNICATION

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 [63–65]. 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 re-synchronization 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. In the literature, [66–69] 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, multi-cast and broadcast communications.

Here we propose a secure communication architecture tailored to the microgrid control system. The main contributions of the 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 the literature 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 the paper is organized as follows: Section II presents background material on microgrids and the challenges they present. Section III provides an overview of 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 our conclusions in Section VII.

4.1 BACKGROUND

As a motivating example, we draw on our recent work [70, 71] which proposed a medium voltage DC microgrid system to supply power to a set of offshore production platforms.

The loads on a 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, HVAC, etc.). The microgrid power system architecture is shown in Fig. 11. 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 MW 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 uses 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 [70].

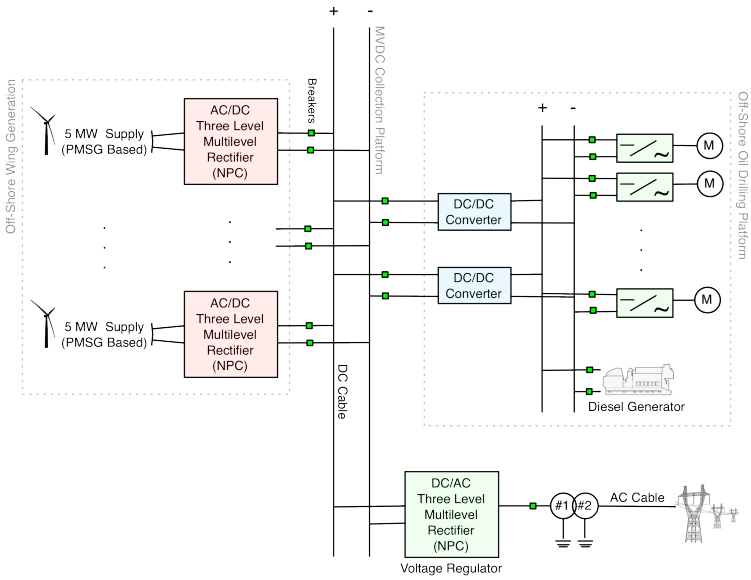

Figure 11: Offshore production platform microgrid with offshore wind power.

In general, a set of offshore platforms (e.g., a oil field) will be powered by a windfarm leading to a system of interconnected microgrids. Fig. 12 adapted from [71] 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 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. 12. Note that there may be a mix of organizations owning and operating the set of microgrids, the main grid and the wind-farm.

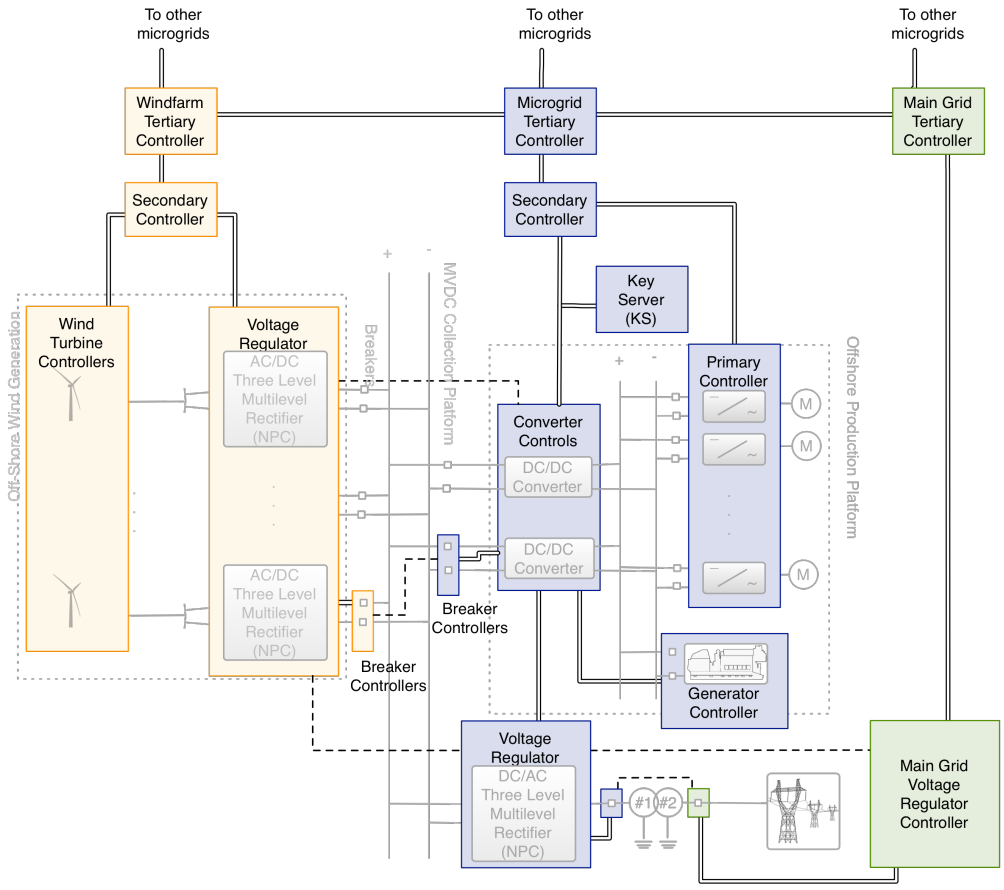

Figure 12: Offshore platform microgrid control and communication architecture.

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 subsystems 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 msecs. 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 msecs or more [72]. 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 the 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.

4.2 RELATED WORK

The literature on cyber security for smart grid systems was recently surveyed in [73] and here we highlight relevant work. One major document addressing security for time-critical smart grid communication is IEC 62351 [74]. Released to build on top of IEC 61850 [75], it attempts to address the shortcomings of [75] 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 [74], 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 [76].

Recently, a number of publications [77–79] 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 symmetric security; and (3) one-time signature (OTS) protocols, making use of hash functions.

MAC based schemes leverage a common symmetric key between a sender and receiver pair. One popular MAC base approach is Timed Efficient Stream Loss-tolerant Authentication (TESLA) [77]. 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 [80]. 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 symmetric cryptography.

A number of OTS schemes have been proposed in the literature, such as [78, 79]. At the core, they all try to address the issues of "one-timed-ness" and the large public key size. Wang et al [81] have proposed TV-HORS which uses pre-computed hash chains to authenticate data. The protocol creates a logical mapping between the data to the pre-computed hash values. However it requires a large number of pre-computations 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 [73] outside of [82]. This is especially true for industrial size microgrids such as studied here. In [82] a survey of microgrid protocols, architectures, equipment and security threats is given. The authors propose 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.

Table 4: 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

4.3 SYSTEM AND ATTACK MODELS

We adopt the system scenario illustrated in Fig. 13. 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. 13, we consider a multicast communication scenario with a single sender S and multiple receivers $R_i, i = 1, 2, ...n$ (note - unicast and broadcast are special cases of multicast). Table 4 summarizes the notation we adopt for the system model.

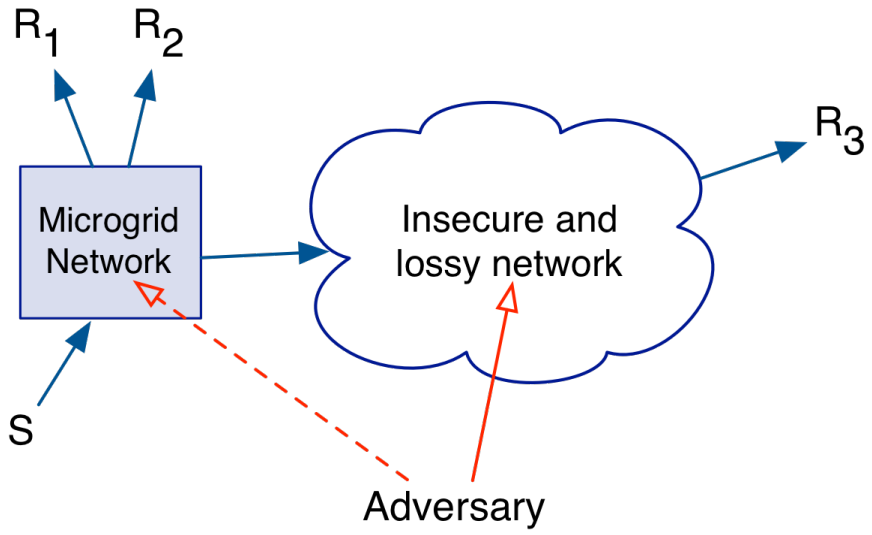

Figure 13: Network model.

In Fig. 14, 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 [83]. 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. 14, 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.

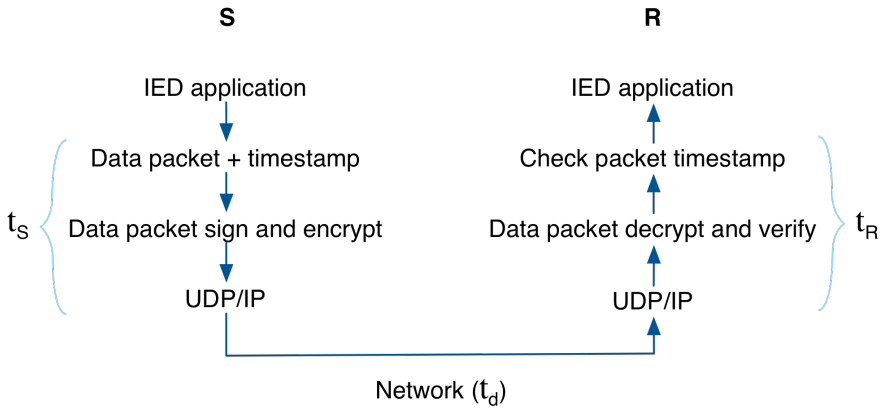

Figure 14: End to end communications model within microgrid

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 re-transmissions; (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; (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.

4.4 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.

4.4.1 Key Bootstrapping

For communication bootstrapping, the protocol adopts a modified version of the Needham-Schroeder protocol [84]. 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 AES key). At the time of installation, the technician enters the IED's bootstrap key into the microgrid's key management server. Once connected to the network, the IED_i sends a k_{b_i} encrypted join request to the microgrid's key management server KS. In response, KS send back the microgrid's shared confidentiality communication key k_c and the IED's individual confidentiality key k_{ks_i}. These steps are illustrated below.

$$IED_i \rightarrow KS : \{IED_i, N_i\}_{k_{b_i}} \tag{1}$$

$$KS \rightarrow IED_i : \{IED_i, N_i, k_c, k_{ks_i}\}_{k_{b_i}} \tag{2}$$

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}.

$$IED_i \rightarrow IED_j : \{IED_i\}_{k_c} \tag{3}$$

$$IED_j \rightarrow IED_i : \{IED_i, N'_j\}_{k_{ks_j}} \tag{4}$$

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.

$$IED_i \rightarrow KS : \{IED_i, IED_j, N_i, \{IED_i, N'_j\}_{k_{ks_j}}\}_{k_c} \tag{5}$$

$$KS \rightarrow IED_i : \{IED_j, N_i, v_{(i,j)}, \{IED_i, N'_j, v_{(i,j)}\}_{k_{ks_j}}\}_{k_{ks_i}} \tag{6}$$

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.

$$IED_i \rightarrow IED_j : \{\{IED_i, N'_j, v_{(i,j)}\}_{k_{ks_j}}\}_{k_c} \tag{7}$$

$$IED_j \rightarrow IED_i : \{N_j, \{N_j\}_{v_{(i,j)}}\}_{k_c} \tag{8}$$

$$IED_i \rightarrow IED_j : \{N_j - 1, \{N_j - 1\}_{v_{(i,j)}}\}_{k_c} \tag{9}$$

4.4.2 Communication

The communication protocol follows the principle of encrypt-then-MAC [85]. 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 communication in turn below.

Unicast Communications

Unicast communications is the normal mode for communications between $IEDs$ and the primary controllers.

$$IED_i \text{ encrypts the message with } k_c \tag{10}$$

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

$$IED_i \text{ creates individual authentication tag} \tag{11}$$

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

$$IED_i \rightarrow IED_j : [\{m\}_{k_c} || \{m\}_{(i,j)}] \tag{12}$$

$$IED_j \text{ creates digest from the received message} \tag{13}$$

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

$$IED_j \text{ compares the local and the received digest} \tag{14}$$

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

$$IED_j \text{ accepts the message} \tag{15}$$

$$\text{ELSE}$$

$$IED_j \text{ rejects the message}$$

$$\text{END}$$

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

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

END FOR

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

EACH R_i (19-21)

Same as unicast communication (13) - (15)

4.5 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).

4.5.1 Bootstrapping and Key size

The parameters used to calculate the performance are listed in Table 5 and are based on a 600 MHz microprocessor widely used in embedded systems such as power grid $IEDs$. We adopt the National Institute 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 CMAC algorithm for message authentication [86]. 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 [87]. 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 [88]. In order to achieve the NIST specified key lifetime security level, TV-HORS requires a key of at least 500 KBytes [81]. In the target offshore platform microgrid system each primary controller sends one message every 80 msec, or 13 messages/sec.

Following [81] one can show the minimal time to bootstrap the key for TV-HORS is 120 sec and the lifetime of the key is only 840 seconds. Thus, for every 14 minutes of operation each IED would have to pause sending data and bootstrap again the keys for 2 minutes. 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., stated similar findings in regards to using TV-HORS for substation communication security [89]. Hence, TV-HORS is not a practical security solution for the target microgrid environment.

4.5.2 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 6. The second column in Table 6 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 5: Security Algorithms time performance statistics. [2] Please note, that we assume SHA-256 performance to be on par with 192-AES. Due to the lack of SHA-256 performance statistic on the target platform we make this safe assumption.

OpenSSL performance statistics for VIA Eden 600Mhz	
Microgrid message payload (d_{msg}) [71]	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

Table 6: 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)

For the calculation of IED's 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. Towards minimizing the overhead, we make use of AES-CMAC-96 [90] 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 pre-configured number of SHA-256 messages digests per single authentication tag. For the data rates in question, the minimum feasible message digests per signature is eleven [79].

In the microgrid of Fig. 12, the communication network connects the following IEDs: 10 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 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 kbps) in comparison to the link bandwidths (.1-10 Gbps), we assume the communication network is congestion free and ignore any intermediate router/switch buffering delays.

4.5.2.1 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 $T_{pri-sec}$. This is illustrated in Fig. 15. 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 $n_{pri} \cdot t_R$ (where n_{pri} is the number of primary controllers in the microgrid). Hence, the controller loop latency $T_{pri-sec}$ is

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

Utilizing Table 5 and assuming 100 Mbps communication links, the one-hop propagation delay t_d is approximately equal to 0.05 ms. Further, taking values from the literature we set $t_{sec} = 500$ ms, $t_{conv} = 500$ ms [69] and $t_{pri} = 80$ ms [72]. For the proposed security

architecture, the resulting control loop delay is $T_{pri-sec} \approx 1080$ ms. By comparison, if RSA (PKI) is used the control loop delay is $T_{pri-sec} \approx 1805$ ms, which is just under the 2 sec latency threshold given in [91] to ensure stable operation of the microgrid's power network.

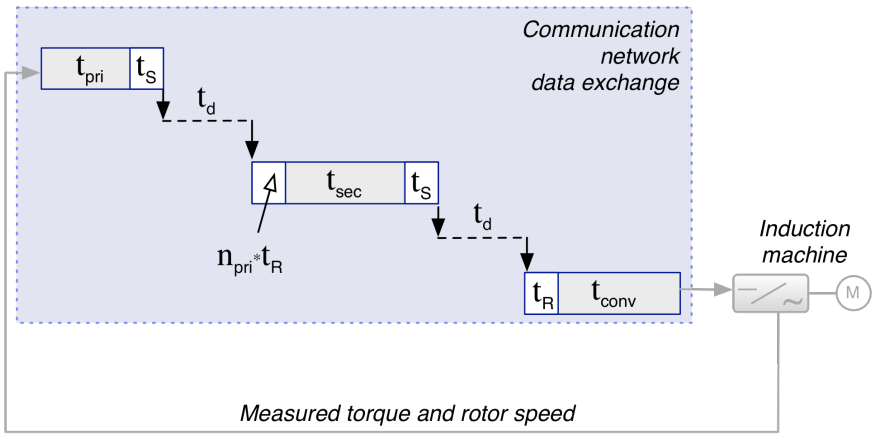

Figure 15: The microgrid's primary-secondary distributed control loop.

4.5.2.2 Tertiary-Secondary Control Loop

In a fashion similar to the above analysis, we evaluate the tertiary-secondary control loop delay $T_{ter-sec}$. The loop latency is expressed as

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

Assuming broadcast communications, with $t_{ter} = 500$ ms [72], the proposed protocol's delay is $T_{ter-sec} \approx 1580$ ms. However, if RSA is used instead, the loop delay is $T_{ter-sec} \approx 2144$ ms, which exceeds the stable operation threshold.

4.5.3 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 [70] 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 Mbps links. The interface between the two simulators was developed using a custom adaptive scheduler in the ADEVS framework [92]. 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 $IED's$ individual computation speed, execution cycle sub-routines and internal/external events, in order to determine the co-simulation synchronization points.

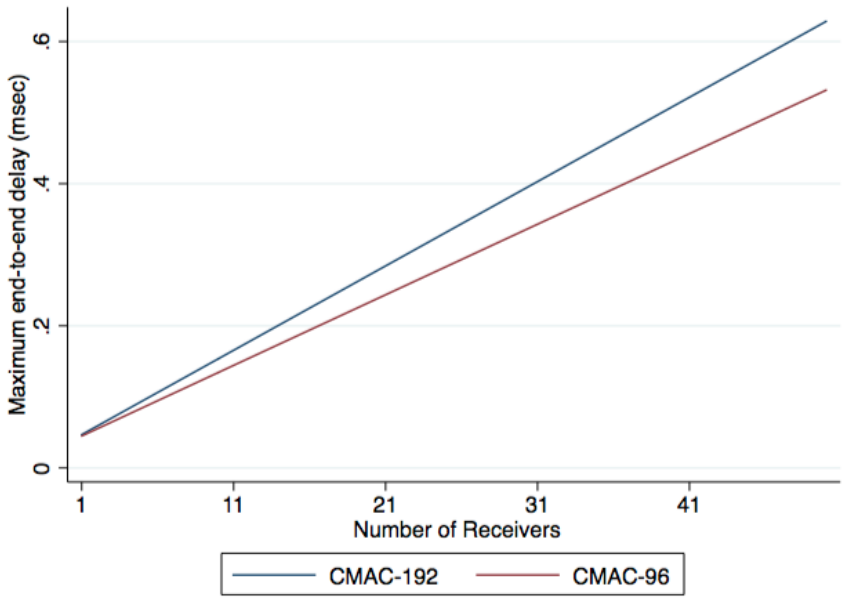

Figure 16: Maximum end-to-end delay vs. number of multicast receivers

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 second 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. 16 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 3ms target. Next we studied the primary-secondary control loop delay $T_{pri-sec}$ for the case of all of the IEDs active. The maximum observed $T_{pri-sec}$ over the set of simulation runs is given in Table 7. 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 $T_{pri-sec}$ 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.

Table 7: 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*

4.6 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.

5.0 MICROGRID CO-SIMULATION ARCHITECTURE

5.1 INTRODUCTION

Microgrids have been proposed as a method to incorporate distributed energy generation, such as, wind and solar [93] into the power grid, as well as, a means to provide continuity of power to key societal and commercial locations (e.g., hospitals, military bases, etc.). The required building blocks of microgrids are the presence of a local energy source, loads, and connectivity to the main grid. 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 re-synchronization with minimum impact to sensitive loads. All of these operations are complex and require synchronized operation of different intelligent electrical devices (IEDs) (e.g., voltage regulators, protective relays, etc.) through extensive communications.

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 which consist of distributed hierarchical control layers termed: primary, secondary and tertiary control [94]. 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 be-

tween 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 microgrid communications network must be modeled in a detailed realistic fashion when evaluating the microgrid power control and general operation.

However, most of the literature focuses on microgrid simulation from one perspective (either power system or communications), while significantly abstracting the other one [95]. For instance, it is a common practice in power system publications [96, 97] to consider a deterministic or random delay between the distributed controllers within a microgrid. Such abstracted delays however do not take into account the specific communication properties (e.g., queueing delay, packet loss), thus reducing the overall system fidelity and real world usefulness of the results.

In this paper, we propose a novel co-simulation architecture to evaluate the performance of microgrids in a high fidelity multidisciplinary fashion. We propose a dynamic time stepped scheduler built around the execution of IEDs within the microgrid to synchronize power system and communication network simulators. We illustrate our methodology using two off the self simulation packages: MATLAB and OMNeT++. The proposed approach ensures minimal simulation synchronization errors while still being computationally feasible.

The remainder of the paper is organized as follows. In Section 5.2, we present background material on existing smart grid co-simulation approaches. In Section 5.3, we describe an example microgrid, our IED model, and associated simulation challenges. Next, Section 5.4 provides an overview of our proposed co-simulation architecture and discusses in detail our novel dynamic scheduler. The co-simulation results are then provided in Section 5.5. Conclusions are finally drawn in Section 5.6.

5.2 RELATED WORK

Due to the lack of analytical tools and real world test beds for performance evaluation, computer based simulation is expected become the standard tool for microgrid evaluation in the forseeable future.

While a number of industry adopted mature power distribution simulators such as PSLF and PowerWorld exist, as well as, a wide variety of communication network simulation tools such as ns-3, ns-2 and OPNET, there is no holistic simulation environment that combines both. A typical approach used in the scientific community is to interconnect independent simulators in order to create a co-simulator. Usually, those efforts involve software packages written in different programming languages that lack common data exchange interfaces. To overcome this issue, researchers develop new middle layer software, often written in another programming language to interconnect independent simulators. This leads to significant performance degradation and limits the overall usefulness of the co-simulation environment. As a result, co-simulations do not scale well, and mostly focus on trivial test cases.

Moreover, there is a significant problem with the co-simulation event schedulers. Usually, two or more independent schedulers are used, one guiding the power network simulation, another executing the communication network, and a third one to interface both. A typical approach for the interface schedulers is to process events using a first-in first-out (FIFO) queue in both networks. Early versions of such event-driven co-simulations use fixed time steps to advance both simulators and execute all buffered events at once [98]. Example efforts are EPOCHS [99], VPNET [100], and PowerNet [101]. Such an approach is undesirable for simulations of involving real-time systems such as smart grids. In more recent efforts, GECO offers a more realistic representation by sequentially simulating all power and communication events via timestamps [102]. However, due to possible synchronization errors in the two independent scheduling internal clocks and small time scales involved (in msecs), we argue that such approaches are not precise enough to capture a given transient sequence of events.

5.3 MICROGRID MODELING

As an example to provide context we draw on our recent work [10, 11], which proposed a medium voltage DC microgrid system to supply power to a set of offshore production platforms. The loads on a 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, HVAC, etc.). The basic microgrid architecture at a platform is depicted in Fig. 17.

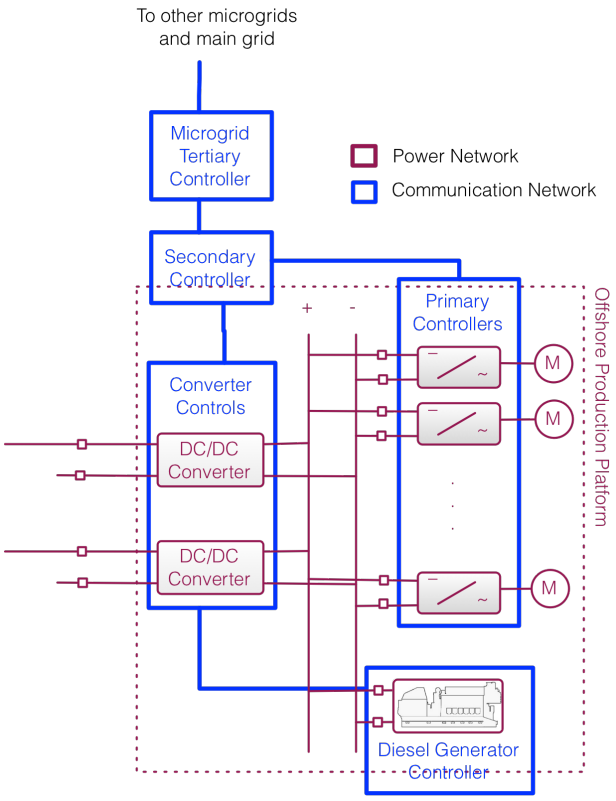

Figure 17: Power system and communication architecture for a given microgrid.

The main local source of electricity is provided by a group of 5 MW offshore wind-turbines that produce AC current. The AC from the wind-farm is converted to DC through a three-level neutral point clamped rectifier that establishes a 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 MW 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 uses a decoupled dq axis control to regulate both machine flux and current. The primary controllers provide measurements to the secondary controller, which controls the the DC/DC converters. The details of the control algorithms are given in [10]

In modeling a microgrid the typical approach is to use separate but linked simulators for the power and communication systems respectively. Often a fixed time step is used in both simulators and depending on the selected time-step size, synchronization errors can occur. To illustrate this, let us consider a simple example with two of the protection relays (IED_1 and IED_2) on either side of the DC/DC converter in Fig. 17. Consider a co-simulation where each simulator uses fixed time steps, noted ΔT (Fig. 18). In the event of a power surge at a motor in Fig. 17 both IEDs detect the transient. However, if IED_1 is the one next to the motor, it will trip instantaneously. After the protective action, IED_1 sends a message to inform IED_2 on the other side of the DC/DC convertor to not trip. As per power system operation, if IED_2 still detects harmonics on the line after a given delay and it has not yet received a trip notification from and IED on the other side of the convertor, it must independently execute protective actions. Thus if ΔT is greater than the execution cycle of both IEDs, the trip control message will not arrive on time at IED_2. An alternative approach is to decrease ΔT, however this leads to long simulation times, and therefore limits the possibility to study many real world scenarios. For this reason, the simulation environment needs to take into account the particular execution times of all IEDs in the simulation.

From a high level perspective, an IED execution cycle consists of five sub-states (Fig. 19): (i) read power network sensors, (ii) receive communication network packets, (iii) execute control logic, (iv) execute power network protective and corrective actions, and (v) send communication packets.

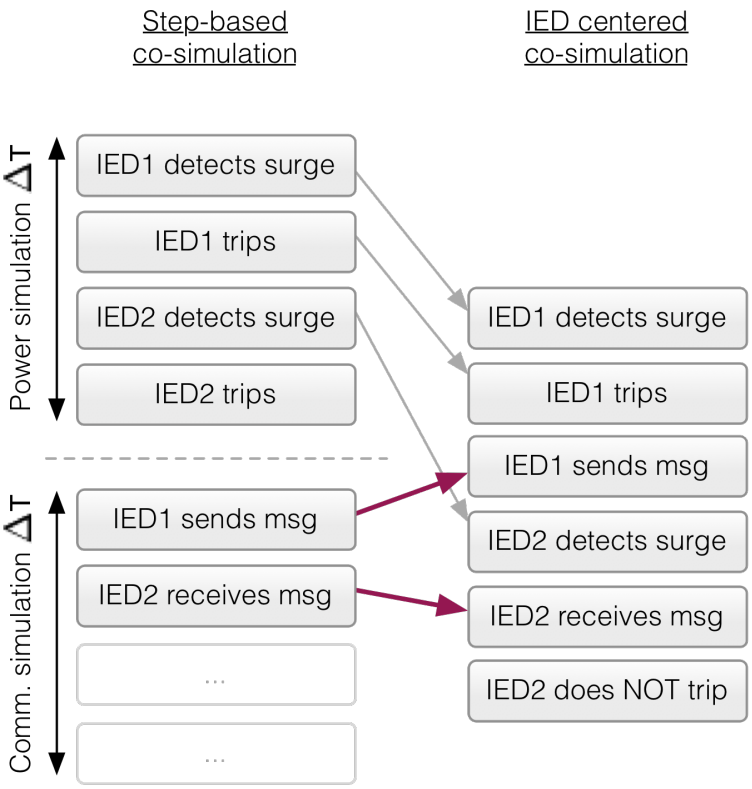

Figure 18: Comparison between step-based and IED centered co-simulations.

Reading sensor inputs and energizing outputs from and to the power network is in the order of microseconds and up to few milliseconds. An example of such operations is a brownout protection, in which the IED detects voltage sag and injects additional power onto the power bus. The power sensor reading delays are under a microseconds and, from a co-simulation point of view, those delays are negligible. The delays associated with the reading and writing data operations from the communications network can substantially take longer. The communications delay consists of the data encryption/decryption, authentication, packetization and depacketization, queuing, propagation, and transmission delays.

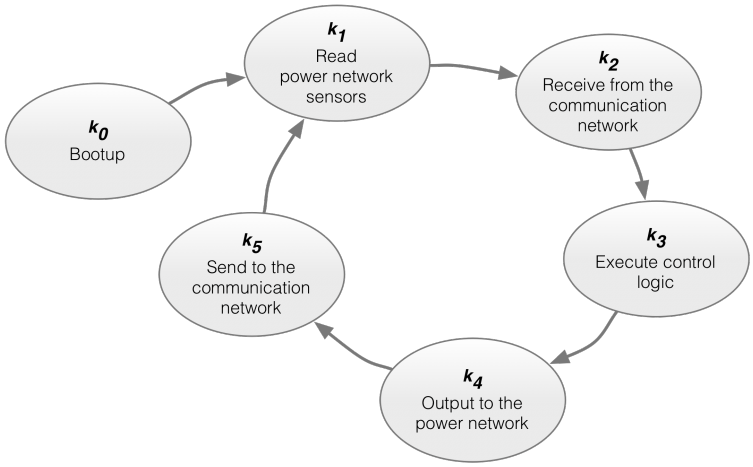

Figure 19: High level execution cycle of an IED.

5.4 PROPOSED CO-SIMULATION ARCHITECTURE

In order to evaluation both the microgrid and communications network, we propose a co-simulation architecture based on off-the-shelf simulators, namely OMNeT++ to model the telecommunications network and MATLAB for the power system (Fig. 20). OMNeT++ is an extensible component-based open source simulation framework. More specifically, it is an event-driven simulator supporting various application areas such as communications networks, queueing networks, and hardware architectures. In order to integrate both OMNeT++ and MATLAB, we use A Discrete EVent System simulator (Adevs).

5.4.1 Atomic Models

One significant property of the proposed co-simulation model is the use of Adevs atomic models. When a component is defined as atomic, an Adevs component is in charge of executing the models in sequence up to a given specified time. Each IED in the microgrid is defined by such a model with specific state transitions. A cycle sub-state is characterized

OMNeT++ homepage: http://www.omnetpp.org/.
Adevs homepage: http://web.ornl.gov/~1qn/adevs/.

by an execution duration and reading and writing interactions with the communications network. The sub-states are used to model the communications channels as well as the security mechanisms employed.

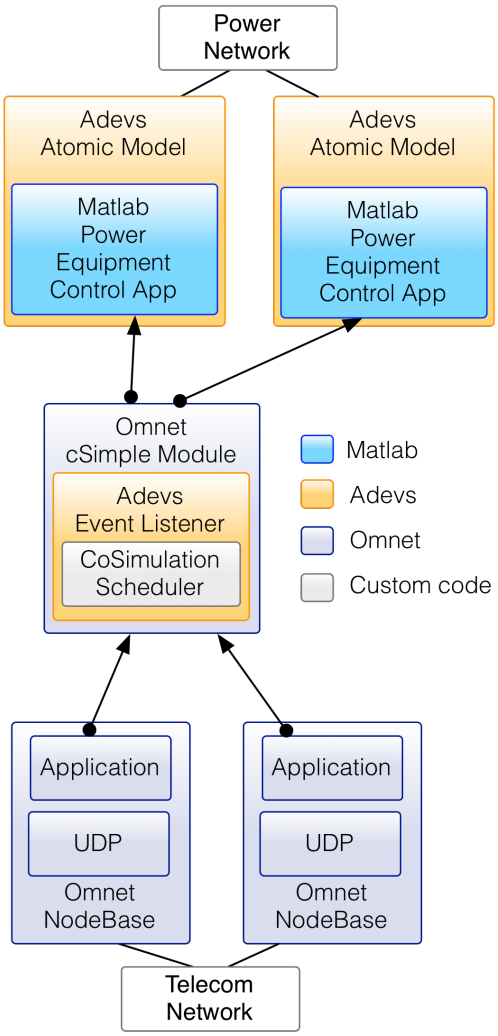

Figure 20: Proposed co-simulation architecture.

The power network, implemented in MATLAB, is also imported as a single Adevs atomic model. The investigated power network has the property of being nonlinear with respect to the inputs and outputs. The nonlinearity comes from the fact that the power voltage and current magnitudes changes as it travels through the transmission lines. Therefore,

it is not possible to split the power network into multiple models with input and output connections between them. Instead, the entire network is kept as a single model with input and output channels. The MATLAB simulation is decomposed with fixed time steps, and the co-simulator is in charge of setting inputs and reading outputs at every MATLAB cycle. The order and the timing of reading and setting of the power network interfaces follow the timing definition of each IED.

5.4.2 Co-Simulation Scheduler

There are two algorithms options for synchronization of both simulators and those are discussed in the following.

5.4.2.1 Fixed Time-Stepped Scheduler In order to compare the proposed dynamic scheduler described shortly, we consider a conventional time-stepped scheduler. As depicted in Fig. 18 (left side), such an approach decomposes the simulation time frame of both simulators into time slots with duration ΔT. During a given time slot, no interaction is done between both simulators. When a given time slot ends, the simulators can interact each other. Therefore, if an event from a certain simulator during a time slot requires an interaction with the other simulator, it is processed at the end of the time slot, thus creating a synchronization error. To mitigate such errors, ΔT can be reduced, however the computation complexity of the overall co-simulation increases.

5.4.2.2 Dynamic Time-Stepped Scheduler The co-simulation scheduler we propose is in charge of the adaptive synchronization between both networks. The power network has a fixed time step of ΔT_p. The communications network, however, is event-driven and the time step is defined dynamically as $\Delta T_C = t_{sync} - t_{current}$. An IED has two possible interactions with the communications network: (i) send a packet and (ii) receive a packet. First, when the simulation starts, the co-simulation scheduler finds the time of the upcoming network event of any IED. We formally define t_{sync} as the closest time to the current simulation clock time, $t_{current}$, that one of the following actions occur at any IED: (i) finish

the communications network writing operation and (*ii*) start the communications network reading operation. Note that the writing operation has a fixed time delay and the reading process has a variable delay, that depends on the number of received packets. Within the microgrid, all communications are machine-to-machine (M2M). Therefore, the recipients of the multicast messages are known in advance, and the packetization delay is also known. On the contrary, the delay to read packets from the communications network is unknown. Note that the delay is variable due to, in particular, the queuing delays and transmission losses.

Table 8: Symbol definitions of the dynamic co-simulation scheduler.

Symbol	**Definition**
$s_{(n,k)}$	The k-th sub-cycle state of the n-th IED.
A	Set of all ADEVS atomic models, $A = \{IED_1, IED_2, ...IED_n, P\}$. P is the atomic model of the power network.
currentState(.)	Method returning the current cycle sub-state index of an IED.
startT(.), *endT(.)*	Methods returning the start and end times of a given cycle sub-state.
writes(.), *reads(.)*	Methods returning true or false if a sub-state is reading or writing to the network.
interacts(.)	Method that returns true is the sub-cycle state interacts with the network or false otherwise.

Let us consider a co-simulation scenario involving two IEDs (IED_1 and IED_2), as depicted in Fig. 21. We assume that IED_1 is a low-level open loop controller with short control application sub-cycles. Also, IED_1 does not receive any data from the communications network, but instead at the beginning of its cycle the device interrogates a power network sensor.

Once the control logic is finished power network outputs are energized and a control packet is sent via the communications network. Let us assume also that IED_2 is a slow controller and uses inputs from IED_1. In this example (Fig. 21), the simulation starts at t_0 with the boot-up of the devices. The co-simulation scheduler then determines the next time t_2 at which an IED interacts with the network, corresponding to the time when IED_2 starts its initial network reading procedure. The next synchronization point t_{sync} is set and the communications network simulation is allowed to proceed. Once the communications simulator reaches t_2, it stops executing and hands over the control to the co-simulator scheduler.

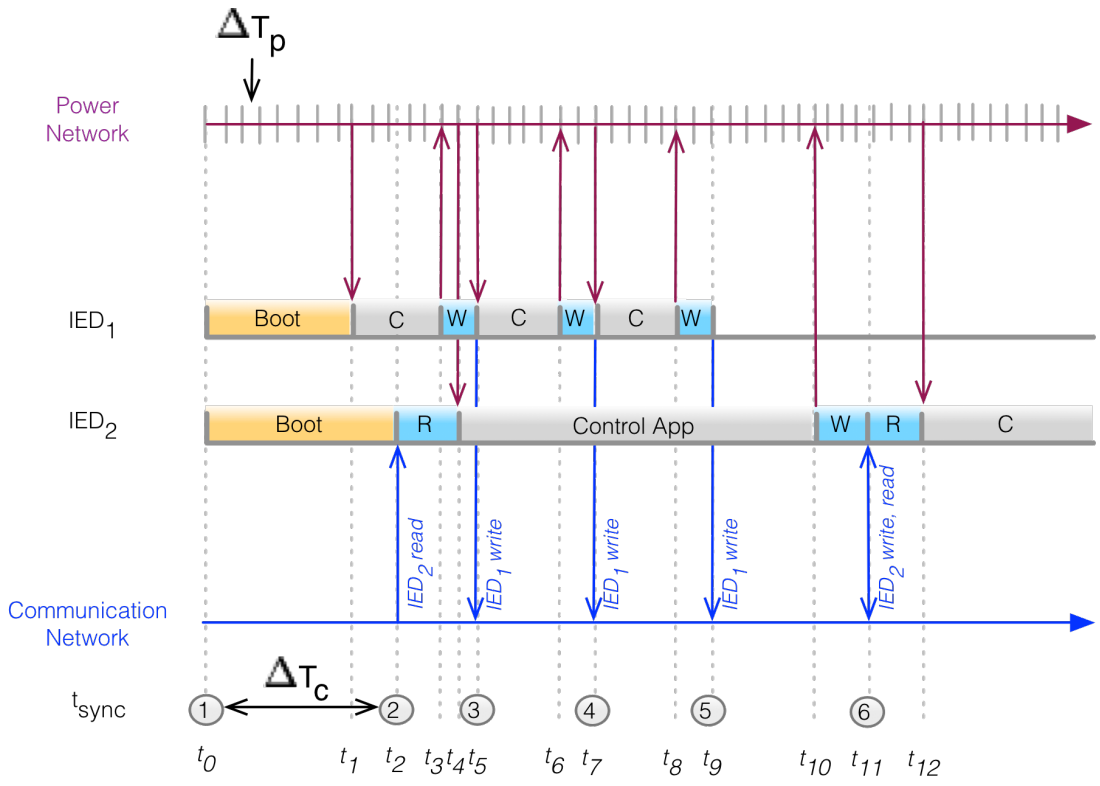

Figure 21: Co-simulation synchronization interrupts (R: read, W: write, C: control application).

The co-simulator scheduler executes 8 cycles from the power simulator until t_1, at which point it passes the inputs from the power network to the control application of IED_1. An-

other 3 cycles of the power simulation are executed until the power simulator reaches simulation time t_2. Next, the co-simulation scheduler informs IED_2 to check its network input queue. It then calculates the packet processing duration required by IED_2. This transmission duration depends on the number of received packets, confidentiality and authentication protocols employed, and processing power of the device.

Algorithm 1 Co-simulation scheduler algorithm.

1: Set next $m_{t_{sync}}$ for $t = 0$
2: **if** m_t is a received message addressed to IED at time t **then**
3: Put m_t into the appropriate IED network input queue
4: **else if** m_t is a $m_{t_{sync}}$ message **then**
5: $t_{sync} \leftarrow t$
6: **for** $\forall x \in A$ **do**
7: $k \leftarrow$ *currentState(x)*
8: **while** $endT(s_{(x,k)}) \leq t$ **do**
9: Execute state $s_{(x,k)}$
10: $k++$
11: **end while**
12: $currentState(x) \leftarrow k$
13: **do**
14: **if** $writes(s_{(x,k)}) \wedge endT(s_{(x,k)}) \leq t_{sync}$ **then**
15: $t_{sync} \leftarrow endT(s_{(x,k)})$
16: **else if** $reads(s_{(x,k)}) \wedge startT(s_{(x,k)}) \leq t_{sync}$ **then**
17: $t_{sync} \leftarrow startT(s_{(x,k)})$
18: **end if**
19: $k++$
20: **while** $interacts(s_{(x,k)})$
21: **end for**
22: Set next $m_{t_{sync}}$ for t_{sync}
23: *Go to line 2.*
24: **end if**

Once the co-simulation scheduler knows the current time states of all network devices, it schedules the next synchronization point t_{sync}. In the discussed example, that point equals to t_5, the time when IED_1 finishes its network write state. Once again, the communications simulator executes until t_{sync}, and hands over the execution to the co-simulator, which in turn executes the IEDs and power network. Due to the fact that IED_1 has a much shorter execution cycle, multiple packets can be sent before IED_2 receives any.

In real-time control networks, this is done to achieve the required transmission reliability, since a retransmission of a given packet is not allowed to avoid transmitting outdated information. In the example, the first time IED_2 sends a packet via the communications

network is at simulation time t_{11}, and the first time the IED_2 receives a packet from IED_1 is at simulation time t_{12}. Since synchronization is done at the end of the writing process and at the beginning of reading operation, only one t_{sync} is required at t_{11}. The co-simulation scheduler algorithm is presented in Algorithm 1.

5.5 CO-SIMULATION RESULTS

In this section, we present the co-simulation results in regards to the synchronization error between both OMNeT++ and MATLAB simulators. By minimizing the synchronization delay errors, we show that it is possible to simulate a more realistic representation of the real-world microgrid system effectively.

The primary controller at each motor provides torque and rotor speed measurements to the secondary controller at a regular interval. The secondary controller collects the measured data and 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, and the adjustment of the power supplied by the DC/DC converters constitutes the primary and secondary control communications loop delay (Fig. 22). Note that the primary controllers and the two DC/DC converters execute in parallel. However, the secondary controllers have to process the incoming data from the primary controllers before operating with an additional delay of $N_{pri} \cdot t_r$ (where N_{pri} is the number of primary controllers and t_r is the multicast packet depacketization delay).

Additionally, we have $t_{pri} = 0.08$, $t_{sec} = 0.5$, and $t_{conv} = 0.08$, which correspond to the primary controller, secondary controller, and DC/DC converter application cycle time, respectively. For each multicast message there is a packetization delay defined as t_s. In the simulation scenarios, we assume 100 Mbps link capacity and a microgrid architecture consisting of three primary controllers, one secondary controller, two DC/DC converters. Further, the maximum multicast packet size corresponds to 336 bits. For more details on the configuration, please refer to [11]. Please note, that the theoretical analysis ignores any

intermediate communication devices processing delays. The controller loop latency $T_{cntrl-loop}$ corresponds to 660 ms, and is appropriated as following

$$T_{cntrl-loop} = t_{pri} + t_{sec} + t_{conv} + 2 \cdot t_s + 2 \cdot t_d + (N_{pri} + 1) \cdot t_r, \tag{5.1}$$

For the simulation evaluation, the OMNeT++ network environment is consistent with the theoretical analysis - 100 Mbps links, application data on top of IP/UDP, multicast communication for all data, and all the distributed controllers are connected to a single router. The control loop delay is measured for every control cycle; i.e. every duty cycle command sent by the secondary controller to the two DC/DC converters. Table 12 presents the measured control loop delays corresponding to the different co-simulation synchronization methods.

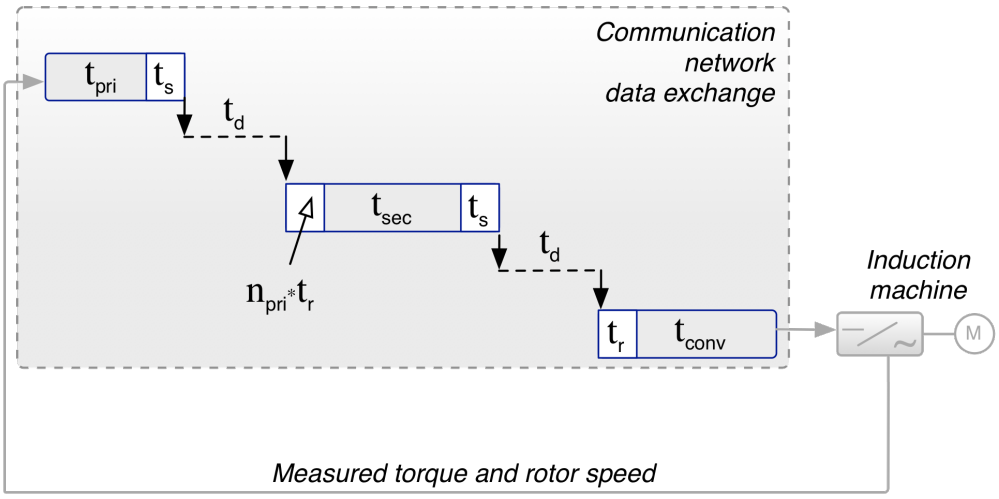

Figure 22: Primary-secondary controller distributed control loop.

For each synchronization option, we executed ten times a five second microgrid cold-start scenario - the procedure of starting all induction machines from an off state. At the beginning, each of the induction machine starts at 1 second interval and creates harmonics on the microgrid DC power exchange bus. After receiving torque and rotor speed values from the primary controllers, the secondary controller sends duty cycle commands to the two DC/DC

converters in order to compensate for the disturbance and stabilize the power bus voltage levels. In addition, each IED has a random boot-up delay between 5 and 10ms in order to represent a realistic environment in which the controllers are not fully synchronized. This is the reason for the standard deviation of the control loop delay between the scenario re-runs ($\overline{\sigma}_{cntrl-loop}$). When using the dynamic synchronization approach, the mean control loop delay ($\overline{D}_{cntrl-loop}$) is the same as when using a fixed step of 0.0005s. The 5μs step corresponds to the fixed step of the MATLABâĂŹs simulation of the power network. However, while using ΔT consistent with MATLAB may not introduce an additional delay in the control loop (row two of Table 12) the mean execution time for each scenario is significantly higher 372 seconds (using 2.7 GHz i7 with 16 GB RAM). In terms of execution speed, selecting one seconds synchronization step results in the fastest scenario run; however this setting results in 1145ms mean control loop delay, thus leading to severe performance degradation of the power control operations. Finally, the mean synchronization error ($\overline{E}_{sync}$) is on close to half ΔT, meaning that packets arriving at the destination controller, have to wait on average half a synchronization step before being passed to the controllerâĂŹs application.

Table 9: Co-simulation results: Comparison of the proposed dynamic co-simulation scheduler vs. a conventional time-stepped synchronization mechanism.

ΔT **(sec)**	$\overline{D}_{cntrl-loop}$ **(ms)**	$\overline{E}_{sync}$ **(ms)**	$\overline{\sigma}_{cntrl-loop}$ **(ms)**	**Sim. duration (sec.)**
Dynamic	666.8	0	49.9	76
0.00005	666.8	0.000025	45	372
0.001	695	0.0006	53.1	86
0.01	745	0.009	42.4	80
0.1	738	0.09	5.6	75
1	1145	0.87	39.3	68

5.6 CONCLUSIONS

To accurately capture the overall operation of the discussed microgrid, we proposed a co-simulation model driven by embedded power controllers. Further, we proposed a novel co-simulation scheduler taking into account events from both the power and communication network simulators, as well as the timing of each embedded controller execution loop to adaptively synchronize both simulators efficiently. The proposed approach ensures minimal synchronization error while still providing the ability to simulate extended operational scenarios. The numerical results illustrate that the proposed dynamic synchronization scheduler outperforms the considered conventional time-stepped synchronization mechanism in terms of synchronization error, while significantly decreasing the computation complexity in terms of simulation duration.

6.0 EFFECTS OF COMMUNICATIONS DELAY ON DISTRIBUTED MICROGRID CONTROL

6.1 INTRODUCTION

Abetter understanding of onshore wind behavior has been the attention of many engineers in the last several years. The Department of Energy (DOE), through FOA-414, has found great interest in exploring the integration of offshore wind and has funded a team of organizations to explore the wind speed behaviors at sea and determine the optimal location for placing large wind turbines on the coasts of the United States. Not only is optimal wind turbine placement important, but investigating ways of integrating the power into the grid are being considered [103]. Drilling rigs and offshore oil platforms rely heavily on AC variable frequency drives (VFD) for applications such as propulsion, station keeping, drilling, and pumping product to the surface. In drilling rigs, drill-ships, and offshore production platforms, the non-linear variable speed drive load makes up 85% of the installed kW. The typical installed drive power for a drilling package is 5,000-12,000 HP (3.7 to 9 MW) [104]. Drilling rigs and oil platforms are placing considerable harmonic strain on generators and degrading the quality of the voltage supplies. As stated in [104], the power quality is degraded due to harmonic currents produced during the conversion from AC to DC for variable frequency drives. Today domestic offshore oil drilling takes place in the Gulf of Mexico and Northern Alaska, as shown in Fig. 23. The eastern seaboards, from North Carolina through Maine, are locations with the greatest potential for offshore oil and gas drilling. Early results from the FOA-414 DOE study are shown in Fig. 24. Comparing Fig. 1 with Fig. 2, one will note a strong overlap between high wind penetration and oil drilling areas approved by the United States government. The medium voltage DC architecture [5] has often been referred to as a type of

microgrid upon first view. The microgrid concept was first proposed in 2002 as a better way to implement the emerging potential of distributed generation. During disturbances, the generation and corresponding loads can separate from the disturbed grid, maintain service, and not harm the overall gridâĂŹs integrity [105]. As pointed out by [106], the difficult task is to achieve the microgrid functionality without extensive custom engineering and still have high system reliability and generation placement flexibility.

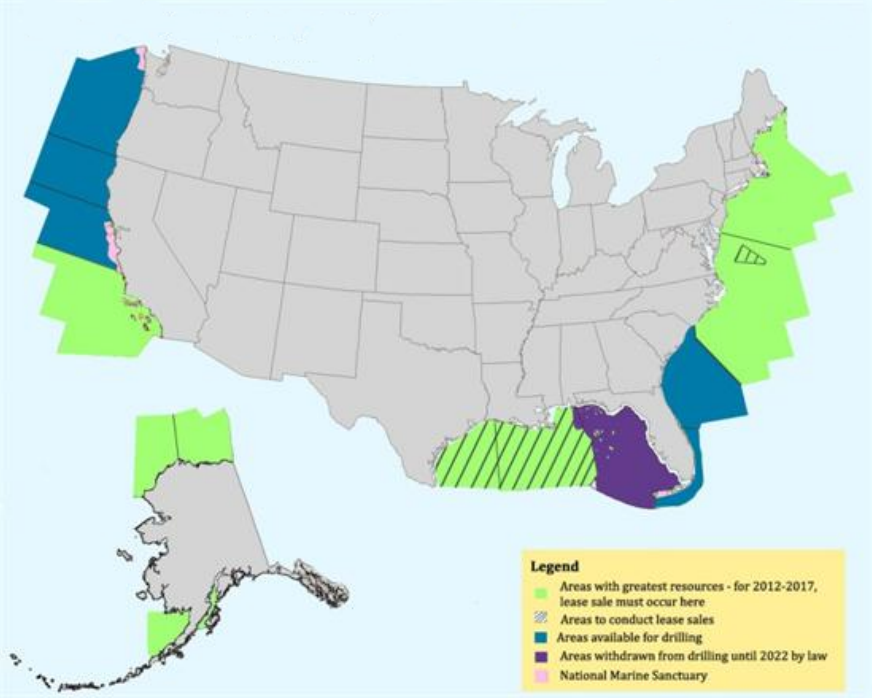

Figure 23: Oil drilling opportunities between 2012 and 2017 [5].

The fundamental microgrid requirements include the capability of operating in islanding and/or on-grid modes with high stability, mode switching with minimum load disruption and shedding during transitions, and after a transition, stabilize in a certain amount of time. The high-level technical challenges associated with microgrids include (1) operation modes and transitions that comply with IEEE 1547 (Standard for Interconnecting Distributed Resources

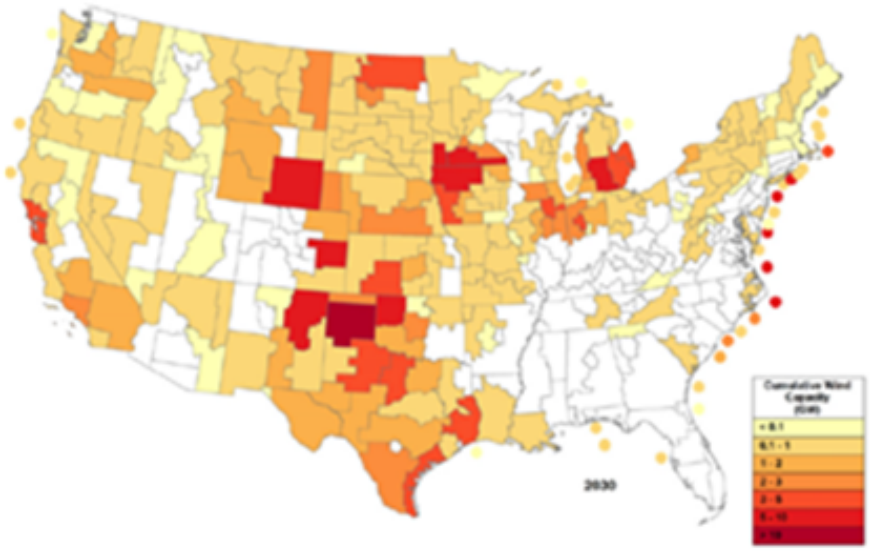

Figure 24: Planned location of offshore wind turbines [6].

with Electric Power Systems) and (2) control architecture and communication. For the case of an AC based microgrid, the following items are considered by various research teams:

Islanding mode: frequency and voltage stability, optimal power flow;

- Grid to islanding mode: transition and stabilization, minimum load shedding and disruption;
- Islanding to grid mode: re-synchronization and re-connection, minimum impact on sensitive loads and electronics as transients evolve during state transitions.

Coupling offshore renewable energy expansion, variable frequency drive based platforms, and the microgrid theme, a proposed system architecture is provided in Fig. 25 utilizing a DC backbone. The directions that many manufacturers of power system equipment are exploring with offshore technologies to harness and transmit electric power provide further encouragement that the proposed research efforts/system architecture is viable [107].

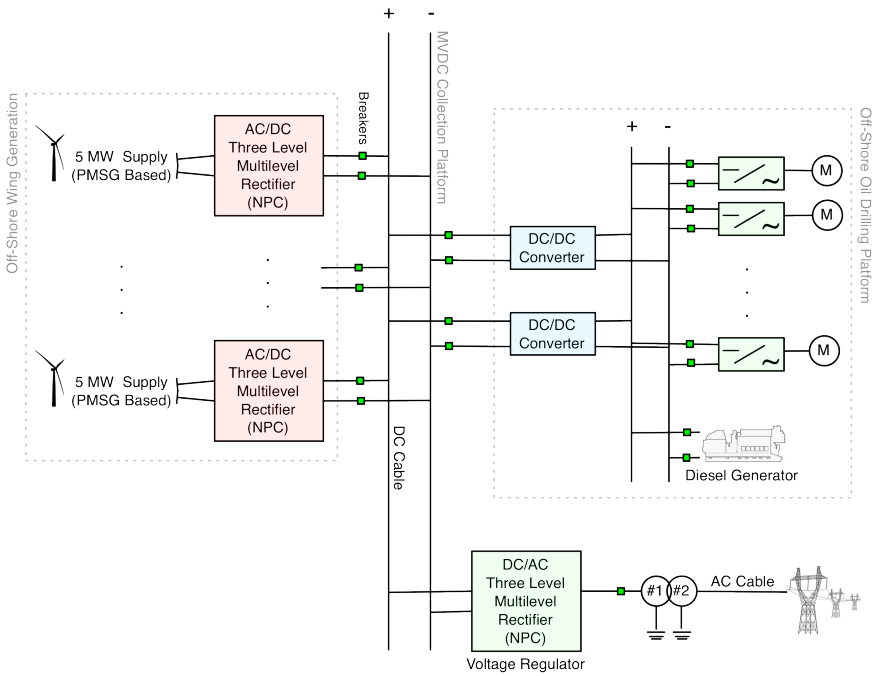

Figure 25: Local offshore wind power supplying power to offshore production platform [5].

6.1.1 Challenges to the Communication Network

Microgrids require fast, secure, and reliable communication means to operate and coexist. Under normal operations, the communications allows microgrids to synchronize with the main grid prior to connecting, thus extending equipment lifetime and minimizing transient periods in the electrical network. In emergencies, signaling would ensure that the power exchange would be disengaged prior to power equipment's detection of abnormal levels of voltage or frequency, thereby avoiding any potential damage.

In order to achieve these goals, the three main requirements of the communication system are: (*i*) real-time performance guarantees, evaluated via worst case delay performance analysis, (*ii*) security, providing tempering and confidentiality guarantees while respecting the real-time boundaries, and (*iii*) extremely high availability, needed to ensure non-interrupted services. All of those requirements are challenging due to the mere fact that both power and communication subsystems are electrical networks. The first, the power, is an analog

electrical system, while the second, the communication, is a digital electrical system. Even in the presence of optical fibre communication links, most of the delays in the communication network would be introduced by the embedded control sub-systems that govern the flow of control messages and the execution of control logic. These systems are digital electrical machines that have interfaces to both the power and communication networks. On a per cycle manner, the devices query the power network sensors, execute control logic, and, if required, take appropriate corrective actions. At the end of a given cycle, each device sends packets via the communication network that carries periodic data and control notifications. Therefore, it is of importance for the node receiver that the message arrives prior to the power network state modification. Since both networks consist of electrical devices, the challenge to the communication network could be viewed as electricity chasing electricity. The time unit of the packetized control signals traveling within the communication network is on the order of milliseconds (msecs) [7]. Also, some of the control and measurement messages are broadcasted or multicasted in nature, resulting in the generation of multiple packets for a single event notification. However, an electrical phenomenon in the power network lasts under tens of msecs. End-to-end packet delay can be close to the upper boundary of the power transient.

Fig. 26 summarizes the different time-scales in the power and communication networks. The time unit of the packetized control signals traveling within the communication network is on the order of msecs.

In this article, we present the control algorithm design for stable microgrid power operations. In addition, we present the distribute system architecture and the communications network that is designed to facilitate the secure message exchange. Finally, we present co-simulation effect and qualify the effect of communication and sub-system delay onto the microgrid's power network stability.

This paper is organized as follows: Section II provides an overview of related work in the fields of power control algorithms and microgrid communication studies. Section III presents the mathematical framework for the design of the controllers. Section IV builds onto the mathematical foundation and presents the distributed system architecture. The co-simulation validation tool and simulation results are presented in Section V. Finally, we

draw our conclusions in Section VI.

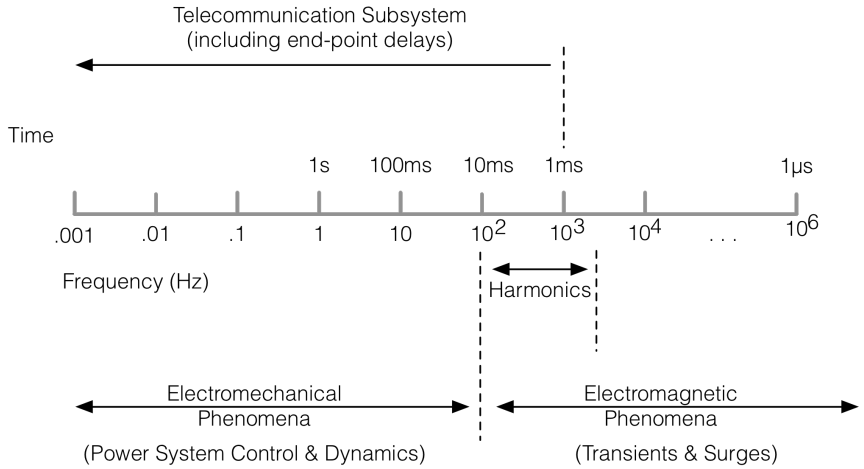

Figure 26: Power vs. Telecommunication subsystems timescale [7].

6.2 RELATED WORK

In commercial or residential buildings, the use of DC distribution architectures is proposed in literature to increase efficiency by allowing the use of larger and more efficient centralized distribution rectification stages rather than individual point-of-load rectifiers for the loads requiring DC [108–110]. Other proposed applications for DC architectures are for microgrid applications to more efficiently integrate energy storage and distributed renewable generation that produce DC voltage, such as in suggested cellular communication microgrids [111,112]. However, most of the research conducted so far has concentrated on AC microgrid design [113]. The DC microgrid has a similar network structure compared to a single phase AC microgrid. The fundamental differences include the existence of a frequency component and reactive power flow control is not necessary in a DC system. Power flow is controlled by voltage droops in AC [114–117] and DC systems [118].

Only a few works conceived the microgrid as a whole problem taking into account the different control levels. In the literature, [119] and [120] provide exceptional overviews of the three control layers within microgrids - primary control, secondary control, and tertiary control. The primary control - droop control discussed earlier - is often used to emulate physical behaviors to make the system stable and more damped. The primary control maintains voltage and frequency stability of the microgrid prior to islanding. The secondary control ensures that the electrical signals through the microgrid are within the required values compensating voltage and frequency deviations toward zero when necessary caused by the operation of the primary controls. Finally, the tertiary layer controls the power flow between the microgrid and main grid. Currently there is little microgrid specific communications research [121] outside of [122]. This is especially true for industrial size microgrids such as studied here. In [122] a survey of microgrid protocols, architectures, equipment and security threats is given. The authors propose 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 intelligent electrical devices ($IEDs$) and the distributed hierarchical nature of the microgrid control systems are not addressed. An in-depth analysis of microgrid distributed controllers and options for the communications network are presented in [123]. As far as the communication network is concerned, the authors' main focus is on the bandwidth of the communication link and the size of message packets. Here, we note that the $IEDs$ are the bottleneck of the electrical and communications co-system and as such we analyze the limits end-device computation at the expense of communication overhead.

6.3 MATHEMATICAL FRAMEWORK OF POWER SYSTEM ARCHITECTURE

The simplified power system architecture under investigation for this study is found in Fig. 27. The model is composed of one, 5MW wind turbine system (permanent magnet syn-

chronous generator and rectifier), two bidirectional DC/DC converters, and motor drive units rated for 1.67 MW each. The purpose of this section is to provide the mathematical framework of all the electrical models and control structures associated with the power converters and electric machines.

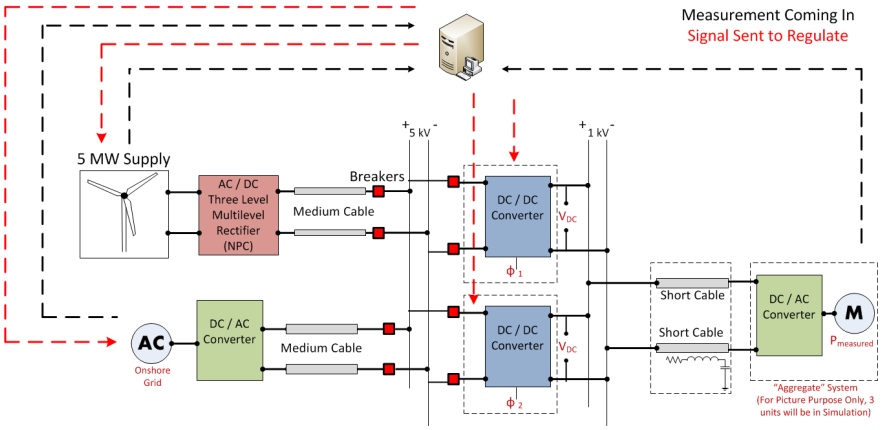

Figure 27: System architecture for power and communication evaluation.

6.3.0.1 Wind Turbine Modeling The wind collection system that was modeled within the Matlab/Simulink environment is composed of 1 wind turbine which will be represented by an aerodynamic model, permanent magnet synchronous generator (PMSG), and a three-level neutral point clamped rectifier that generates the required DC bus voltage. The parameters associated with the machine and wind turbine characteristics are provided in [124]. A standard set of electrical equations, with respect to the dq rotor reference frame, describing the permanent magnet synchronous machine are listed as (1) with output torque listed as (2). Note that Ls is the stator leakage inductance, Îżm is the permanent magnet flux of constant magnitude, ĬĽ is the rotor speed, P is the number of pole pairs, F is a friction factor, and J the moment of inertia of the machine [125]. The machine model described by (1) and (2) assumes that saturation is neglected, induced emfâĂŹs are sinusoidal, the Eddy currents and hysteresis losses are negligible, and there are no field current dynamics. Finally, the

mechanical equation, based on NewtonâĂŹs second law, of the machine is listed as (3).

$$V_d = R_s i_d + L_s \frac{di_d}{dt} - \omega_r L_s i_q \tag{1a}$$

$$V_q = R_s i_q + L_s \frac{di_q}{dt} + \omega_r L_s i_d + + \omega_r \lambda_m \tag{1b}$$

$$T_{em} = \frac{3}{2}\frac{P}{2}(\lambda_m i_q + (L_{ds} - L_{qs})_s i_q) \tag{2}$$

$$T_e - T_m - F\omega_r = J\frac{d\omega_r}{dt} \tag{3}$$

According to [126], the optimal torque reference can be obtained using (4) through (6). Note that Îżopt is the optimal tip speed ratio, Cp is the constant power coefficient, A is the area swept by the turbine, R is the blade radius, and Îš is the blade pitch.

$$T_{ref} = K\omega_r^2 \tag{4}$$

$$K = \frac{1}{2}\rho A R^3 \frac{C_{p \cdot max}}{\lambda_{opt}^3} \tag{5}$$

$$C_{p,max} = C_p(\beta|_{\beta=0}, \lambda_{opt}) \tag{6}$$

Three-phase power systems are conveniently modeled and controlled in the dq coordinate system. For maximum torque control applications, itâĂŹs always desired to drive the d-axis current to zero and maximize the q-axis current capability as indicated in (2). Hence establishing the q-axis current reference based on the maximum torque determined with (4) to (6) is logical for extracting maximum power. The wind turbine controller is shown in Fig. 28.

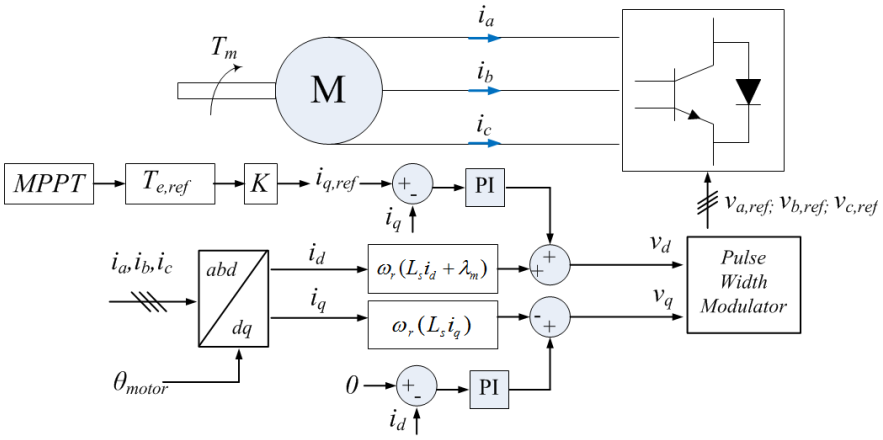

Figure 28: Maximum Power Point Tracking Implementation and Control of Wind Turbine.

6.3.0.2 Wind Turbine Modeling The half-bridge converter is a basic building block for the multilevel neutral point clamped converter. The neutral point clamped converter is utilized to interface the wind turbine to the medium voltage DC bus bar. The average model of the half-bridge converter is adequately discussed in [127]. Using the terminal voltage of the converter described by (7) and noting the power balance relationship written as (8) that relates the AC and DC sides, Fig. 29 provides the average circuit model of the neutral point clamped converter. The modulation index, shown in red, is dynamic whose value is adjusted by the control system.

$$\overline{V}_t = m\frac{V_{DC}}{2} \tag{7}$$

$$i_{dc}V_{dc} = v_{ta}i_a + v_{tb}i_b + v_{tc}i_c \tag{8}$$

6.3.0.3 Grid Connected Average Rectifier Model The average model of the pulse width modulated rectifier can be shown to be (9) and (10) with definitions listed as (11). For further reading on the subject, consider [128]. The approach to regulate real and reactive

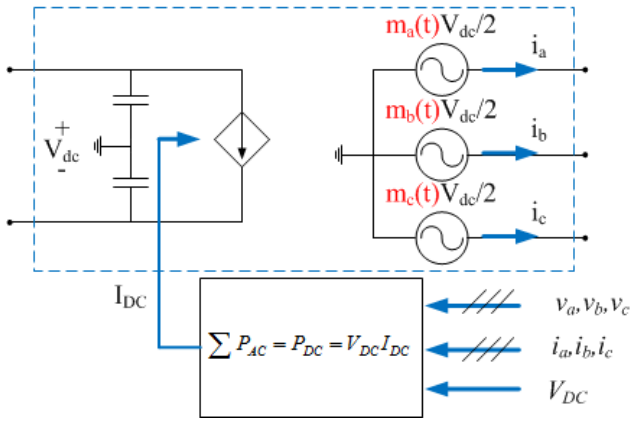

Figure 29: Average Model of Neutral Point Clamped Converter.

power through the power converter is provided in Fig.30. This converter serves as the main interfacing entity between the grid and 5 kV medium voltage bus.

$$\frac{d_{i_{II}}}{dt} = \frac{1}{3L} v_{LL} - \frac{1}{3L} \cdot d_{LL} \overline{v}_{dc} \tag{9}$$

$$\frac{d\overline{v}_{dc}}{dt} = \frac{1}{C} d_{ll} \cdot i_{LL} - \frac{v_{dc}}{RC} \tag{10}$$

$$v_{LL} = \begin{bmatrix} v_{AB} \\ v_{BC} \\ v_{CA} \end{bmatrix} \; v_{ll} = \begin{bmatrix} v_{ab} \\ v_{bc} \\ v_{ca} \end{bmatrix} \; i_{ll} = \begin{bmatrix} i_{ab} \\ i_{bc} \\ i_{ca} \end{bmatrix} \; d_{ll} = \begin{bmatrix} d_{ab} \\ d_{bc} \\ d_{ca} \end{bmatrix} \tag{10}$$

6.3.0.4 Grid Connected Average Rectifier Model The dual active bridge DC/DC converter was first proposed in [129]. The converter topology has grown in popularity as demand in bidirectional power flow capability has increased in research pursuits such as battery charger applications for electric vehicles. Research teams have devised new control techniques for improving system efficiencies [130] and using state of the art semiconductor

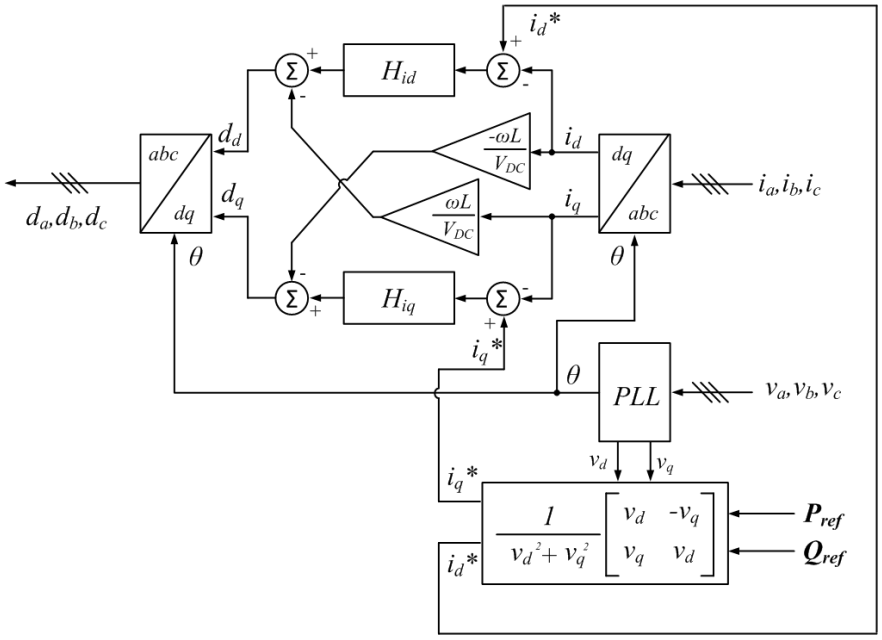

Figure 30: Open Loop PQ Regulator of Pulse Width Modulated Boost Rectifier.

devices for high frequency operation of the topology [131]. Research efforts have been primarily centered upon low power applications. In this work, we utilize the dual active bridge as an interface between two medium voltage (kV) DC busses. The most notable characteristic is the phase delay, ÏŢ, between both full bridges, which controls the allowable power flow in the circuit. The relationship between the phase delay and duty cycle, dh, is described by (14).

$$\phi = \frac{d_h T_s}{2} \tag{12}$$

where T_s is the switching period. The average inductor current can be described by (15).

$$I_{avg} = \frac{nV_{DC}T_s}{2L_T} d_k(1 - d_k) \tag{13}$$

where VDC is the input voltage, LT the transformer leakage inductor, and n the turns

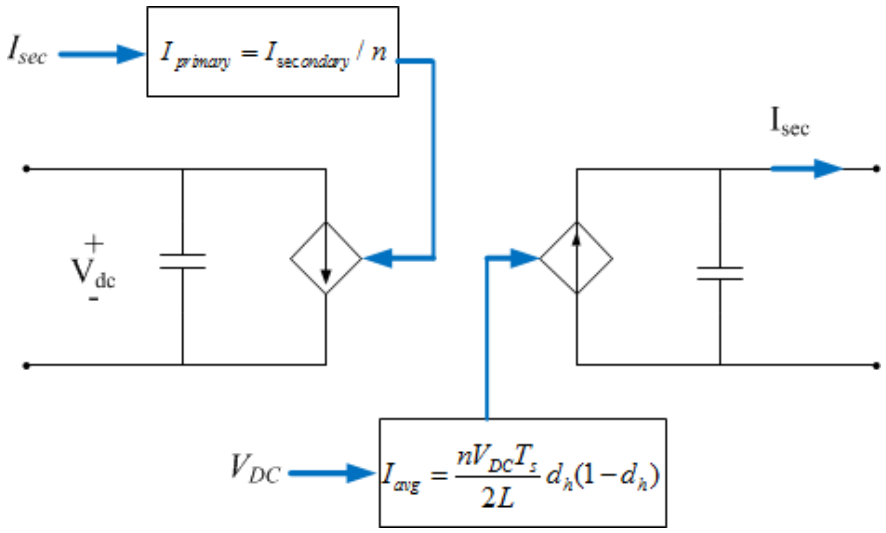

Figure 31: Average model of bidirectional DC/DC converter.

ratio of the high frequency transformer [29]. The DC/DC converter average model is implemented into the computer as shown in [[TO DO]]Fig. 9.

6.3.0.5 Variable Frequency Drive Model The dynamic relationships that govern the current controller for the variable frequency motor drive on the offshore platform are listed as (14) and (15). The details of their derivation can be found in [127]. Note that Vsd and Vsq are the direct and quadrature voltages, imr is the magnetization current, ÏĽ is machine speed, isq and isd are the direct and quadrature currents, ÏČ and ÏĎs are machine variables defined by (16) through (18). Note that Ls, Lr, and Lm are the stator, rotor, and magnetizing inductance, respectively. All variables are referred to the stator of the machine.

$$V_{sq} = R_s\left[u_q + \sigma\tau_s\omega i_{sd} + (1-\sigma)\tau_s\omega i_{mr}\right] \tag{15}$$

$$\sigma_s = \frac{L_s}{L_m} - 1, \sigma_r = \frac{L_r}{L_m} - 1 \tag{16}$$

$$\sigma_s = 1 - \frac{1}{(1+\sigma_s)(1+\sigma_r)} \tag{17}$$

$$\tau_s = \frac{L_m(1+\sigma_s)}{R_S} \tag{18}$$

Motor drive parameters and controller are provided in Table I and Fig. 11, respectively. One important feature of Fig. 32 is the established isd.

Table 10: Induction Motor Drive Machine Parameters.

Parameter	**Numerical Quantity**
Nominal Power, P	1.678 MW
Pole Pairs	12
Nominal Voltage, V_{LL}	2300V
Nominal Frequency, ω_o	377 rad/s
Stator Resistance, R_s	29 mΩ
Rotor Resistance, R_r	29 mΩ
Magnetizing Inductance, L_m	34.6 mH
Stator Inductance, L_s	35.2 mH
Rotor Inductance, L_r	35.2 mH
Stator Leakage Factor, σ_s	0.0173
Stator Leakage Factor, σ_s	0.0173
Total Leakage Factor, σ	0.0337
Stator Time Constant, τ_s	1.213 secs
Rotor Time Constant, τ_r	1.6 secs
Controller Constant, τ	3 ms
Controller Gains, K_P, K_I	13.67,333 sec^{-1}
i_{mr} Controller Gains	79.6, 50 sec^{-1}

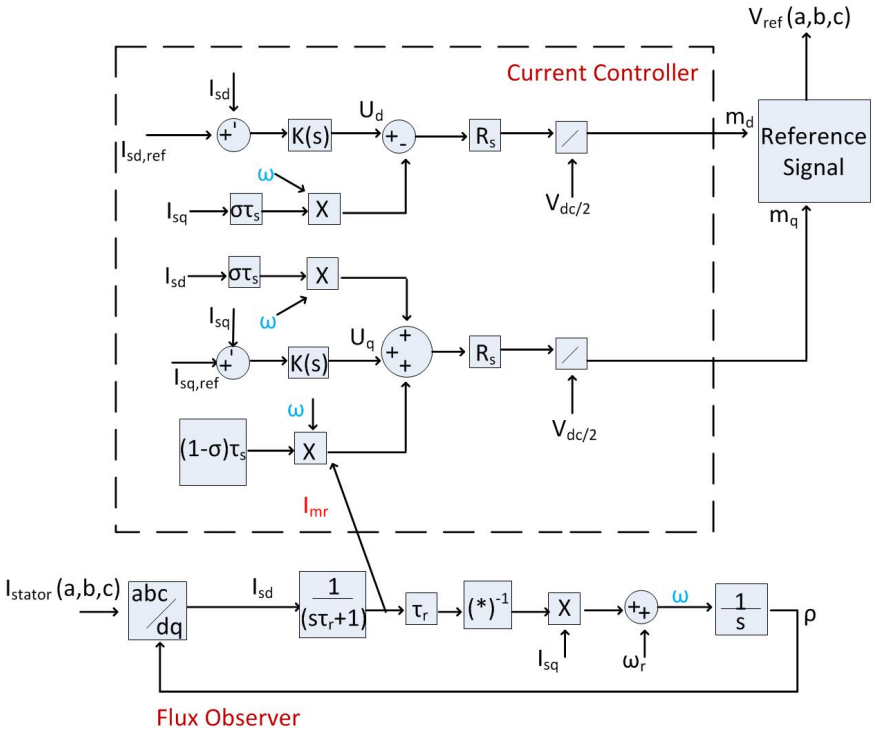

Figure 32: Average model of bidirectional DC/DC converter.

6.4 DISTRIBUTED SYSTEM ARCHITECTURE

During cycling to cycle operation, each type of embedded controller, the primary, the secondary, and the DC/DC converter, experience fixed and variable tasks. Each of that operation require computation resources, e.g. control logic calculation, for instance, that introduce delay within the distributed control loop. In the fallowing subsections, we discuss each delay in detail.

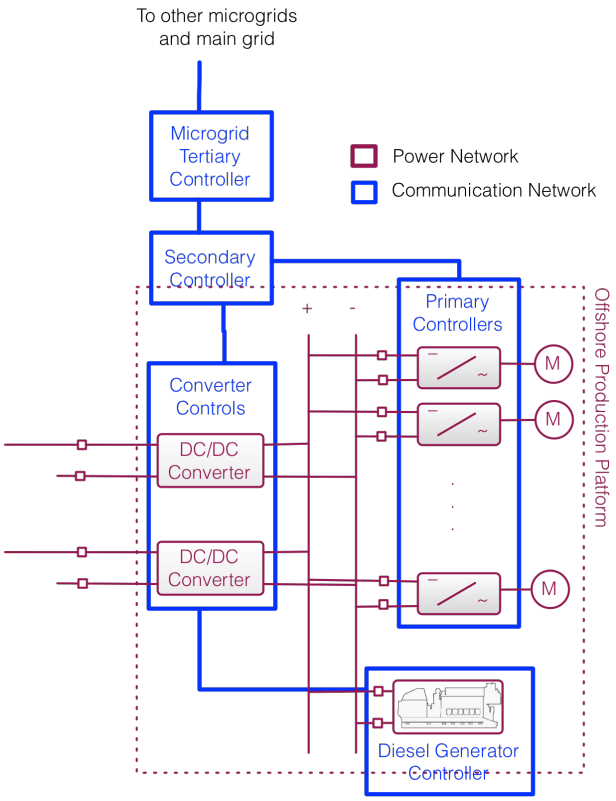

Figure 33: Microgrid's distributed communication architecture.

6.4.1 Power Control Loop

As to evaluate the real-time performance of the power control system, here we define the distributed control loop. The loop includes the hierarchical 3-level distributed controllers. At the lowest level is the independent open-loop primary controller. At the end of every cycle, the primary controller sends measured torques and speed of the attached induction machine. One level higher, the secondary controller receives the measured torques and speed values from all primary controllers located in the microgrid. In addition to the primary controller measurements, the secondary controller receives voltage level samples from the two DC/DC converters. Similarly to the primary controllers, the DC/DC converters send the

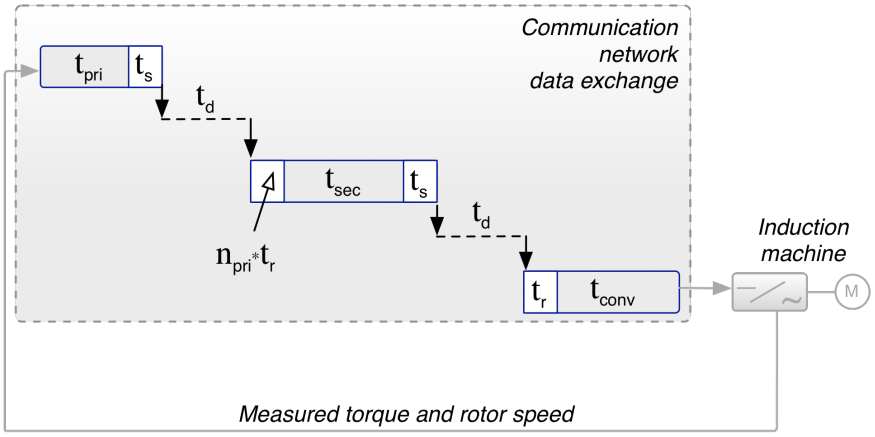

Figure 34: Microgrid's distributed control-loop.

measurements at the end of each execution cycle. Given all measured values in the microgrid, at the end of its cycle the secondary controller send adjusted duty cycle commands to the DC/DC converters. As the last step, the two DC/DC converters apply their respective commanded duty cycles. Graphical representation of the distributed control loop delay is shown by Fig. 34. At the highest control level, the Tertiary controller is in charge of facilitation conversation between the local microgrid and outside power networks. Those could be the main "stiff" grid, power generating facilities such as windfarm or other microgrids. Outside microgrid operations that involve the Tertiary controller, such as the transition from island to grid modes and vice versa, are outside of the scope of this paper. Fig. 33 presents the distributed communication architecture.

6.4.2 System Delays

Here we define formal the end-to-end delay $T_{cntrl-loop}$, as the time a sample is read until an adjustments is applied, of the distributed control loop

$$T_{cntrl-loop} = t_{pri} + t_{sec} + t_{conv} + 2t_s + 2t_d + (N_{pri} + 1)t_r \tag{18}$$

6.4.2.1 Control Logic Execution Delay In order to execute the control logic, each embedded controller's application needs a fixed amount of execution time. The embedded application would run on top of Real-Time Operating System (RTOS) which will have a fixed time slot for the execution of the application. Table 11 presents the assumed application execution time-slots for each of the embedded controller, that are consistent with [120]. The control logic delay in each microgrid controller is assumed to be deterministic.

Table 11: Microgrid's co-simulation parameters.

Parameter	**Numerical Quantity**
Number of primary controllers, N_{pri}	3
Primary controller cycle duration, t_{pri}	0.08 sec
Secondary controller cycle duration, t_{sec}	0.5 sec
DC/DC converter cycle duration, t_{conv}	0.08 sec
Transmission & Propagation per link delay, t_d	0.00005 sec
Packetization (inc. encryption) delay, t_s	0.24 sec
Depacketization (inc. decryption) delay, t_r	0.16 sec
Size of message payload (IP/UDP)	42 bytes

6.4.2.2 Security delay In our previous work [132], we presented a multicast security protocol that complies with the 3ms end-to-end delay posed by IEC 61850 [133]. The protocol leverages symmetric AES encryption confidentiality within the microgrid, and AES-based CMAC-96 message signatures for authentication. The targeted microgrid network [[Figure Ref]] consists of around 50 IEDs. At worst case, assuming that each secure multicast message

would need to be verified by each device within the network, the overhead due to the security protocol in terms of delay and packet size is given in Table 11.

6.4.2.3 Transmission and Propagation Delay Prior to the beginning and after the end of each application cycle the RTOS would receive, depackatize, and transmit, or packatize, communication packets. The microgrid employs the Ethernet/UDP/IP protocols. We define the packatization and depackatization delay at the sending and received end, that is expired by each packet to be the transmission delay. Furthermore, we assume conventional 100Mbps links to be employed within the communication network. The time between the last bit of a packet to be send and the first bit of the packet to be received by the other side is defined as propagation delay. All message within the microgrid are assumed to be of two types - sampled values and control messages. The message size is fixed at 42 bytes [134]. One link transmission and propagation delay is listed in Table 11. In addition to the fixed packets size, there is variable security overhead discussed in the previous section.

6.4.3 Communication Reliability

Due to the real-time delivery requirements, in order to minimize end-to-end delay the transmission protocol employed is UDP. Another reason for not employing TCP is the fact that by the time re-transmission arrive at the destination the data contained is stale. Since UDP does not provide re-transmission, reliability is achieved via periodic transmission of the most current measured values. In addition, the secondary controller cycle duration is about six times longer, than the duration of the primary controller or DC/DC converter. As such, at the beginning of its cycle the secondary controller has multiple packets from each logical incoming communication channel.

6.5 CO-SIMULATION

In order to evaluate the performance of the power control algorithms in realistic setting, we developed co-simulation tool. The tool incorporated the microgrids power and communication network via adaptive simulation co-scheduler [135]. The power network was simulated via Matlab, the communication network employed OMNeT++ , and the scheduler used the Adevs framework . The co-simulator was primary build as to investigate the performance of the power control algorithms in a realistic environments. In addition the tool, let us observe the adverse effect of delay onto the power control. Furthermore, we were able to compare different security architectures and their stability to be used in real-time multicast protocol for use in power networks' communications. From the investigation, we were able to quantify the effect of the types of delays.

The initial set-up was used as a baseline against the standalone Matlab simulations of the microgrid's power network. The communication network was bypassed, and the separate distributed controllers were directly exchanging cycle-by-cycle inputs and outputs. The only delay presents in the system was 0.005ms Matlab's internal fix-step. In those ideal conditions, the power output levels stabilized after transient periods, e.g. the star-ups of each induction machine. In the test scenario 3 induction machines started at over a second intervals (Fig. 35). For instance, at the first induction machine starts 1 seconds after the start of the scenario. The distributed controller can stabilize the output power prior to the start-up of the second induction machine at 1.7 seconds. The final induction machine starts and has no unsuitability effects on the output power.

OMNeT++ homepage: http://www.omnetpp.org/.
Adevs homepage: http://web.ornl.gov/~1qn/adevs/.

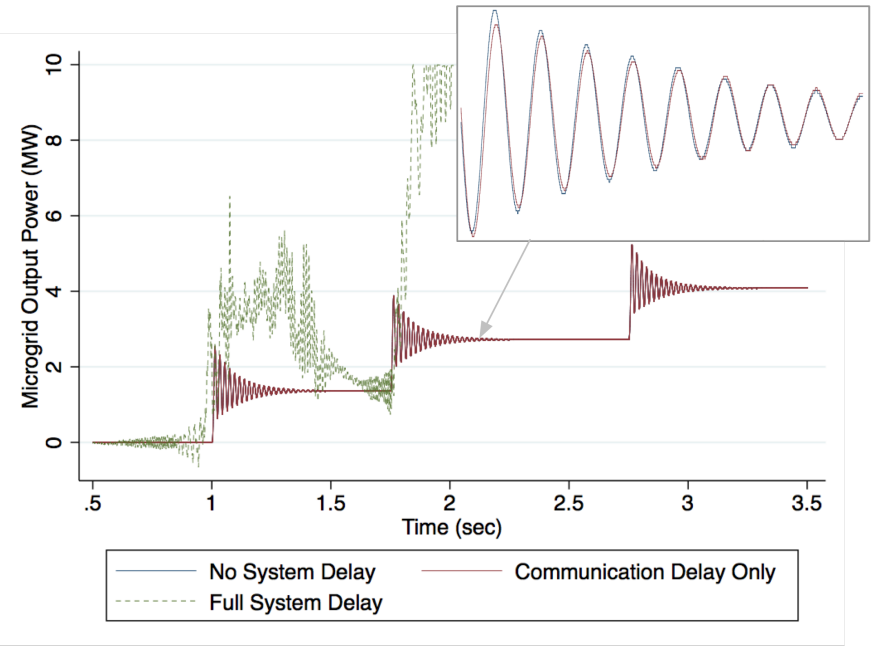

Figure 35: Stability of Microgrid'd output power under different delay constraints.

6.5.1 Effect of Communication Network Delay

For next step, the communication network was introduced in the loop. The initial test involved only transmission and transportation delay. The communication network makes use of the UDP/IP/Ethernet protocols. Since the output data rates of each embedded controller is low (10-100kbps) compared to the link bandwidths (.1-10Gbps), we assume that the communication network is congestion free. Furthermore, since the microgrid network is private dedicated industrial control network, there is no other traffic than the control messages exchanged and therefore there is no background traffic.

During the simulation, the data packets transmitted did not have any security measurements and were all of unicast nature. The presentation of those results is omitted from Fig. 35, due to the fact each link hop introduced marginal 0.05ms delay. The power control algorithm was more than capable of correction of the transmission and transportation delay.

6.5.2 Effect of Security Protocol Delay

In out previous work [132] we proposed a real-time secure multicast aimed at smart grid operational technology data exchanges. Here we present the simulations result when the security measures were introduced within the microgrids control loop. The zoomed window in Fig. 35 shows a closeup of the two power output waveforms. The direct connection (light blue), with no communication network present, is used a baseline to compare to the full communication delay (magenta). The communication delay graph includes transmission, transportation and secure protocol packetization and depacketization delay at each end-device. Furthermore, when employing security measures, the data packets have addition bits of overhead. However, the transportation delay for the additional data is negligible compared to the encryption and decryption delays. Table 12) presents measured results from the simulation scenario. The scenario was ran 10 different time with different random start-up delay for each embedded controller. The start-up delay is normally distributed 0.01-0.005 seconds. In the presence of communication delay, the mean control loop delay is 0.74 sec. This introduced a mean output error of 0.00057 MW. This is the difference between the two waveforms obsessed on the zoom region in figure 35.

Table 12: Co-simulation results: Comparison of the effects of delay on the microgrid's power output stability.

Scheme	$\overline{D}_{cntrl-loop}$ **(ms)**	$\overline{E}_{Output}$ **(MW)**	$\overline{\sigma}_{Output}$ **(MW)**
No System Delay	0.005	-	-
Comm. Delay Only	0.66	0.00057	0.000186
Full System Delay *unstable*	666.8	-5.74	0.026

6.5.3 Effect of Operating System Delay

As discussed prior, each embedded controller will have internal delay associated with the execution of the control logic, as well as miscellaneous tasks (reading or writing to outputs, etc.). We assume that primary controller and DC/DC Converters have 80ms internal delays, and the secondary controller has 500ms delay [120]. When such delay was introduced within the distributed control loop, the system becomes unstable. The power output levels of the microgrid while considering all system delay is the presented as well in Fig. 35. The presence of such large control loop delay, 666.8ms on average is too significant to maintain a stability power levels within the microgrid.

6.6 CONCLUSION AND FUTURE WORK

In this paper, we presented a microgrid power control architecture and the supporting communications infrastructure. In addition, a mathematical framework was provided as to justify the design of the distributed control approach. Simulation results were presented and discussed, as well as the future direction for research. A novel design of microgrid control is needed in order to cope with the significant delays introduced by the embedded controller.

7.0 CLOSING REMARKS

This dissertation presents an overview of the emerging trends in the power network and the challenges posed to the supporting communication network. Chapters II-V present an overview of microgrid communication networks, the design of secure real-time communication protocols, and the simulation framework created to validate those protocols. In chapter VI, the effect of system delay on power control algorithms and their ability to maintain stable voltage output level is presented.

7.1 LIMITATIONS OF THIS WORK

There are a number of assumption and omissions from this work. For the purpose of clarity, those limitations are listed in this section.

Data Characteristics. The profile of the microgrid's data considered in this work is the real-time control messages used for synchronization of the hierarchical distributed controllers. Non-vital data used for maintenance and logging functions, such as NERC CIP historian requirements [136], are not explicitly addressed. The overall goal of this dissertation is the design of the telecommunication network by aiming to address the most stringent requirements - the end-to-end real-time data transportation requirements. The underlying assumption is that a network designed for real-time data transfer and reliability should be robust enough to handle the non-real-time data flow. However, this approach relies on the premise that the data links are underutilized, which may not be the case in the presence of non-vital data flow. Any further investigation should consider maintenance data traffic's effect on the control data flow. Furthermore, throughout this work the IEC 61850 and IEC

62351 protocols are used to derive baseline requirements for the microgrid's communications network. It is the authors opinions that those are the two substation automation communication protocols with the most demanding communication requirements. The solutions presented in this work are designed with generosity in mind. As such any designs are transferable to networks making use of other application layer SAS protocols, such as DNP 2/3 or Modbus [137].

Communication Network. The data links employed within the microgrid are assumed to be UDP over IP over Ethernet or fiber-optic cables. The main consideration in the evaluation is the transmission speed of each link. Those are assumed to be 100Mbps. Due to the real-time end-to-end delay requirements of all control data, TCP over IP communication is considered unsuited for the application [138]. The re-transmission and sequence (re-)ordering functionalities of TCP are not desired. Each control data packet is self-contained, and the data carried does not depend on prior or post frames. The packet with the freshest timestamp makes all prior timestamped packets obsolete (even if received out of order).

Cyber-security. Most notably this work omits an in-depth discussion on cyber-security key distribution, storage, and renewal. These authors feel that this topic is significant enough to be addressed on it own merit. A key distribution analysis should consider the events of devices quasi-dynamically leaving and joining the microgrid network. The current assumption is that the network communication participants are static. The solution uses a single key to ensure confidentiality within the microgrid. However, integrity and authentication is ensured via point-to-point keys between a sender-receiver pair. Admittedly, this solution is less scalable than multicast group solutions [139]. However, the authors feel that the extra cost is justified since a compromise of a single note does not jeopardize the authentication security of the entire microgrid. Finally, the proposed security protocol does not comply with NERC-CIP's requirements for substation automation communication networks. Most notably, the devices within the Microgrid network are IP addressable, which is not the case in NERC-CIP specification [140].

Real-time operating system (RTOS). The investigation in this work assumes the use of RTOS as operating systems on the microgrid IEDs. This assumption is inline with best case practices employed by the utility equipment manufacturers. Most notably, this

techniques is used to ensure real-time guarantees on the execution of high-priory systems tasks [141].

7.2 FUTURE DIRECTION

As discussed earlier in this work, the results show that power control algorithms are very sensitive to delay within the control loop.ÂăA possible future research direction would be an investigation into more robust distributed algorithms. One approach would be to push more of the control logic onto the edge open-loop independent controllers - mainly the primary controllers and DC/DC Converters. This would result in removing the relatively slow secondary controller from the cycle-to-cycle operations loop, and changing its role to a profile setting function.Âă âĂÍAn important question to address is how microgrids fit into today's power distribution network. A natural comparison to the microgrid's communication network is the substation communication network. The communication protocols employed in those networks, e.g., IEC 61850, DNP3, do not provide cyber-security and instead rely on perimeter security - firewalls and private networks. Therefore, an important investigation would be to evaluate the suitability of the secure real-time protocol discussed in Chapter IV to substation communication. Such investigation would require greater substation investment in a simulation tool, mainly in order to assess the ability to simulate a network of hundreds or even thousands of real-time embedded devices. Investigation of this area would require paralyzation of the simulation and the simultaneous execution of simulator sub-parts on networked cluster machines. The foundation for paralyzation of the simulation is presented in Chapter V, and describes a co-simulation scheduler that treats devices as independent entities until a future synchronization point.Âă âĂÍ On microgrid specific topics, this dissertation omits any discussion of intra-microgrid communications as in these cases, the tertiary controller would be involved in setting-up, tearing-down and facilitating message sessions between two or more microgrids. As is shown in this current investigation, a slow responsive device, such as the secondary controller, has an adverse effect on the stability of power voltage levels. With the introduction of the even slower responding tertiary

controller, the power control strategy is bound to become more complex and challenging. From a communications standpoint, there would then be a need for the investigation of how the microgrid would conduct an initial handshake. Having a third party certificate authority may pose a security risk and increase the overall system delay.Âă

Another opportunity for extension of this work is investigating real-time secure communication at billion devices scale. Notoriously, such protocols do not scale well beyond a few hundred devices. The current trends in Information Technology, such as Internet of Things (IoT) and Cloud Computing, are focusing on secure, persistent connectivity. However, the current generation of vendor solutions provide less than real-time communication performance as far as the power network is concerned. A round trip time of the hundred milliseconds is satisfactory for personal device communications, however, in smart grid context, it is inadequate.

BIBLIOGRAPHY

[1] X. Lu, W. Wenye , and J. Ma, "Authentication and integrity in the smart grid: An empirical study in substation automation systems." International Journal of Distributed Sensor Networks, Nov. 2012.

[2] The OpenWrt developer team, "Openwrt," 2014.

[3] P. Kundur, *Power system stability and control.* Tata McGraw-Hill Education, 1994.

[4] C. A. G. Jianqing Zhang, "Application-aware secure multicast for power grid communications," *International Journal of Security and Networks*, vol. 6, no. 1, pp. 40–52, 2011.

[5] G. F. Reed, B. M. Grainger, A. R. Sparacino, and Z.-H. Mao, "Ship to grid: Medium-voltage dc concepts in theory and practice," *Power and Energy Magazine, IEEE*, vol. 10, no. 6, pp. 70–79, 2012.

[6] E. Ibanez, T. Mai, and L. Coles, "Analyzing the deployment of large amounts of offshore wind to design an offshore transmission grid in the united states," in *11th International Workshop on Large-Scale Integration of Wind Power into Power Systems*, 2012.

[7] P. Kundur, *Power System Stability and Control.* McGraw-Hill Professional, 1994.

[8] H. Farhangi, "The path of the smart grid," *Power and Energy Magazine, IEEE*, vol. 8, no. 1, pp. 18–28, 2010.

[9] D. Bakken, A. Bose, C. Hauser, D. Whitehead, and G. Zweigle, "Smart generation and transmission with coherent, real-time data," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 928–951, 2011.

[10] B. Grainger, G. Reed, T. McDermott, M. Zhi-Hong, V. Kounev, and D. Tipper, "Analysis of an offshore medium voltage dc microgrid environment: Power sharing controller design,"

[11] V. Kounev, D. Tipper, B. M. Grainger, and G. Reed, "Analysis of an offshore medium voltage dc microgrid environmentâĂŤpart ii: Communication network architecture," in *T&D Conference and Exposition, 2014 IEEE PES*, pp. 1–5, IEEE, 2014.

[12] S. Amin and B. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *Power and Energy Magazine, IEEE*, vol. 3, no. 5, pp. 34–41, 2005.

[13] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *Security Privacy, IEEE*, vol. 7, no. 3, pp. 75–77, 2009.

[14] V. Gungor, B. Lu, and G. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *Industrial Electronics, IEEE Transactions on*, vol. 57, no. 10, pp. 3557–3564, 2010.

[15] M. S. Obaidat, A. Anpalagan, and I. Woungang, *Handbook of green information and communication systems*. Academic Press, 2012.

[16] R. Lasseter and P. Paigi, "Microgrid: a conceptual solution," in *Power Electronics Specialists Conference, 2004. PESC 04. 2004 IEEE 35th Annual*, vol. 6, pp. 4285–4290 Vol.6, 2004.

[17] F. Katiraei and M. Iravani, "Power management strategies for a microgrid with multiple distributed generation units," *Power Systems, IEEE Transactions on*, vol. 21, no. 4, pp. 1821–1831, 2006.

[18] J. Bryson, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0." NIST, Feb. 2012.

[19] V. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. Hancke, "Smart grid technologies: Communication technologies and standards," *Industrial Informatics, IEEE Transactions on*, vol. 7, no. 4, pp. 529–539, 2011.

[20] P. Piagi and R. Lasseter, "Autonomous control of microgrids," in *Power Engineering Society General Meeting, 2006. IEEE*, pp. 8 pp.–, 2006.

[21] M. Prodanovic and T. Green, "High-quality power generation through distributed control of a power park microgrid," *Industrial Electronics, IEEE Transactions on*, vol. 53, no. 5, pp. 1471–1482, 2006.

[22] S. Anand, B. G. Fernandes, and M. Guerrero, "Distributed control to ensure proportional load sharing and improve voltage regulation in low-voltage dc microgrids," *Power Electronics, IEEE Transactions on*, vol. 28, no. 4, pp. 1900–1913, 2013.

[23] J. Guerrero, J. Vasquez, J. Matas, L. de VicuÃśa, and M. Castilla, "Hierarchical control of droop-controlled ac and dc microgrids - a general approach toward standardization," *Industrial Electronics, IEEE Transactions on*, vol. 58, no. 1, pp. 158–172, 2011.

[24] Q. Shafiee, J. Guerrero, and J. Vasquez, "Distributed secondary control for islanded microgrids - a novel approach," *Power Electronics, IEEE Transactions on*, vol. 29, no. 2, pp. 1018–1031, 2014.

[25] Technical Committee 57, "IEC 61850." IEC, Jan. 2003.

[26] IEEE-SA, "IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." IEEE, 2012.

[27] E. Callaway, P. Gorday, L. Hester, J. Gutierrez, M. Naeve, B. Heile, and V. Bahl, "Home networking with ieee 802.15.4: a developing standard for low-rate wireless personal area networks," *Communications Magazine, IEEE*, vol. 40, no. 8, pp. 70–77, 2002.

[28] C. Bisdikian, "An overview of the bluetooth wireless technology," *Communications Magazine, IEEE*, vol. 39, no. 12, pp. 86–94, 2001.

[29] J. W. Depeng Li, Zeyar Aung and A. Sanchez, "Efficient and fault-diagnosable authentication scheme for advanced metering infrastructure," May 2013.

[30] D. Seo, H. Lee, and A. Perrig, "Secure and efficient capability-based power management in the smart grid," in *Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on*, pp. 119–126, 2011.

[31] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 327–332, 2010.

[32] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 327–332, 2010.

[33] A. Bartoli, J. HernaÌĄndez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation for smart grid m2m networks," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 333–338, 2010.

[34] Technical Committee 57, "IEC 62351." IEC, Jan. 2003.

[35] S. Fuloria, R. Anderson, K. McGrath, K. Hansen, and F. Alvarez, "The Protection of Substation Communications." SCADA Security Scientific Symposium, 2012.

[36] L. Reyzin and N. Reyzin, "Better than biba: Short one-time signatures with fast signing and verifying," in *Information Security and Privacy* (L. Batten and J. Seberry, eds.), vol. 2384 of *Lecture Notes in Computer Science*, pp. 144–153, Springer Berlin Heidelberg, 2002.

[37] K. Cairns, C. Hauser, and T. Gamage, "Flexible data authentication evaluated for the smart grid," in *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, pp. 492–497, 2013.

[38] Y.-C. Hu, M. Jakobsson, and A. Perrig, "Efficient constructions for one-way hash chains," in *Applied Cryptography and Network Security* (J. Ioannidis, A. Keromytis, and M. Yung, eds.), vol. 3531 of *Lecture Notes in Computer Science*, pp. 423–441, Springer Berlin Heidelberg, 2005.

[39] 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 *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ASIA CCS '13, (New York, NY, USA), pp. 287–298, ACM, 2013.

[40] D. S. Adrian Perri, Ran Canetti and J. D. Tygar, "Efficient and secure source authentication for multicast," May 2013.

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

[42] W. Neumann, "Horse: an extension of an r-time signature scheme with fast signing and verification," in *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, vol. 1, pp. 129–134 Vol.1, 2004.

[43] Q. Li and G. Cao, "Multicast authentication in the smart grid with one-time signature," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 686–696, 2011.

[44] Eaton, "Smp 16 gateway (data concentrator)." http://www.cooperindustries.com/content/public/en/power_systems/products/automation_and_control/smp_products/smp-16-gateway.html, 2014.

[45] S. E. Laboratories, "Sel-3530-4." https://www.selinc.com/sel-3530/, 2014.

[46] V. Kounev and D. Tipper, "Advanced metering and demand response communication performance in zigbee based hans," in *Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on*, pp. 31–36, 2013.

[47] B. R. Haverkort, K. S. Trivedi, G. Rubino, and R. Marie, *Performability modelling: techniques and tools*, vol. 1. Wiley New York, 2001.

[48] N. R. Committee, "Reversing president obama's offshore moratorium act (h.r. 1231)." http://naturalresources.house.gov, March 2011.

[49] S. Besore, "Fuel consumption, overload capacity among critical criteria in selection of generator sets." http://www.drillingcontractor.org/, 2010.

[50] P. Yadav, R. Kumar, S. Panda, and C. Chang, "An improved harmony search algorithm for optimal scheduling of the diesel generators in oil rig platforms," *Energy Conversion and Management*, vol. 52, no. 2, pp. 893 – 902, 2011.

[51] GreenRig, "Drilling and production with lower fuel consumption and reduced environmental impact." http://comprehensivepower.com/wp-content/uploads/2012/04/green-rig-comprehensive-power.pdf, 2012.

[52] D. Wetteroth, *OSI Reference Model for Telecommunications*. McGraw-Hill Professional, 2001.

[53] B. A. Forouzan, *TCP/IP Protocol Suite*. New York, NY, USA: McGraw-Hill, Inc., 2 ed., 2002.

[54] P. Vas, *Sensorless Vector and Direct Torque Control*. New York, NY, USA: Oxford University Press, 1998.

[55] T.-Y. Yen and W. Wolf, "Performance estimation for real-time distributed embedded systems," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 9, no. 11, pp. 1125–1136, 1998.

[56] M. Tornatore, G. Maier, and A. Pattavina, "Availability design of optical transport networks," *Selected Areas in Communications, IEEE Journal on*, vol. 23, no. 8, pp. 1520–1532, 2005.

[57] L. Bastos and H. Wietgrefe, "Wimax at traffic-demanding electronic warfare air exercise elite 2008," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, pp. 1–7, 2009.

[58] "Satellite orbits." http://www.inetdaemon.com/tutorials/satellite/orbits/, 2013.

[59] P. Mach and R. Bestak, "Wimax performance evaluation," in *Networking, 2007. ICN '07. Sixth International Conference on*, pp. 17–17, 2007.

[60] B. Vojcic, R. Pickholtz, and L. Milstein, "Performance of ds-cdma with imperfect power control operating over a low earth orbiting satellite link," *Selected Areas in Communications, IEEE Journal on*, vol. 12, no. 4, pp. 560–567, 1994.

[61] A. Dandalis, V. Prasanna, and J. Rolim, "A comparative study of performance of aes final candidates using fpgas," in *Cryptographic Hardware and Embedded Systems âĂŤ CHES 2000* (Ã. KoÃğ and C. Paar, eds.), vol. 1965 of *Lecture Notes in Computer Science*, pp. 125–140, Springer Berlin Heidelberg, 2000.

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

[63] P. Piagi and R. Lasseter, "Autonomous control of microgrids," in *Power Engineering Society General Meeting, 2006. IEEE*, 2006.

[64] M. Prodanovic and T. Green, "High-quality power generation through distributed control of a power park microgrid," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1471–1482, 2006.

[65] 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 Transactions on Power Electronics*, vol. 28, no. 4, pp. 1900–1913, 2013.

[66] R. Lasseter and P. Paigi, "Microgrid: a conceptual solution," in *IEEE 35th Annual Power Electronics Specialists Conference*, June 2004.

[67] K. De Brabandere, K. Vanthournout, J. Driesen, G. Deconinck, and R. Belmans, "Control of microgrids," in *IEEE Power Engineering Society General Meeting*, 2007.

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

[69] 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 Transactions on Industrial Electronics*, vol. 58, no. 1, pp. 158–172, 2011.

[70] B. Grainger, G. Reed, T. McDermott, Z. Mao, V. Kounev, D. Tipper, "Analysis of an Offshore Medium Voltage DC Microgrid Environment âĂŞ Part I: Power Sharing Controller Design," in *IEEE T&D PES*, 2014.

[71] V. Kounev, D. Tipper, B. Grainger, G. Reed, "Analysis of an Offshore Medium Voltage DC Microgrid Environment âĂŞ Part II: Communication Network Architecture," in *IEEE T&D PES*, 2014.

[72] 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 Transactions on Industrial Electronics*, vol. 56, no. 3, pp. 726–736, 2009.

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

[74] Technical Committee 57, "IEC 62351." International Electrotechnical Commission, Jan. 2010.

[75] Technical Committee 57, "IEC 61850." International Electrotechnical Commission, Jan. 2003.

[76] S. Fuloria, R. Anderson, K. McGrath, K. Hansen, and F. Alvarez, "The Protection of Substation Communications." SCADA Security Scientific Symposium, 2012.

[77] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proceedings IEEE Symposium on Security and Privacy*, 2000.

[78] L. Reyzin and N. Reyzin, "Better than biba: Short one-time signatures with fast signing and verifying," in *Information Security and Privacy*, 2002.

[79] K. Cairns, C. Hauser, and T. Gamage, "Flexible data authentication evaluated for the smart grid," in *Smart Grid Communications (SmartGridComm) IEEE International Conference on*, pp. 492–497, 2013.

[80] C. Szilagy and P. Koopman, "A flexible approach to embedded network multicast authentication," 2008.

[81] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, "Time valid one-time signature for time-critical multicast data authentication," in *INFOCOM 2009, IEEE*, 2009.

[82] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, "Microgrid cyber security reference architecture.," tech. rep., Sandia National Laboratories (HierarchicalSNL-NM), Albuquerque, NM (United States), 2013.

[83] W.-j. Kim, J. Kun, and A. Ajit, "Real-time operating environment for networked control systems," *IEEE Transactions on on Automation Science and Engineering*, vol. 3, no. 3, pp. 287–296, 2006.

[84] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[85] ECRYPT, "Yearly report on algorithms and keysizes," *European Network of Excellence in Cryptology II*, vol. 21, 2010.

[86] M. J. Dworkin, "Sp 800-38b. recommendation for block cipher modes of operation: the cmac mode for authentication," 2005.

[87] Enisa, "Algorithms, key sizes and parameters report," 2013.

[88] 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 *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, 2013.

[89] X. Lu, W. Wenye , and J. Ma, "Authentication and integrity in the smart grid: An empirical study in substation automation systems." International Journal of Distributed Sensor Networks, Nov. 2012.

[90] IETF, "The aes-cmac-96 algorithm and its use with ipsec," May 2014.

[91] Q. Shafiee, J. C. Vasquez, and J. M. Guerrero, "Distributed secondary control for islanded microgrids-a networked control systems approach," in *IECON 2012-38th Annual Conference on IEEE Industrial Electronics Society*, 2012.

[92] J. J. Nutaro, *Building software for simulation: theory and algorithms, with applications in C++*. John Wiley & Sons, 2011.

[93] M. Montoya, "Islands in the storm: Integrating microgrids into the larger grid," *IEEE Power and Energy Magazine*, vol. 11, no. 4, pp. 33–39, 2013.

[94] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control systems," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1963–1976, 2012.

[95] J. A. O. K. Mets and C. Develder, "Combining Power and Communication Network Simulation for Cost-Effective Smart Grid Analysis," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1771–1796, 2014.

[96] R. Mao, H. Li, Y. Xu, and H. Li, "Wireless Communication for Controlling Microgrids: Co-Simulation and Performance Evaluation," in *Proc., IEEE PES Power and Energy Society General Meeting*, pp. 1–5, 2013.

[97] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, "Distributed Secondary Control for Islanded Microgrids - A Novel Approach," *IEEE Transactions on Power Electronics*, vol. 29, no. 2, pp. 1018–1031, 2014.

[98] X. Tong, "The Co-Simulation Extending for Wide-Area Communication Networks in Power System," in *Proc., IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, pp. 1–4, 2010.

[99] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "EPOCHS: A Platform for Agent-Based Electric Power and Communication Simulation Built from Commercial Off-the-Shelf Components," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 548–558, 2006.

[100] Y. Li, W. Li, and Y. Lu, "Computer-Aided Simulation Analysis of A Novel Structure Hybrid Magnetic Bearing," *IEEE Transactions on Magnetics*, vol. 44, no. 10, pp. 2283–2287, 2008.

[101] W. Li, A. Monti, M. Luo, and R. A. Dougal, "VPNET: A Co-Simulation Framework for Analyzing Communication Channel Effects on Power Systems," in *Proc., IEEE Electric Ship Technologies Symposium (ESTS)*, pp. 143–149, 2011.

[102] H. Lin, *Communication Infrastructure for the Smart Grid: A Co-Simulation Based Study on Techniques to Improve the Power Transmission System Functions with Efficient Data Networks*. PhD thesis, Virginia Polytechnic Institute and State University, 2012.

[103] ABB in the United States, "U.S. Department of Energy to fund major Offshore Wind Grid Interconnection study," 2015.

[104] I. Evans and R. Limpaecher, "High power clean dc bus generation using ac-link ac to dc power voltage conversion, dc regulation, and galvanic isolation," in *Electric Ship Technologies Symposium, 2009. ESTS 2009. IEEE*, pp. 290–301, IEEE, 2009.

[105] R. H. Lasseter and P. Paigi, "Microgrid: a conceptual solution," in *Power Electronics Specialists Conference, 2004. PESC 04. 2004 IEEE 35th Annual*, vol. 6, pp. 4285–4290, IEEE, 2004.

[106] T. L. M, "Power conversion systems for microgrids," in *Rap Session*, ECCE, 2012.

[107] Falco F, "Subsea Technologies at the Heart of Future Oilfields," 2014.

[108] W. Zhang, F. C. Lee, and P.-Y. Huang, "Energy management system control and experiment for future home," in *Energy Conversion Congress and Exposition (ECCE), 2014 IEEE*, pp. 3317–3324, IEEE, 2014.

[109] K. Engelen, E. Leung Shun, P. Vermeyen, I. Pardon, R. D'hulst, J. Driesen, and R. Belmans, "The feasibility of small-scale residential dc distribution systems," in *IEEE Industrial Electronics, IECON 2006-32nd Annual Conference on*, pp. 2618–2623, IEEE, 2006.

[110] M.-H. Ryu, H.-S. Kim, J.-H. Kim, J.-W. Baek, and J.-H. Jung, "Test bed implementation of 380v dc distribution system using isolated bidirectional power converters," in *Energy Conversion Congress and Exposition (ECCE), 2013 IEEE*, pp. 2948–2954, IEEE, 2013.

[111] A. Kwasinski and A. Kwasinski, "Operational aspects and power architecture design for a microgrid to increase the use of renewable energy in wireless communication networks," in *Power Electronics Conference (IPEC-Hiroshima 2014-ECCE-ASIA), 2014 International*, pp. 2649–2655, IEEE, 2014.

[112] A. Kwasinski and A. Kwasinski, "Role of energy storage in a microgrid for increased use of photovoltaic systems in wireless communication networks," in *Telecommunications Energy Conference (INTELEC), 2014 IEEE 36th International*, pp. 1–8, IEEE, 2014.

[113] L. Xu and D. Chen, "Control and operation of a dc microgrid with variable generation and energy storage," *Power Delivery, IEEE Transactions on*, vol. 26, no. 4, pp. 2513–2522, 2011.

[114] K. De Brabandere, B. Bolsens, J. Van den Keybus, A. Woyte, J. Driesen, and R. Belmans, "A voltage and frequency droop control method for parallel inverters," *Power Electronics, IEEE Transactions on*, vol. 22, no. 4, pp. 1107–1115, 2007.

[115] J.-W. Kim, H.-S. Choi, and B. H. Cho, "A novel droop method for converter parallel operation," *Power Electronics, IEEE Transactions on*, vol. 17, no. 1, pp. 25–32, 2002.

[116] J. M. Guerrero, N. Berbel, J. Matas, L. G. de Vicuña, and J. Miret, "Decentralized control for parallel operation of distributed generation inverters in microgrids using

resistive output impedance," in *IEEE Industrial Electronics, IECON 2006-32nd Annual Conference on*, pp. 5149–5154, IEEE, 2006.

[117] J. Rocabert, A. Luna, F. Blaabjerg, and P. Rodriguez, "Control of power converters in ac microgrids," *Power Electronics, IEEE Transactions on*, vol. 27, no. 11, pp. 4734–4749, 2012.

[118] I. Batarseh, K. Siri, and H. Lee, "Investigation of the output droop characteristics of parallel-connnected dc-dc converters," in *Power Electronics Specialists Conference, PESC'94 Record., 25th Annual IEEE*, pp. 1342–1351, IEEE, 1994.

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

[120] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. De Vicuña, and M. Castilla, "Hierarchical control of droop-controlled ac and dc microgridsâĂŤa general approach toward standardization," *Industrial Electronics, IEEE Transactions on*, vol. 58, no. 1, pp. 158–172, 2011.

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

[122] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, "Microgrid cyber security reference architecture.," tech. rep., Sandia National Laboratories (HierarchicalSNL-NM), Albuquerque, NM (United States), 2013.

[123] Q. Shafiee, J. C. Vasquez, and J. M. Guerrero, "Distributed secondary control for islanded microgrids-a networked control systems approach," in *IECON 2012-38th Annual Conference on IEEE Industrial Electronics Society*, 2012.

[124] J. Li, A. Q. Huang, S. Bhattacharya, and W. Jing, "Application of active npc converter on generator side for mw direct-driven wind turbine," in *Applied Power Electronics Conference and Exposition (APEC), 2010 Twenty-Fifth Annual IEEE*, pp. 1010–1017, IEEE, 2010.

[125] P. C. Krause, O. Wasynczuk, S. D. Sudhoff, and S. Pekarek, *Analysis of electric machinery and drive systems*, vol. 75. John Wiley & Sons, 2013.

[126] K. Johnson, L. J. Fingersh, M. Balas, and L. Pao, "Methods for increasing region 2 power capture on a variable speed hawt," in *Paper No. AIAA-2004-0350, Proc. 23rd ASME Wind Energy Symposium, Reno, NV*, pp. 103–113, 2004.

[127] A. Yazdani and R. Iravani, *Voltage-sourced converters in power systems: modeling, control, and applications*. John Wiley & Sons, 2010.

[128] S. Hiti, D. Boroyevich, and C. Cuadros, "Small-signal modeling and control of three-phase pwm converters," in *Industry Applications Society Annual Meeting, 1994., Conference Record of the 1994 IEEE*, pp. 1143–1150, IEEE, 1994.

[129] R. W. De Doncker, D. M. Divan, and M. H. Kheraluwala, "A three-phase soft-switched high-power-density dc/dc converter for high-power applications," *Industry Applications, IEEE Transactions on*, vol. 27, no. 1, pp. 63–73, 1991.

[130] D. Costinett, D. Maksimovic, and R. Zane, "Design and control for high efficiency in high step-down dual active bridge converters operating at high switching frequency," *Power Electronics, IEEE Transactions on*, vol. 28, no. 8, pp. 3931–3940, 2013.

[131] D. Costinett, H. Nguyen, R. Zane, and D. Maksimovic, "Gan-fet based dual active bridge dc-dc converter," in *Applied Power Electronics Conference and Exposition (APEC), 2011 Twenty-Sixth Annual IEEE*, pp. 1425–1432, IEEE, 2011.

[132] V. Kounev, D. Tipper, A. Yavuz, B. Grainger, G. Reed, "A secure communication architecture for distributed microgrid control," *Smart Grid, IEEE Transactions on*, 2015.

[133] Technical Committee 57, "IEC 61850." International Electrotechnical Commission, Jan. 2003.

[134] V. Kounev, D. Tipper, B. Grainger, G. Reed, "Analysis of an Offshore Medium Voltage DC Microgrid Environment âĂŞ Part II: Communication Network Architecture," in *IEEE T&D PES*, 2014.

[135] V. Kounev, D. Tipper, M. Levesque, B. Grainger, T. McDermott, G. Reed, "A Microgrid Co-Simulation Framework," in *IEEE T&D PES*, 2014.

[136] A. Hahn, B. Kregel, M. Govindarasu, J. Fitzpatrick, R. Adnan, S. Sridhar, and M. Higdon, "Development of the powercyber scada security testbed," in *Proceedings of the sixth annual workshop on cyber security and information intelligence research*, p. 21, ACM, 2010.

[137] J. Makhija and L. Subramanyan, "Comparison of protocols used in remote monitoring: Dnp 3.0, iec 870-5-101 & modbus," *Electronics Systems Group, IIT Bombay, India, Tech. Rep*, 2003.

[138] M. Felser, "Real-time ethernet–industry prospective," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1118–1129, 2005.

[139] IETF, "The multicast group security architecture." https://tools.ietf.org/html/rfc3740, 2015.

[140] R. Anderson and S. Fuloria, "Security economics and critical national infrastructure," in *Economics of Information Security and Privacy*, pp. 55–66, Springer, 2010.

[141] S. E. Laboratories, "Sel-3530-4." https://www.selinc.com/WorkArea/DownloadAsset.aspx?id=8273, 2015.