


2022

## Examining Cooperative System Responses Against Grid Integrity Attacks

Alexander D. Parady  
*University of Central Florida*

 Part of the [Computer Engineering Commons](#), and the [Information Security Commons](#)  
Find similar works at: <https://stars.library.ucf.edu/honorsthesis>  
University of Central Florida Libraries <http://library.ucf.edu>

This Open Access is brought to you for free and open access by the UCF Theses and Dissertations at STARS. It has been accepted for inclusion in Honors Undergraduate Theses by an authorized administrator of STARS. For more information, please contact [STARS@ucf.edu](mailto:STARS@ucf.edu).

---

### Recommended Citation

Parady, Alexander D., "Examining Cooperative System Responses Against Grid Integrity Attacks" (2022). *Honors Undergraduate Theses*. 1183.  
<https://stars.library.ucf.edu/honorsthesis/1183>

EXAMINING COOPERATIVE SYSTEM RESPONSES  
AGAINST GRID INTEGRITY ATTACKS

by

ALEXANDER PARADY

A thesis submitted in partial fulfillment of the requirements  
for the Honors Undergraduate Thesis Program  
in Electrical Engineering in the  
College of Engineering and Computer Science  
and the Burnett Honors College  
at the University of Central Florida  
Orlando, Florida

Spring Term 2022

Thesis Chair: Zihua Qu, Ph.D.

## **ABSTRACT**

Smart grid technologies are integral to society's transition to sustainable energy sources, but they do not come without a cost. As the energy sector shifts away from a century's reliance on fossil fuels and centralized generation, technology that actively monitors and controls every aspect of the power infrastructure has been widely adopted, resulting in a plethora of new vulnerabilities that have already wreaked havoc on critical infrastructure. Integrity attacks that feedback false data through industrial control systems, which result in possible catastrophic overcorrections and ensuing failures, have plagued grid infrastructure over the past several years. This threat is now at an all-time high and shows little sign of cooling off.

To combat this trajectory, this research explores the potential for simulated grid characteristics to examine robust security measures by use of a cyber-physical system (CPS) testbed constructed across the University of Central Florida (UCF) Resilient, Intelligent and Sustainable Energy Systems (RISES) Lab Cluster. This thesis explores hypothesized defense mechanisms and awareness algorithms to protect against unforeseen vulnerabilities brought on by grid attacks that will test the boundaries of commercial cybersecurity standards. Through an extensive probe across proposed defenses and vulnerability analysis of industrial systems, a blueprint for future research is outlined that will yield results that have the potential to ripple improvements across the power sector. The sanctity of critical infrastructure is of the highest priority for global powers. As such, this research bolsters the tools at the disposal of international entities and seeks to protect the ever-expanding lifestyle that reliable access to energy provides.

## **ACKNOWLEDGEMENTS**

This research is possible in part by DOE award DE-EE0009339 and from support from Siemens Energy, General Electric, and Florida Power & Light.

I would like to thank my research team across the RISES Lab Cluster who has assisted me in this research. A big thank you to my thesis chair and research advisor Dr. Zhihua Qu for taking me under his wing through the entire process and giving me the resources to flourish within our field. Additionally, a lot is owed to my thesis committee consisting of Dr. Aleksandar Dimitrovski, Dr. Qun Zhou Sun, and Dr. Wei Sun for guiding my research to a deliverable product. This paper would not be possible without all their guidance and support.

Recognition is owed to my IEEE UCF, Theta Tau, and UCF families as well as my mother for supporting me through my time in university thus far and in being my crutch through the most challenging times. They have given me the support I have needed in my toughest times through the past four years and they will always have my back in whatever comes next!

# TABLE OF CONTENTS

ABSTRACT.....	ii
ACKNOWLEDGEMENTS.....	iii
LIST OF FIGURES .....	vi
1. INTRODUCTION .....	1
1.1 Critical Infrastructure .....	4
1.2 Power System Control Center.....	8
1.3 Power Grid Cybersecurity.....	10
1.4 Vulnerability Analysis.....	14
1.5 Distributed Cooperative Control for Grid Edge.....	17
1.6 Industry Adoption .....	18
2. ENHANCED OPERATIONAL TECHNOLOGY SYSTEM DEFENSES.....	21
2.1 Cooperative Network Precision Timing Protocol.....	21
2.2 Resilient Control from Embedded Dynamic Encoding & Decoding.....	25
2.3 Competitive Interaction for Distributed Consensus .....	29
3. CYBER-PHYSICAL SECURITY TESTBED .....	32
3.1 UCF RISES CPS Testbed .....	32
3.2 Siemens CrossBow.....	40
3.3 Future Proposed OT Experiments.....	42

3.4 Future Vulnerability Assessment .....	48
3.5 Desired Outcomes .....	51
4. CONCLUSION.....	54
REFERENCES .....	55

## LIST OF FIGURES

Figure 1. ISO New England Power Grid Monitoring Room [15].....	9
Figure 2. Typical PTP Topology [28].....	23
Figure 3. Typical CN-PTP Topology [28].....	23
Figure 4. Standard CPS Networked Control System [3] .....	25
Figure 5. Example of a Transistor Based Chaotic Circuit. [30].....	26
Figure 6. Chua Circuit Realized using Op Amps and Resistors to Implement Chua Diode [30].	26
Figure 8. Enhanced CPS Control System with Embedded Nonlinear Components [3] .....	27
Figure 7. Chua Circuit Chaotic Waveform Output Examples [30] .....	27
Figure 9. Interconnection of the cooperative system with the hidden network [6] .....	29
Figure 10. Three-layer Cooperative System Networked Model [6] .....	30
Figure 11. UCF RISES CPS Testbed Overall Scope.....	36
Figure 12. Microgrid Control Laboratory Testbed Diagram .....	37
Figure 13. Smart Protection and Control Laboratory Testbed Diagram.....	37
Figure 14. Smart Infrastructure Data Analytics Lab Testbed Diagram .....	38
Figure 15. Siemens Digital Grid Laboratory Testbed Diagram.....	38
Figure 16. Cyber-Physical Systems Laboratory Testbed Diagram.....	38
Figure 17. CPS Testbed Central Control in HEC 434 .....	39
Figure 18. OPAL-RT OP5707CG Interfacing with Physical Oscilloscope [35] .....	39
Figure 19. CrossBow Software Interface.....	41
Figure 20. CN-PTP Digital Grid Lab Proposed Experimental Topology.....	44

## 1. INTRODUCTION

Digitalization of the power grid has expanded far and wide and will be a critical gateway to increased productivity and boosting new business models for years to come. Remote access, system automation, and distributed energy are some of the features of the energy sector that have made the onset of the smart grid a foregone conclusion. However, the tremendous benefits in efficiency, sustainability, and convenience come with their tradeoffs. Contradictory goals within the complexity of the digital energy landscape result in added vulnerabilities in system security as ease of use often results in a direct decrease in security [1]. Additionally, as the internet of things (IoT) becomes more intertwined with the power grid, vast public connections and resulting back doors will arise, yielding added opportunities for viruses to be introduced and run rampant [2].

Attackers have a gauntlet of methods for disrupting operational technology (OT) systems' nominal performance across the grid. Integrity attacks pose a noticeable threat to infrastructure given their ability to allow facilitated control systems to correct course nominally, resulting in possibly catastrophic damage to physical systems. Results like these commonly occur when compromised data pathways or actuators and sensors have their inputs manipulated while avoiding detection countermeasures [3]. Cyber-physical systems (CPS) have been adopted across the grid, leading to a corresponding increase in the vulnerability to this type of attack. Systems interfacing between software and hardware regularly is of the highest risk, but their defenses can be enhanced. Supervisory, control, and data acquisition (SCADA) devices are the most significant contributor of these OT CPSs to the grid. The increased ease in automation,



access to data, control over grid components, etc., have made the power sector much more efficient in recent years and laid the foundation for distributed power to take hold worldwide. However, this distribution of power generation and edge devices has led to numerous cracks within the defense architecture of the power sector, and typical defense strategies are rapidly becoming obsolete.

Various approaches can be deployed to combat these risen vulnerabilities. Response-oriented approaches to cybersecurity attacks on critical infrastructure such as the power grid are insufficient in our current world climate. A sit-and-wait approach holds the prospect of catastrophic societal effects given that this mindset could allow for one malicious party to cripple their enemy's energy sector. Resulting responses to such an aggressive move could include severe escalation from the defending party in retaliation or a complete dominance of the already hindered recipient of the attack. Blueprints for this sort of battle strategy have a great deal of a gray area and could lead to chaotic responses by world powers.

For this reason, proactive and dynamic defenses have the potential to combat attack schemes before the attacks are even understood. The robust enhancements introduced in this research are devised to avoid the results of future, unknown attacks rather than prevent already expected schemes. Operational technology enhancements to current grid systems and other critical infrastructure can bolster a robust framework to prevent future attacks in a scalable manner across industries and standards.

As optimistic as these hypothesized dynamic approaches and enhancements can appear under the ideal conditions, they require validation in research settings. If rolled out directly to the

field, deploying experimental changes to industry technology could house risks. For this reason, testing across a stable, isolated testbed that can simulate physical characteristics carries tremendous value to the research community to determine the benefits and limitations present. Avoiding the costs of failed security measures on real infrastructure, having the freedom to attack controlled defenses purposefully, and utilizing technology that is in use throughout the industry are just a few benefits of a testbed environment. The UCF RISES CPS testbed exemplifies these precise characteristics. Its interconnection across five UCF laboratories simulating individual parts of the grid is ideal for simulation and testing due to technology from Schweitzer Engineering Laboratories (SEL), Siemens, and other names synonymous with the highest standard in the industry building the backbone of the testbed. For simulating the critical mechanisms of the power grid, a testbed such as this is optimal for extrapolating adoptable standards to the industry and can integrate unique technological configurations.

In addition to having an integrated testbed, wise practices should be deployed across its hierarchy and within individual labs. Guidelines are proposed for proper monitoring and access nodes throughout the testbed that can be extrapolated into the power industry. Siemens' secure access management system CrossBow is deployed across the RISES testbed and offers several advantages to a system distributed across multiple physical locations. Resilient remote access and monitoring of the entire system while securing data points is the software's primary goal. The system must be pushed to its limits by testing proposed enhancements to the grid to warrant improvements to devices deployed throughout utilities such as CrossBow.

While defensive enhancements are crucial for future approaches to grid cybersecurity, they cannot be adopted once proven possible. Offensive tests against their validity will be used to

determine where limitations are present in the dynamic algorithms, the devices and standards deployed throughout the grid, and the flaws in the construction of the experiments. Vulnerability assessments of the entire system and penetration testing against enhanced systems can properly examine where the risks of introducing them to the industry may be hiding. Attackers will constantly evolve. Performing such analyses on behalf of proposed security measures and the orientation of the experiments seeks to bolster the mechanisms that may make this evolution futile.

One of the RISES Cluster's primary goals at its founding was the commercialization of the techniques researched within the cluster's confines. The OT enhancements proposed in this research can help usher in a safer future that can protect the lives of countless civilians and corporations alike. Future paths are outlined for experiments that can be executed across the testbed. If validated at scale, these improvements have the chance to reach their impactful goal and be adopted across not just the power sector but the world's critical infrastructure at large.

### 1.1 Critical Infrastructure

Current international reliance on electricity usage for nearly all factors of the modern-day human experience has placed the electrical grid as one of the most crucial foundations of society. This reliance continues to grow in importance as technology treks into more powerful innovations that require more and more energy. As this evolution occurs, the power grid is categorized as critical infrastructure. The United States' Cybersecurity & Infrastructure Security Agency (CISA) proposes that 16 sectors fall under critical infrastructure classification. These

sectors are deemed so valuable and worthy of protection by the U.S. that “their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.” [4] Sectors of similar importance classified as such by the CISA include communications, emergency responses, water/waste management, and financial services. This underlying trend of value across these sectors binds them to all be placed at the highest level of importance. As such, bolstering the protection of one sector can be scaled and yield benefits where commonalities exist.

One commonality amongst several forms of critical infrastructure is the presence of cyber-physical systems. CPSs constitute the backbone of the advancement in smart grid technologies. The fundamental concept of CPSs lies in the interconnection of computational, networking, and physical processes controlled by feedback loops delivering data to computational systems that constitute a change for the physical space and vice versa [5]. A specialization of CPSs stems from cooperative systems in which intelligent electronic devices (IEDs) communicate not only to and from a centralized location but also to one another. Systems such as these allow for quicker responses to changes in system dynamics and, most relevant to the research conducted within this thesis, seek to prevent the onset of attacks on the CPS. Many forms of critical infrastructure and industrial applications can be constructed with this sort of topology. Examples include cooperative drone systems for military defense or entertainment, self-driving vehicles, and smart cities. This research's primary applied focus on cooperative systems and OT enhancements is centered on the smart grid. However, the defenses proposed have the potential to be applied across a plethora of applications where conducive characteristics prevail.

Across the 2010s, security for critical infrastructure has been at the forefront of diplomatic concern for world powers, and for a valid reason. Hostile advisories have taken advantage of present vulnerabilities. Integrity attacks have been deployed across many battlegrounds, most notably within Iran's nuclear program. Dating back to an initial attack in June 2010, a malware virus named 'Stuxnet' plagued the Natanz nuclear plant in Iran by infecting Windows and Siemens software connected to the programmable logic controllers (PLC) of the industrial control systems wired to nuclear equipment at the plant. Centrifuges used to enrich uranium began to feedback inaccurate data, resulting in the centrifuges spinning out of control and yielding devastating damage to the facility [3]. This same type of attack was carried out as recently as 2021 at the same Iranian plant [6], showing that the vulnerabilities persisted even with widespread awareness of the issue.

In response to the initial Stuxnet attack, in October of 2012, then U.S. defense secretary Leon Panetta warned that future attacks on critical infrastructure could be realized through derailed trains, poisoned water supplies, and crippled power grids [3]. These warnings did not take long to come to fruition. Major power grid failures occurred throughout Ukraine [7] and India [8] in 2016 and 2021, respectively, due to hackers feeding unflagged false data readings into IEDs within their industrial control systems. In all of these cases, it is suspected that global adversaries carried out these attacks as a repercussion for disputes between nations. These case studies emphasize the impending danger for utilities if proper robust countermeasures are not implemented. Simply implementing a rudimentary layer of protection to wall off control systems from outside interference is no longer sufficient for utilities' approach to defense [6]. Industry

leaders in the power and cybersecurity sectors have noticed and invested in the future of protection within the various critical infrastructure constructs.

Even with this enhanced focus on added defense, recent escalations in global tensions now raise the question: are attacks like these rising in likelihood? As nuclear powers edge closer to the brink of war with ever-expanding proxy actions occurring tangentially to the Russian invasion of Ukraine, U.S. and NATO powers have also braced for likely attacks on critical infrastructure on their home fronts. In March 2022, U.S. President Joe Biden shined a light on this threat saying the White House has “evolving intelligence that the Russian government is exploring options for potential cyberattacks.” [9] Given these comments, national partners have begun to examine their grid parameters more tightly, with dire consequences weighing in the balance. Many states, such as Texas within the U.S., have been reprioritizing their efforts given the state’s heavy reliance on its energy sector [9]. Although there has been enhanced discussion in recent months, these threats did not appear overnight. Similar rhetoric was cast throughout the Trump administration and has been a focal point for the Department of Homeland Security dating back to the early 2010s. [10] This timeline correlates with two events: the mass digitalization of the grid and the increase in cases of integrity attacks, as discussed previously.

Although the warning of debilitating attacks on the grid alone poses an existential threat to society, the slippery slope that succeeds it is of a greater fear. Cyberwarfare is a realm in which the world is shockingly naïve to its consequences when escalated at scale. While the concept is widely discussed amongst the leaders in cyber defense, wide-scale attacks that expand beyond attacks on information technology (IT) systems – computer network-oriented systems - have yet to reach the borders of a country like the United States. Cybersecurity consultant

Jonathan Lancelot explains how in the presence of a cyberattack on critical infrastructure that endangers the population of a world power such as the U.S., Russia, or China, there is no framework for how a complementary world power should deploy a justified response. [11 Even more staggering is the concept of disrupted vital communications and inaccurate known state qualities being reported, leading to disproportional responses being executed. With a stage set in this manner, the deployment of unthinkable nuclear weapons enters the Rolodex of rational responses for a nuclear world power, and the slippery slope to the unthinkable veers its head. These worries do not warrant panic, but as the threat of integrity attacks is very legitimate and the technology to conduct them is being rapidly enhanced, defenses that stager the benefits of this development could be a saving grace in an uncertain future.

Antagonistic realities have been identified, and the apocalyptic narratives that can arise from their successes are incredibly daunting. While these have become the most apparent, the cybersecurity and power industries have developed preliminary defenses that protect systems from advancing attacks. Those standards have arisen through the advancements made within centralized control and automation of a large slate of the power grid. These developments have significantly improved the functionality of the energy sector, yet they have to be monitored against the threat of new attacks.

## 1.2 Power System Control Center

In the early 20<sup>th</sup> century, the rising popularity of the power grid brought about a need to protect the expensive equipment deployed in delivering power to countless residents and

businesses. Through their evolution in the last quarter of the century, microprocessor relays were introduced in 1986 and were widely adopted for measuring state variables across transmission lines, substations, and generators into the 21<sup>st</sup> century. [12] Rapid responses to shortcomings in performance continue to be the industry's focus as every minor inefficiency can cascade into significant financial losses or nontrivial loss of services. SCADA systems have been widely adopted and integrated across all modern power devices since their standardization in 1996 for embedded process control and automation of systems [13]. SCADA devices introduced superior control over the existing power infrastructure in data communication and presentation, sensory measurements, remote access, and PLCs [14], leading the power industry to the cutting edge of CPSs and enhancing nearly all aspects of the industry. This shift has led to the entire industries based around the products that enable this level of control and monitoring to spring up, such as companies like SEL and Siemens that produce the broadest range of SCADA products. The SCADA market space is expected to continue to grow as renewable energy dominates the new sources penetrating the power grid.

Grid characteristics and designs have faced a significant shift in their orientation due to a core factor. Traditionally, the grid was constructed with the concept of centralized control at its core. Revolving around various



**Figure 1. ISO New England Power Grid Monitoring Room [15]**

utilities working with one another, suppliers deliver power through coordinated power plant operations to ensure reliable responses to demand [16]. This format resulted in consumers not



relying on one supplier to meet, or possibly miss on, power demand. Centralized grid control would not be possible without control centers like those seen in Figure 1 that examine the current demand and responses being made across the grid. Through a proper examination of the desired power across a region, generators can increase or decrease their output to match the current needs of the populous.

Even though the centralized distribution of power has dominated the sector for its over hundred-year existence, the trajectory of the future grid paints an alternative picture. The U.S. Department of Energy's (DOE's) National Renewable Energy Laboratory (NREL) has examined how concepts like "Autonomous Energy Grids" built around intelligent energy devices, renewables, and advanced controls are poised to alter the industry to be much more decentralized. [17] The future of the grid then transitions to have more generating bodies at endpoints that send power back into the grid and event to utilities, straying from the utility to user model that has stood tall. These factors build the case for the necessity of smart grid technology to enhance the overall operation of the grid. Once again, these factors introduce many problems that require rigorous examination and understanding of how they affect power distribution.

### 1.3 Power Grid Cybersecurity

Transitioning to a standardized adoption of SCADA technologies, a grid decentralization, and subsequent adoption of cooperative system characteristics have occurred within the early 21<sup>st</sup> century. International goals to curb greenhouse emissions have been proposed, and the

improvements to energy usage and the development of more sustainable energy sources are greatly enhanced by these digitalized technologies. While they bring about added utility to the systems they augment, IoT approaches increase the probability of damaging attacks drastically to their hosted systems. According to the *MIT Technology Review*, the research done by Gartner, Inc. estimated the inclusion of over 11 billion IoT-connected devices in the year 2018, which the MIT group said creates a “cybersecurity nightmare” [18]. Billions of new devices ranging from integral line relays in the power grid to a simple thermostat in a cooperating building will continue to be added and interface with one another. Expanding on these data points could show that one simple weak link in this system can open a cybersecurity back door from a simple toaster to a substation that powers Manhattan, leading to a setting ripe for an integrity attack to enter into focus.

NREL and the National Institute of Standards and Technology (NIST) have published studies on the current state of the cybersecurity industry regarding the power sector and smart grids. According to the NREL study outlining the building blocks for the power sector's security mainframe, many standards have been developed that lay a deep foundation for corporations to build off for hardening their networks. However, the study states that many public and private organizations struggle to develop a balanced program that protects all areas of their assets from attacks.

With a system's weakest link having the possibility to cascade across an entire network of devices, approaches that do not cover every base are an issue. NREL outlines a baseline of building blocks that utilities should utilize as a roadmap for a foundational defense of their technology. Various building blocks are introduced, including governance over cybersecurity

efforts as a leading operating body within an organization. Policy and management hierarchies expand on this leading body by delivering a response-oriented technical framework consisting of technical controls, awareness training, and responses and research toward improving defense. A solid response-oriented structure to expand the foundation of defenses is a necessary first step to achieving more dynamic responses to ever more complex attacks. Following a structure such as the one proposed can lead to an optimal starting point [19].

NIST examined a more specialized scope of security yet arrived at a similar outcome. The study found that, even though a currently deployed framework for protecting the smart grid yielded strong protection, the bulk of security practices applicable to current domains may become obsolete when new interfaces develop [20]. A consistent worry when new technology arises is that there will be new attack vectors that have not seen the open world of flowing hackers, leaving little methodology for sealing the holes yet to be brought to the surface of the technology.

Regarding new technologies, companies try their best to seal any holes they may be bringing into the framework of a system. From the corporations' point of view, introducing an entry point for attackers across an entire line of products would be devastating for their public image and very likely would drastically hurt company trust and future profits. With this in mind, the best in the energy sector deploy comprehensive examinations of their equipment and propose measures for their customers that allows for minimal vulnerabilities when their equipment is integrated into a larger network. For example, Eaton, a multinational power management company, described their approach for a sound cyber defense strategy involving properly secured devices and the proper software layer to manage them as the threat of cyberattacks is consistently

escalating. Some of their deployed mechanisms include UPS gigabit network cards for stronger encryption, physically and software locked device access, required usage of multiple digital certificates, and turning off unused access points to prevent unauthorized access [21]. In distributing user manuals, companies often include practical measures clients can take to enhance the security of their deployed devices and send downloadable patches over the internet for existing issues.

The industrial baseline precautions commonly deployed can be valuable but are sometimes not enough to ward off attacks. In April of 2021, one of the most significant data breaches in recent memory fell into the lap of the information technology firm SolarWinds. Russian sponsored hackers infiltrated the company's corporate system and embedded their software, called Orion, with malicious code that attached itself to updates sent out within patches to corporate and organizational customers of SolarWinds. This malware then secreted itself as a backdoor within up to 18,000 infiltrated customers [22]. Attacks like this put the information of numerous users at risk through a mechanism that is very much at the edge of user interaction and end up ruining the developer's reputation for years.

This subtle form of attack is not the only one present within this space. Cisco's encompassing report on cyber attacks outlines the broad scope of the issues at large. The company lays out the wide range of the problem, with Cisco's CEO John Chambers going as far as saying, "There are two types of companies: those that have been hacked, and those who don't yet know they have been hacked." With their cited statistic of 53% of cyber attacks resulting in damages of \$500,000 or more, it is no wonder the company makes such an emphatic statement. Within their report, they link the most common IT cyber-attacks to the following: malware (as

discussed regarding SolarWinds), phishing – fraudulent communications to victimize the recipient, denial-of-service attacks – forcing systems to be inept at responding to access requests, man-in-the-middle attacks – intercepting data through communication transactions, and SQL injections – inserting malicious code into servers to reveal sensitive data [23]. Although there are countless combinations of attack vectors and methods for at-risk clients to be aware of, the precautions proposed by companies such as using VPNs, advanced firewalls, and additional precautions can limit the probability of a successful attack on fully digital devices.

#### 1.4 Vulnerability Analysis

Understanding the weaknesses of a system is a crucial step needed to improve the security in place within said system. Proper examinations of possible vulnerabilities begin with understanding the issues that may exist and their causes. Corporations attempt to be as robust as possible against issues to their product. Even with the immense pressure and the vigorous testing that goes into validating product lines, companies can tunnel-vision and miss vulnerabilities they are not mindful of. Within this research, the focus will be on four sources of vulnerability: shortcomings in industry-designed equipment, experimental setup errors, client access backdoors, and the limitations of the experimental applications for security measures.

While very impressive in their scale, Sprawling OT systems are limited to their weakest link. In the case of industrial equipment, a testbed environment seeks to examine both each individual deployed device within a system and how they interface with one another as a collective. Turning over every stone on proposed practices, system setups, communications, etc.,

can expose unforeseen limitations of specific industry devices. This concept goes hand in hand with possible errors in the playground of experimentation, i.e., a testbed. If the battleground for assessing the security of experimental enhancements is inherently flawed, then meaningful results for experiments are impossible to be drawn upon. In cases where wide-spanning networks are deployed that touch various disciplines, departments, and personnel, the likelihood of an error or miscalculation of setup orientation is relatively high and increases with more hands within a system. This relates to both the case of a testing environment and wider real-world deployment. As discussed previously, administrative governing bodies have their value in this regard to security, as they standardize practices and check on the activities of individual branches.

Once a system and its components are deemed robust, access to users becomes a top priority and balances several factors. Organizations seek to give ease of access to approved users while keeping all data points secured against unauthorized individuals or actions. Client portals are a weakness that has many moving parts and can be a challenge to stay on top of and robustly respond to. Additionally, the blurred lines between the work and home environments during the COVID-19 pandemic create even more significant concerns. Drastic increases in personal web searching on company interfaces led to a 54% increase in companywide phishing, a 56% increase in web browser-related infections, a 44% increase in compromised devices infecting broader business operations, and a 45% in utilizing devices such as wireless printers as attack vectors [24]. To avoid the shortcomings of cyber integrity and the prioritization of client-based goals, optimal solutions lie with adequate separation of user access from broader company networks. Upon properly assessing these foundational vulnerabilities within a setting, the

validity of experimental designs can be examined. Without this proper initial framework, issues may arise at later stages to confound results, leading to possible misinformed conclusions and months to years of misguided workflow.

Penetration testing can be deployed to examine an entire network or subsystem properly. “White hat” hackers, or champions of cybersecurity enhancement, often assist organizations in protecting their systems from cybercriminal “black hat” hackers [25]. These tests can be done through typical baseline friendly attacks and more system specialized attacks conducted by focused experts. Examining the previously stated vulnerabilities is a prerequisite for testing proposed experiments for any new system. Given a network with ideal standard threshold constraints for security, examining the methods proposed now removes many confounding variables.

For this reason, emphasis is put on examining control group setups for experiments to determine if fundamental flaws persist in the face of attacks that trivial responses are understood for. This baseline allows for meaningful conclusions and data to be drawn from the deployment of altered settings. Once preliminary security is in place, the proposed experiments seek to validate hypothesized results performed via simulation. If these base cases are proven correct, the next step is to continue with additional confounding variables in attacks. This can take the form of more attacks on a single node or overall system, different orientations of attacks, or expanding the experimental setup to continue testing the disadvantage of a defensive framework. These gradual steps can quantify the known uses and robustness of these setups and allow future research to be proposed. Additionally, combinations of varying mechanisms can be deployed to examine further their viability for industry adoption, the primary goal of this research.

### 1.5 Distributed Cooperative Control for Grid Edge

Decentralization of the grid has led to power-related IEDs encompassing many points of urban and generation-rich areas alike. The evolved orientation allows grid-edge devices to have a more valuable role within the grid that lies outside of simply improving profit and efficiency. The concept of cooperative systems is introduced in which a distributed control methodology is networked across many devices and only requires the exchange of local information among the system's agents. This type of orientation has been previously applied through various neural network problems and within smart grid technologies [26]. Having more vectors within a system can shift the number of vulnerabilities to assets within a system by both detecting attacks and being resilient to them. The integrity attacks previously introduced seek to ride into a system undetected. Cooperative system OT approaches are ideally able to snuff out various forms of these attacks prior to them taking root and dislodging normal operations of a system. By enhancing these end devices and maintaining a centralized control center, the grid can edge toward the utopian smart grid construct frequently envisioned.

Within the realm of critical infrastructure and technological advancements, several applied areas are ripe for deploying cooperative systems to bolster both control and the sanctity of operation in the manner described. As previously mentioned, self-driving cars and cooperative drone sets are rampant with IDEs. Additional technology conglomerations that share this potential to function as cooperative systems include collaborative robot cells, surveillance mechanisms, communication technology, and satellite apparatuses. Given that the characteristics of cooperative systems are transferable in this manner, it bodes well that the security measures they can deploy within the smart grid can be transferred to these other industries in a robust



sense. Chapter 2 outlines two cooperative system approaches, and the transferable practices are apparent. With a focus on device nodes, communication methodology, and OT characteristics, cooperative system orientations can both be scaled and applied throughout numerous industries.

### 1.6 Industry Adoption

Standards for industry adoption and recognition of necessary improvements require research, validation, and hardline conclusions. What is proposed within this research can potentially improve the lives of billions without them even being aware of the change. For that change to occur, it is required to examine the typical steps for industry partners to adopt practices and enhancements to existing technology. Meaningful experimental results are the foundation upon which any industry change extends. Proving a hypothesis to be correct is not the only desired goal. Gathering results of any kind goes leaps and bounds and can alter the progress of an industry in a more accurate direction. Positive or negative results can guide the future of experiments in a field and deliver a comprehensive understanding of the technology and industry. Whether it be examining a different approach for an algorithm or throwing the next gauntlet of test cases into the queue to be examined, future testing can disprove previous results or progress designs closer to the threshold of industry adoption. When it comes to crossing into that frontier, industries conduct thorough and redundant examinations, and for a good reason. Hasty decisions are rewarded infrequently, while rigorous analysis yields results that are worthy of attention, praise, and eventual adoption.

While success can be viewed through a spectrum of results, industry adoption can take several paths or varying extremes. In the realm of technology, innovation occurs rapidly, leading to big booms and busts for companies. If certain practices are not adequately vetted, they could cause cascading negatives from minor errors overlooked within that evolutionary process. As discussed in the Harvard Business Journal, the rate of change in the industry will dictate the pace at which a company must correspondingly adapt and leave old business models behind. However, too rapid change can lead to misreading clues and false conclusions. For this reason, companies analyze the consensus of the industry at large and calculate economic, technological, and statistical variables for how to respond to innovations, adapting in ways ranging from radical – extreme and rapid, progressive – gradual and with reason, creative, to intermediate – infrequent and required [27].

In the realm of cybersecurity, especially the security of critical infrastructure, many possibilities are being examined to adapt to changing times. Utilities do not want to face the consequence of a failure to evolve that leaves millions of customers in the dark or their bottom line out millions for repairs due to critical damage done to equipment. For this reason, it is reasonable to expect rapid adoption and change within the energy sector as solutions to cybersecurity issues continue to progress. While this is to be expected, verified robustness must be a trait of most new practices at the forefront of the innovation, and a process of validation reflects closer to the concept of progressive, gradual adoptions. Unproven, experimental practices could leave the industry more vulnerable than before, leading to a rational skepticism toward new practices. As they are universally verified and tested by independent sources, the likelihood of maneuvering toward integrating new practices will increase. However, this pace is

weighed against the rapid growth of cyberattacks. Good practices could avoid a self instilled problem for industry technology but may cause these sectors to fall behind their malicious adversaries. This being the case, lab studies like what is proposed within this research are imperative for the growth of the industry's defenses. Many test cases can be subjected to devices in rapid sequence, accelerating timelines in meaningful manners and leading to an enhanced understanding of enhanced defenses.

## **2. ENHANCED OPERATIONAL TECHNOLOGY SYSTEM DEFENSES**

The state of the energy sector has been introduced along with its vulnerabilities, standard practices, and widely adopted systems. Static responses can only go so far in protecting against attacks. Dynamic responses to grid environments have been proposed in different forms and become more viable with the increase in the adoption of smart grid technologies. OT and cooperative system and their expanding uses open the door for the next stage of defenses that can realize evolving countermeasures against expanding weaknesses. Three approaches that have the potential to enhance the security of the grid against attacks are proposed. These, when used in conjunction with one another and the previously introduced baseline mechanics, have the potential to minimize the scope of attack vectors for assailants. The following chapter outlines the initial state of various grid subsystems, the enhancements that can improve their operation, and the hypothesized deliverable results for each.

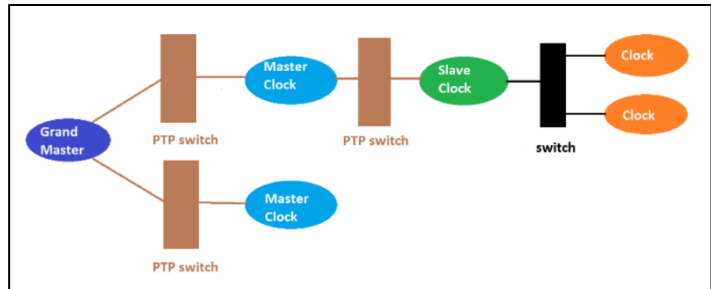
### 2.1 Cooperative Network Precision Timing Protocol

Electricity travels at near-instantaneous speeds, meaning precise timing across the electrical grid is imperative to optimal performance. Phasor analysis and synchronization of phasors are some of the subsequent applications that require a near-perfect understanding of instantaneous state values of systems. This practice allows for separated power systems/devices to be merged based on matching the time varied waveforms of alternating AC delivered power. Phasor measurement units (PMU) are required to measure time delays based on the distance signals must travel and then actively shift the phase to a corresponding value of the interfaced

device. This shift is frequently deployed in the emerging microgrid specialty of power engineering as it allows for devices to be removed and then resynchronized from larger parts of the grid. In order to execute on tight time constraints, two commonly used communication protocols seek to give universally accurate device times throughout a distributed system of devices in Network Timing Protocol (NTP) and Precision Timing Protocol (PTP). NTP is the industry standard for computer networks whose time requirements are not stringent – within 100 milliseconds. NTP deploys a unidirectional synchronization where a time is deployed from a centralized source to many devices, and the expected transmission delay is calculated using estimates of communication distances. PTP, on the other hand, is deployed for systems with greater time sensitivity. Portions of the power grid considered crucial are the perfect network for it to be deployed throughout. Its main advantage over NTP comes from its calculation of time delays based on bidirectional communication and analysis of the delays endured through the transmission of signals between a master clock and slave clocks. [28]

PTP has been widely adopted and is a standard industry protocol, but it has an underlying vulnerability to attacks on the timing packets delivered by the source clock. Usually from satellite communications with atomic clocks being used as a grandmaster source, there are chances for data to be disrupted and altered to inaccurate states. Data disruption can be less of an issue to systems, given that most relays and PMUs will raise error flags. In contrast, spoofed data with inaccurate information could lead to what seems like nominal operation with inaccurate timing, leading to unstable control states. An analysis of GPS signal spoofing done by the PNNL

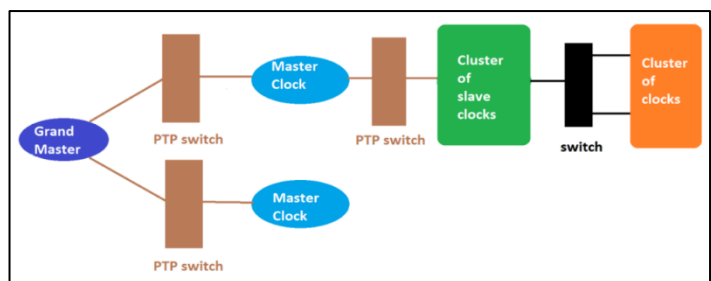
saw a drastic shift in accurate times across devices polling from these satellite interfaces and a corresponding drastic shift in phase correlation between devices. [29] PTP deployment via



**Figure 2. Typical PTP Topology [28]**

ethernet has allowed the protocol to be scaled across various industries requiring instantaneous response and time synchronization. One issue recognized with standard PTP topologies, shown in Figure 2, lies within scalability at a large number of IEDs introduced due to physical transmission distance between the master clock and devices and the router queue selection process for selecting device synchronization order. Previous research conducted at UCF has determined that by scaling up the quantity of PMUs and control systems, the current PTP standards will not suffice if sub-microsecond synchronization is desired [28].

An augmentation to the typical protocol is proposed to resolve these limitations in scalability and the security of PTP. A distributed algorithm convention utilizes clusters of IEDs to cooperate with one another rather than only with the master clock devices. Several benefits present themselves. Geographical clusters face lesser delays and can match frequency, phase, and times with limited jitter, even with just standard ethernet protocols. Each cluster of devices can utilize physical equations and OCXO-based crystal clocks to extrapolate sub-microsecond accurate time for hours through propagation between devices via non-PTP protocols.



**Figure 3. Typical CN-PTP Topology [28]**

With isolated clock maintenance in mind, devices can maintain accurate times while insulated from external communications, even if a system is isolated from synchronizing signals for hours. Through this distributed consensus algorithm termed “cooperative network precision timing protocol” (CN-PTP), systems are robust against variable delays within a cluster primarily by using standard technology and standards built into system topologies.

With this cooperatively controlled outlook on PTP in place, the performance-optimizing design in conjunction with several common communication methods can instill superior security measures against attacks on the integrity of a system’s time state. Two security loopholes can be closed. First, if a master clock is disconnected from a cluster, the time that has been established between devices remains within the cluster and is kept relatively constant for several hours of run time, keeping time, phase, and frequency within desired constraints. Secondly, if an integrity attack occurs, feeding in false times that drastically alter the previously defined state, clusters can observe this alteration and respond accordingly. This latter scenario could even intentionally isolate communications from higher-level devices orientations due to likely security breaches. A similar cooperative communication method is discussed in Section 2.3 and is defined as a distributed consensus algorithm. This enhancement refers to local area devices establishing proper state variable understandings and then being able to respond to items that have been given false data that changes to improbable values. Implementing these methods in conjunction could bring a robust defense that would bolster specific systems.

## 2.2 Resilient Control from Embedded Dynamic Encoding & Decoding

Integrity attacks spanning from introduced data within communication channels are a very susceptible vector for attacks and are a fundamental threat to industrial systems. If data can be replaced with little to no awareness within a network, this can cause inputted data to be seen as standard communications. At the same time, it could be a malignant implant from an adversarial campaign or have sampled in signals with malware. These attacks can be achieved through a stealthy attack driving the physical systems to an unsafe state behavior similar to that of those attacks discussed in the case studies against critical infrastructure described in Chapter

1. Within Figure 2, it is seen that the standard industrial control system detects attacks employing output-measurement residual-based detection within a control loop. This detection

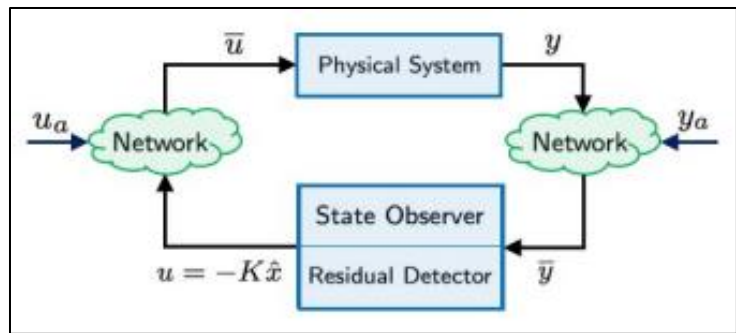


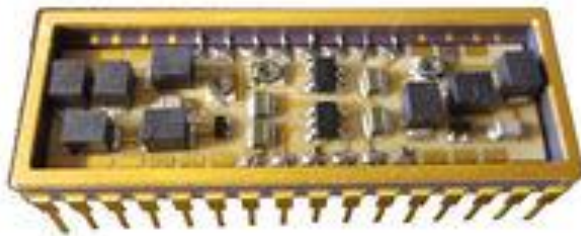
Figure 4. Standard CPS Networked Control System [3]

occurs using physically accurate electromagnetic models and comparing their accuracy with the data received from network inputs.

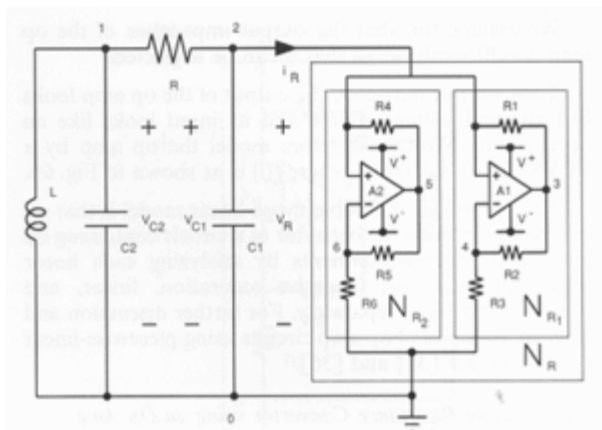
For this reason, when unstealthily attacks enter into a control loop, they are swiftly snuffed out by residual detection due to these attacks pushing the physical bounds of the state observer to unrealistic and irrational extremes. A pressing threat against this defense is when the construct of a system is well known by an attacker, allowing a stealthy attack to slip under the gaze of grid protection and wreak its havoc. Given the case through physically bugging systems or a personnel leak from the operational organization, legitimate threats are present in this form of attack.



Previous UCF research proposes a scheme where the attacker has full knowledge of a system and has gained access to the communication network sending data between end devices within a control system but does not have knowledge of current information for the data input, plant state, or other real-time information. These attacks are considered stealthy, meaning that the control system's residual feedback does not detect the presence of the attack in the standard feedback system described. The developed research concludes that this hypothetical perfect stealthy attack strategy allows the assailant to go undetected for the attack to result in changes to the steady-state value and manipulate the dynamic response of the physical plant. Figure 4 displays the plant system under attack with traditional defenses and a state observer monitoring the system. [3]

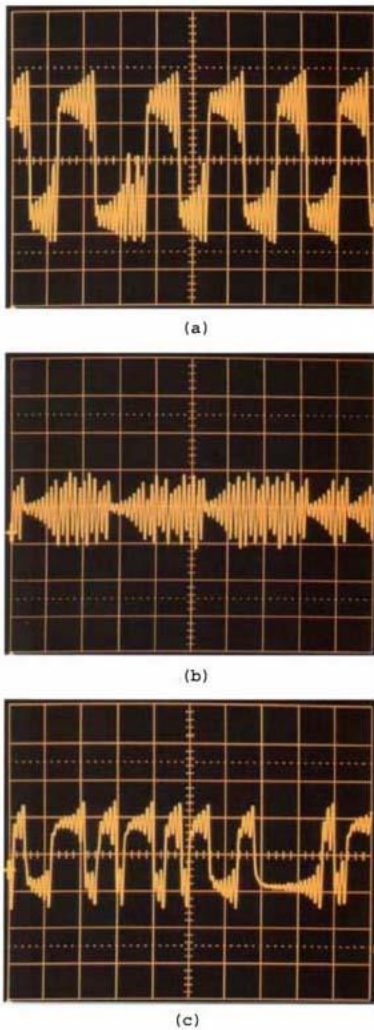


**Figure 5. Example of a Transistor Based Chaotic Circuit. [30]**

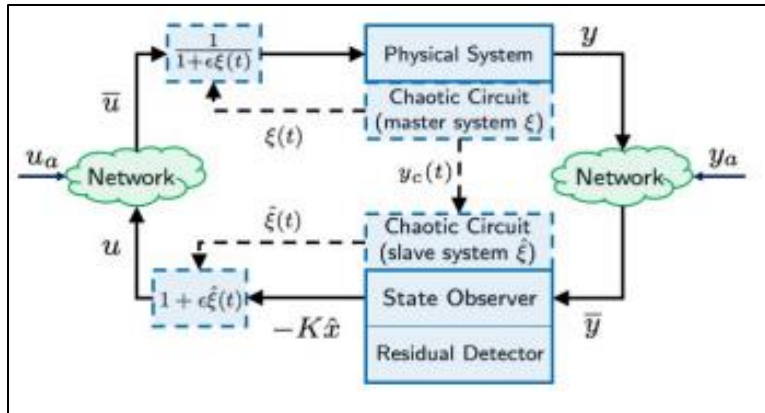


**Figure 6. Chua Circuit Realized using Op Amps and Resistors to Implement Chua Diode [30]**

Resilient control can be maintained over an OT system under such attack by implementing embedded nonlinear circuits to encode output transmission signals and utilizing a complementary designed circuit to decode such a signal. A process like this would use internal nonlinear circuitry in the form of chaotic oscillators within each IED to produce a signal that would be impossible for a user to replicate without real-time knowledge of the system and that can then be decoded at the destination site undisturbed. Chaotic circuits



**Figure 7. Chua Circuit Chaotic Waveform Output Examples [30]**



**Figure 8. Enhanced CPS Control System with Embedded Nonlinear Components [3]**

can be simulated by applying a nonlinear mathematical transfer function in software like MATLAB. To realize this function in the physical realm, such a circuit could be created utilizing transistors that autonomously output a distorted signal when a signal passes through its system. Circuits like this tend to be structurally dynamic and straightforward and utilize the nonlinear behavior standard within the saturation region of BJTs [30]. Secondly, previous research references Chua's chaotic oscillator as a separate candidate for

implementation. Chua's circuit is a classic example of a chaotic circuit. It is deemed the simplest electronic circuit exhibiting behavior such as bifurcation, or dynamic outputs produced by varying parameters [30]. Figure 6 shows one orientation of this circuit. Suppose signals are encrypted in this chaotic analog manner. In that case, it is very challenging for the attacker within the constructs of their knowledge of the system to comprehend and react accordingly to the hurdle they now face to attack. For instance, the waveforms in Figure 7 showcase several

outputs that occur based on altered voltages across the Chua circuit from Figure 6. Given the variability of these waveforms, the defense of the state machine is now bolstered in response to many possible attacks. As the signal encryption is up to probabilistic constraints to determine how the information will be transmitted, even an intelligent neural network AI would find it near impossible to implement a stealthy integrity attack. On the other hand, the state observer has several possible responses to recognized attacks. Signals determined to be spoofed can just be discarded, or the system can determine specific incoming signals as attack vectors and respond accordingly. Figure 8 shows the diagram of the original plant with added chaotic circuits to the system diagram, which introduces new transfer function outputs to the data transmission in a manner that encodes at the source and decodes at the destination. Note that these functions are inverse of one another.

UCF CPS simulations performed previously compared results for four different attack scenarios: absence of an attack, an uncoordinated data attack, a coordinated attack with an unstable response, a coordinated data attack with a stable response (altered variable values rather than an exponential increase in variables), and an attack with the proposed protection scheme. This data determined the hypothesis of the proposed enhancements to be accurate. The system snuffs out the false data points under the influence of no attack or an unstealthy attack, but stealthy attacks sneak through securities. On the other hand, the residual detection was triggered when the above protection enhancement was deployed, giving validity to the proposed design.

### 2.3 Competitive Interaction for Distributed Consensus

While the control over an extensive network of devices can be challenging to maintain, many benefits can arise. Smart grid landscapes at scale include hundreds to thousands of device nodes across a distributed network. While they have been described as vulnerabilities, each node can interact with one another in a cooperative system manner. In addition, a mirrored, hidden network of virtually

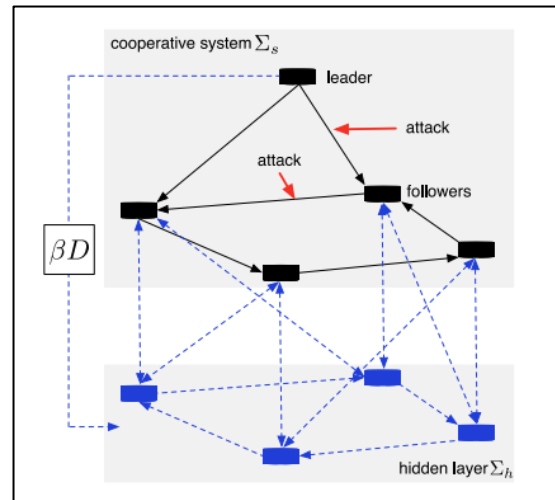
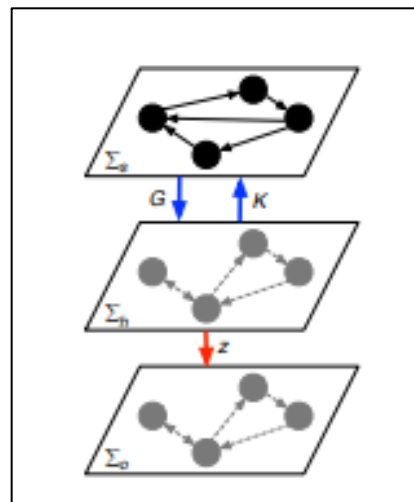


Figure 9. Interconnection of the cooperative system with the hidden network [6]

replicated devices is created to combat a leader-follower consensus problem presented in previous UCF research. Suppose some follower agents within a system stray from nominal behavior due to exterior influence. Designated attackers could inject nonlinear or linear dynamics into this network node to corrupt commands and communication between the devices, intercept communications, or corrupt state estimates of the device via interconnection for integrity attacks. The goal of the virtual network is to maintain the overall system stability against drastic changes in the original consensus network. [6] Standard system responses may be limited in their ability to respond based on the orientation of device communications, knowledge of the attack constraints – a factor of high priority for robust responses to attacks, or interactions directly with the physical network. The competitive interaction design for distributed consensus seeks to avoid these limitations and robustly respond without directly affecting the physical network, even if the hidden network is breached and attacked. [6]

A method for developing a hidden layer must be introduced to achieve the setup described by this proposed orientation. A hidden layer of digital devices can be accomplished by communicating with internal signal components among every physical network node, a common trait of most SCADA systems. This characteristic refers to building a digital clone local to the physical device rather than having it stored externally. An alternative to this approach would be replicating the states of each node through cloud-based,

software-defined networking. The software-defined variables have no physical meaning in this scheme and are not subject to meaningful attacks. This being the case, they will most likely be protected from the scope of the attackers or at least would not yield valuable information to adversaries. Additional hidden layers on top of one another, as shown in Figure 10, can further bolster the framework of enhanced security provided by the digital clones. Even



**Figure 10. Three-layer Cooperative System Networked Model [6]**

though the number of computation nodes has increased by approximately 50%, the computational bandwidth introduced is simplistic and leads to trivial increases in operational performance, while the momentum of the system's security is meaningfully improved. Communication expenses are also limited since the virtual nodes have no physical space and can be performed using standard network protocols. [6]

This cooperative system enhanced approach proposes a subsistent increase in the number of nodes within a CPS network to increase the system's momentum against alterations in state variables of devices. Through simulation-backed data within UCF research, it is shown that

offensive and common attacks that result in debilitating or disrupting of nodes and system stability will be handled accordingly. Across several test cases, networks that included this distributed algorithm would approach a steady-state compared to control groups under attack with just a physical distributed network formation. These results bolster the hypothetical design of this OT enhancement and are a simple programming-based implementation that can lead to specialized responses to varying scenarios.

### **3. CYBER-PHYSICAL SECURITY TESTBED**

The UCF RISES CPS testbed developed across five of the university's labs exemplifies the ideal characteristics found across the newest technology in sustainable energy. Utilizing Siemens' RuggedCom CrossBow interface, the testbed has connected these previously separate labs to interface with one another and be accessed from varying locations. This chapter dives into the orientation of the RISES testbed, the good practices to be deployed across it, and guidelines oriented around the expansion and future use of the system. As the cornerstones of the grid are integrated, so are devices and configurations most applicable to each enhanced OT mechanism discussed in Chapter 2.

Extensive validation of the enhanced mechanisms is required prior to wide-scale adoption throughout the power industry. Experimental applications are simplified and streamlined using testbeds like the one located across RISES. While the digital smart grid enhancements have opened a wide range of vulnerabilities, the benefits of this transition shine brightly in the research community's ability to examine real-world grid characteristics while not disrupting nominal operations and delivery to consumers.

#### **3.1 UCF RISES CPS Testbed**

Cyber-physical testbeds yield many practical advantages to research scenarios. As discussed earlier, the ability to conduct experiments, especially in examining a system's vulnerabilities, is invaluable to researcher findings due to the ability to intentionally attack and possibly disable devices that would otherwise be interacting with critical infrastructure.

Performing these tasks with industry-grade technology that behaves as if connected to the power grid will emulate real-world applications of the proposed algorithms and general vulnerability testing. Since its founding in 2015, the University of Central Florida's Resilient, Intelligent and Sustainable Energy Systems Faculty Cluster has brought together educators and researchers across all 16 disciplines at the university for a common goal: developing cutting-edge advancements in the energy sector for positive worldwide impacts. [31] Sponsored research funded by federal agencies such as the Department of Energy and industry partners such as Siemens, General Electric, and Florida Power and Light creates a clear path for commercialization. By working with the conglomerates that would most benefit from the deployed tactics of the lab and utilizing their technology in the process, RISES bolsters commercial connections amongst entities as the cluster uses practices deployed across these factions in a manner that ideally portrays the best solution of all the technologies. The RISES testbed has the potential to be a breeding ground for innovation and collaboration for these partners.

One of the major objectives of the RISES Cluster is to enhance the apparent cybersecurity of the cutting-edge sustainable energy technologies being deployed across the world. The RISES CPS testbed emulates the spectrum of devices commonly seen within the power grid ranging from generation, transmission, and delivery to the digital controls that continue to enhance efficiency and safety. The variety of labs that have been developed since the cluster's founding have been conducting isolated research on their focused disciplines. Developing an interconnected testbed across the current five labs included bridges the setup to the next frontier of discoveries that can be made based on realistic commercial network



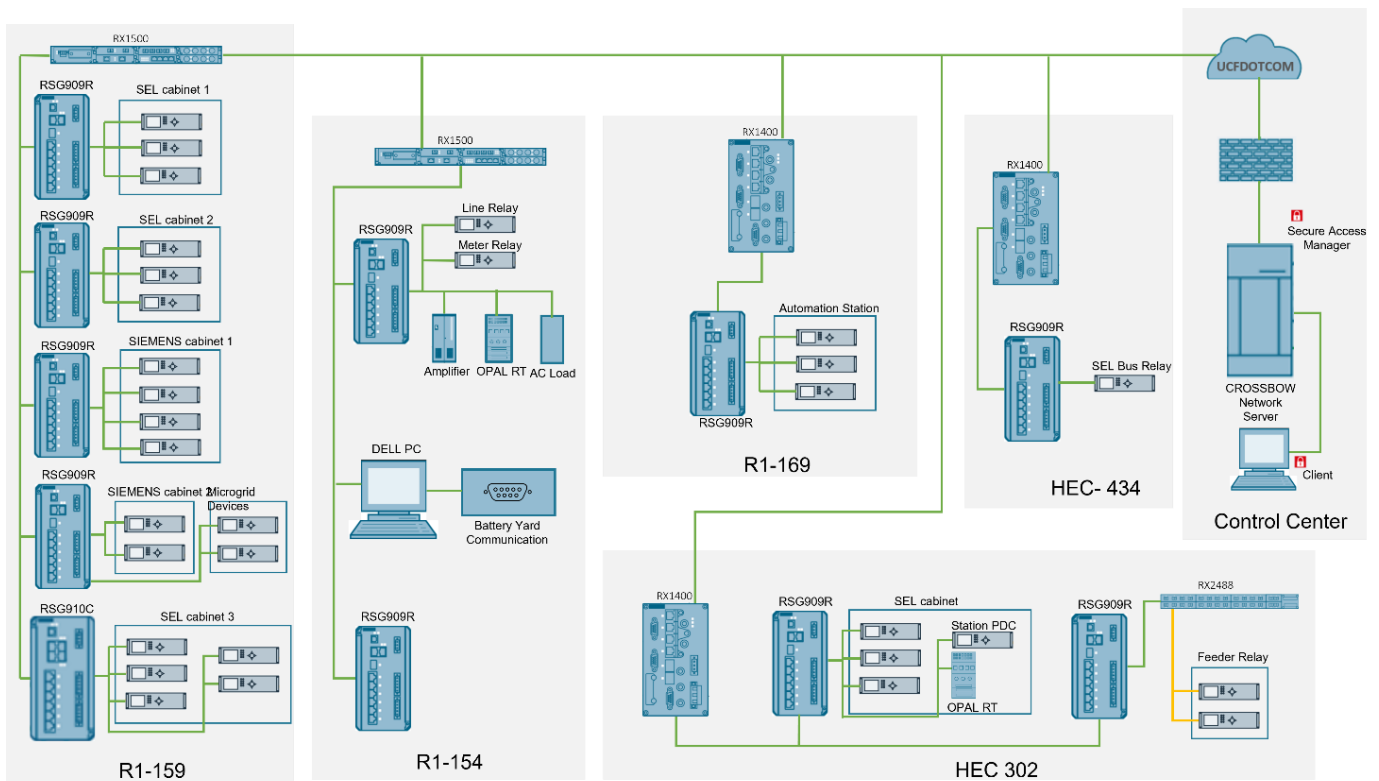
orientations. Through the centralized interconnection of all devices across these labs using Siemens RuggedCom routers and switches conjoined via computer networks, UCF now has a web of devices that emulate the grid at a similar scale seen across research at the U.S. National Laboratories. As shown in Figure 11, the current testbed setup ranges into five lab spaces of different purposes with varying technology across them. Figures 12-17 show the wiring diagrams of each laboratory, showcasing the technology across them. The following is a list of each lab and their corresponding grid characteristics.

- **Microgrid Control Laboratory (R1 154):** No subsection of the power grid has garnered more growth from the onset of the smart grid transition than microgrid technologies. Microgrids behave similarly to the overall grid. This subsection can control local energy, break off and operate on its own using local generation, and operate nominally while connected to the grid. Renewables like wind and solar combined energy storage and digital controls have allowed microgrids to become popularized for segments of the grid that require power in case of emergencies (military bases, emergency response, etc.) [32]. The UCF microgrid lab emulates these same standards. With simulated loads, generators, a battery testing yard, real-time simulation, and the devices to connect it all, the lab aims to test large-scale distribution networks' safe, reliable, efficient, and secure operation.
- **Smart Protection and Control Laboratory (R1 159):** The Smart Protections and Control Lab at UCF has nearly 20 of the industry's highest quality devices as shown in Figure 13, and deploys them for valuable research on their responses to simulating the interconnections that allow for the grid to run smoothly in its power outputs. The lab best models transmission

line junctions and substation behavior using the numerous protections needed within these systems and allows for simulated results on the backbone of the centralized grid model.

- **Smart Infrastructure Data Analytics Laboratory (R1 163):** For the smart grid to reach its highest potential, the end devices and infrastructure the power is fed into should be equally enhanced. The UCF Smart Infrastructure Data Analytics Lab examines challenges for grid edge components. It is devoted to improving the energy efficiency, building intelligence, and customer engagement deployed when developing smart cities [33]. Efficient energy usage boils down from the large electric machinery to the subsystems controlling building temperature. As previously discussed, bolstering the protection of these IoT devices and their connections allow for one vulnerability to not cascade into a spiraling disaster.
- **Siemens Digital Grid Laboratory (HEC 302):** With the smart grid at the center of the RISES research, the Siemens Digital Grid Lab emulates portions of the grid that complement those within the Microgrid Lab for an encompassing field of digital controls for high penetrating renewables [34]. Precision time devices such as PMUs, satellite clocks, and the ability for added devices by using OPAL real-time simulations are a focus within this lab. While the Microgrid Control Lab is centered on the physical components making up a microgrid, this lab focuses on the devices making the technology scalable and more efficient.
- **Cyber-Physical Systems & Control Laboratory (HEC 434):** Centralized & decentralized power distribution is often built around a centralized control infrastructure. The RISES CPS testbed houses its CrossBow controlled server within this lab, which focuses on cooperative control for distributed power generation and delivery. Being a controlled space, the lab houses special security measures to protect the data of all devices and requires adequate

testing to ensure this is the case. It additionally presents visual representations of the testbed at large, as shown in Figure 18, for demonstration and monitoring purposes for technicians, engineers, and analysts.



**Figure 11. UCF RISES CPS Testbed Overall Scope**

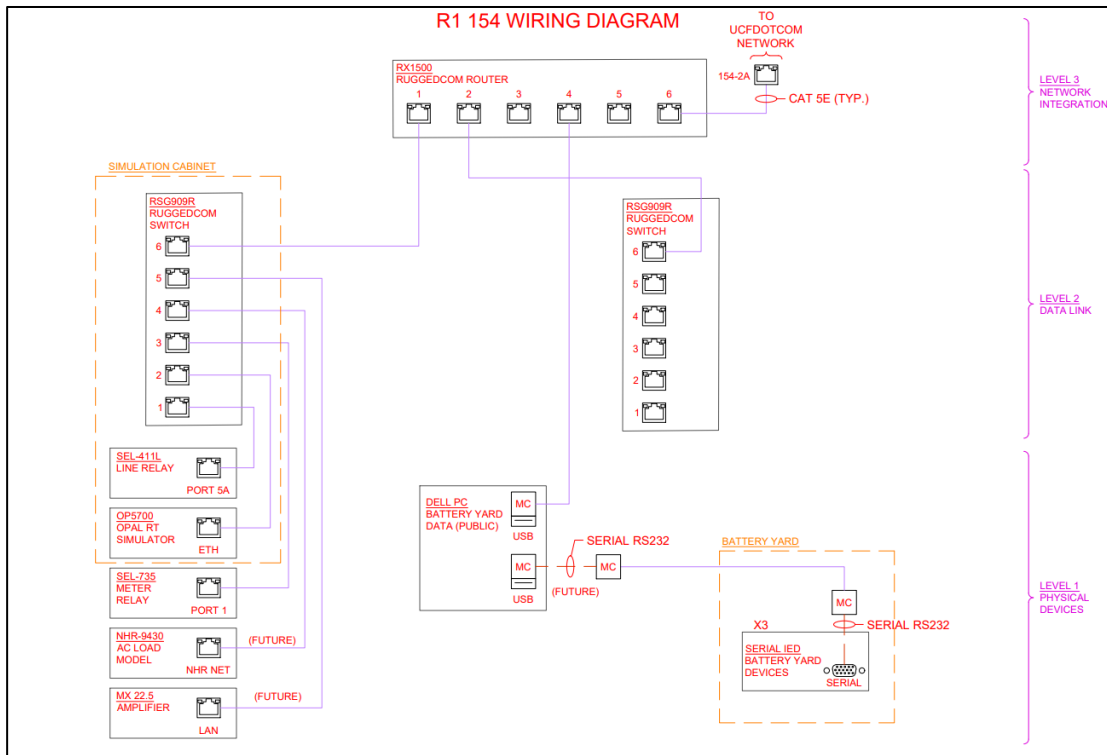


Figure 12. Microgrid Control Laboratory Testbed Diagram

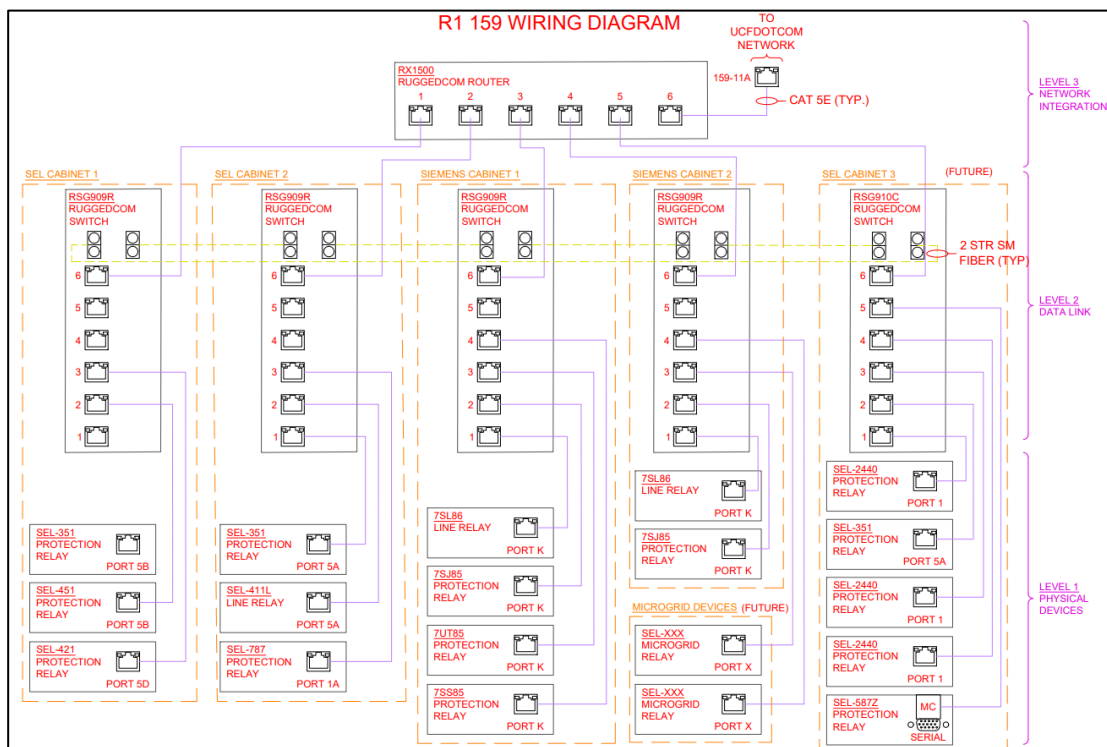


Figure 13. Smart Protection and Control Laboratory Testbed Diagram

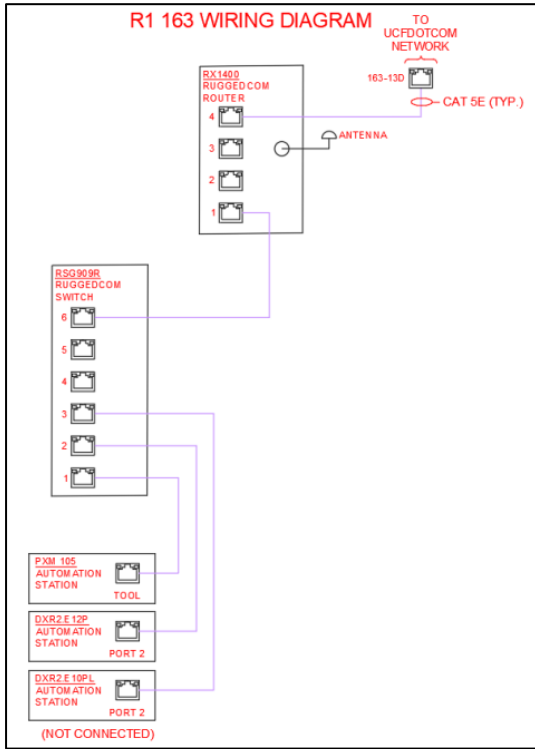


Figure 14. Smart Infrastructure Data Analytics Lab Testbed Diagram

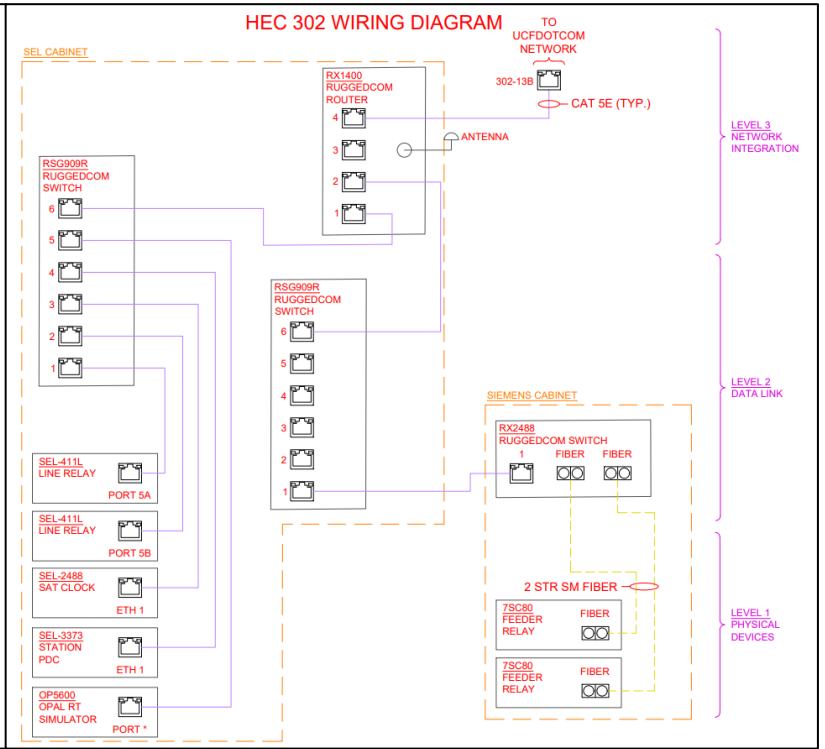


Figure 15. Siemens Digital Grid Laboratory Testbed Diagram

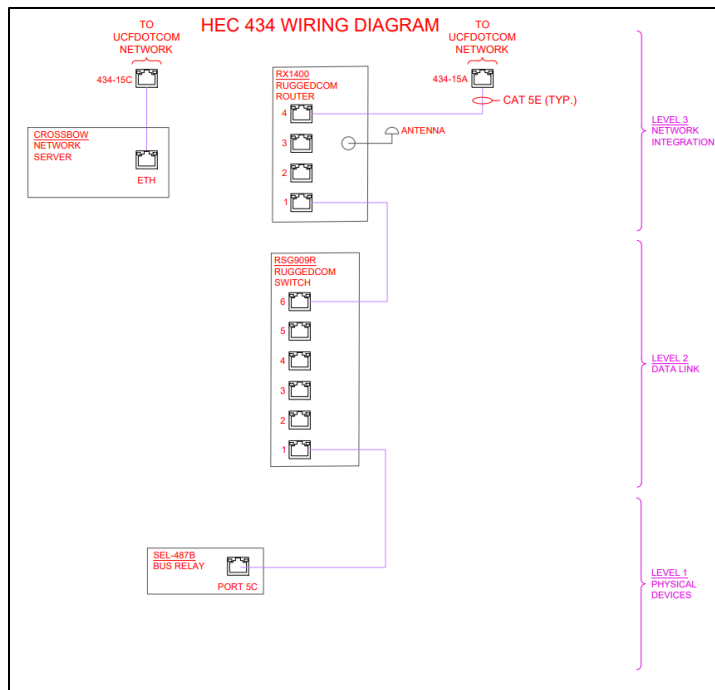


Figure 16. Cyber-Physical Systems Laboratory Testbed Diagram

Real-time simulation of scaled components of the grid can be a challenge of both technological and space complexity. OPAL-RT is one of the biggest names in open and high-performance real-time digital simulation for power systems.



**Figure 17. CPS Testbed Central Control in HEC 434**

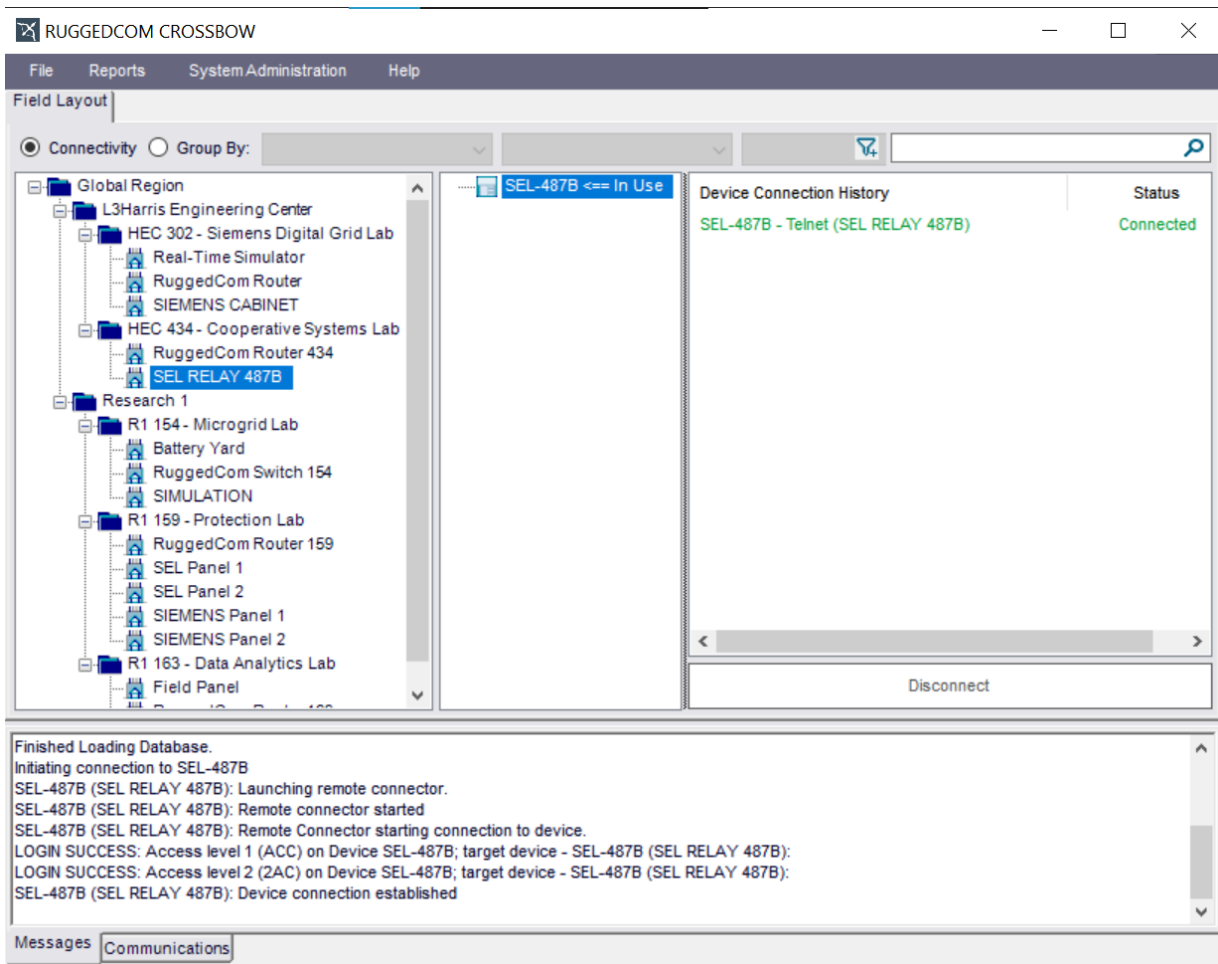
Industry and researchers alike can use their technology to simulate sections of the grid and emulate/duplicate devices through their devices. With numerous data ports, there are many ways the OPAL-RT systems can be integrated with surrounding equipment to reliably study the impact of the power grid and its failures [35]. The RISES testbed deploys two OPAL-RT devices across two of the labs. With the end devices across the entire testbed, the potential to simulate scalable growth of the power grid through real-time models is achievable perpetually. The simulation possibilities presented by OPAL's technology and software allow for the network model centered around Siemens devices and software, accurate standards, practices, and shortcomings to be examined to draw meaningful conclusions via experimentation at scale.



**Figure 18. OPAL-RT OP5707CG Interfacing with Physical Oscilloscope [35]**

### 3.2 Siemens CrossBow

As discussed in the lab descriptions, the Cyber-Physical Systems & Control Lab houses the RISES testbed's primary control system that deploys the Siemens CrossBow software housed within the lab located server. This server houses the data of the entire testbed, programmed in by the admin and, to a limited extent, by clients, through an SQL database routed to the local CrossBow server. Users from any location can then remotely log into the CrossBow apparatus using the proper IP and credentials to access parts of the testbed or, in the case of industry, devices within the grid. Users will be granted certain permissions and access to what portions of the testbed they can access through an admin-determined hierarchy. Direct access to data such as the SQL database is prohibited for clients and allows for a desirable separation between user and organizational networks. CrossBow's primary purpose is to monitor the grid, investigate its current states, and respond to events accordingly. This industry-grade technology is one of the primary focuses of the testbed's research. Looking into possible vulnerabilities that may be present can allow for future improvements and an understanding of how CrossBow can best interface with the technologies and topologies deployed by the biggest names in energy. Figure 19 shows the CrossBow interface deployed from the client-side within the RISES testbed. This figure shows the connection to an SEL relay within the control room. Some clients will only see a select number of these devices and groups depending on permissions, as this point of view is from an admin log-in.



**Figure 19. CrossBow Software Interface**

The RISES Testbed currently has basic functionality through CrossBow, and has the potential to grow into the ambitious goals outlined in this research. Within the cluster’s setup flowing from the control room’s PC that houses the CrossBow server across an array of labs, the scalability of the infrastructure is standardized according to processes outlined by Siemens. The software warrants admin and users with proper permissions to add in additional components across various items, including new users, user groups, device clusters, devices, and device types. The CrossBow manual outlines these processes in a step-by-step manner.



### 3.3 Future Proposed OT Experiments

With the scale of the RISES CPS Testbed, the OT enhancements proposed in Chapter 2 can be appropriately examined given the present capabilities of the labs across the testbed. A crucial feature deployed across each experiment is that each will rely heavily on the simulation of device characteristics brought on by the OPAL-RT OP5600 and OP5700 found in the two labs each is present in - the Microgrid Control and Digital Grid Lab. Examining our Cooperative Network Precision Time Protocol hypothesis requires equipment where high-performance timing is a prerequisite as CN-PTP bolsters local device clusters' timing synchronization and security. Additionally, master clock devices and access to secured ethernet connections are some of the necessary constraints. As within the industry, there will be direct communication lines to a synchronizing master clock and a possible redundant communication to an external satellite master clock for deployable timing and communication reliance testing. The Siemens Digital Grid Lab meets all of these specifications in the following manner. The lab contains a master clock from SEL and Siemens Ruggedcom, line relays and PMUs – precision time devices, and having access to both rooftop satellite antennas and direct lines to UCF's university-wide time-synchronized server, all the required materials are in place to model the proposed application.

The UCF synchronized time server is an NTP-based server, which does propose issues as NTP and PTP prioritize device synchronization in a different manner, but can be used in conjunction within the same setup [36]. However, through a protocol conversion from the lab's Ruggedcom router, patching in signal inputs from UCF networks to the clock devices using a data converter such as the Meinberg Syncbox (shown in Figure 20), the simulated version of direct line PTP can be emulated. An additional option for introducing bolstered precision time

using PTP is a satellite synchronized PTP server similar to Meinberg's PTP grandmaster server [37]. A device like this could add the benefit of redundancy that could make for a surplus in resilience against disruption and open more possible experimental orientations. Using these sources as grandmaster clocks, the two satellite clocks in the RuggedCom RSG2488 and SEL-2730 will be able to interface as a cluster of slave clocks with both physical devices such as the SEL-411L line relay and PMUs and with virtual nodes simulated within the OP-5600. With this in mind, this application can be expanded to a more significant number of devices and clock nodes while still seeing some physically oriented results within the lab space. Communication between local devices that add cooperative network augmentation to the protocol can be realized using standard ethernet synchronization protocols such as NTP. Two control hierarchies will be introduced to compare the resulting topology that uses PTP versus NTP within this same system. The addition of virtual devices with the physical equipment in the lab will allow for an accurate representation of the proposed design, as shown in Figure 3 in Chapter 2, as Figure 20 displays the proposed orientation of a CN-PTP setup within the Siemens Digital Grid Lab.

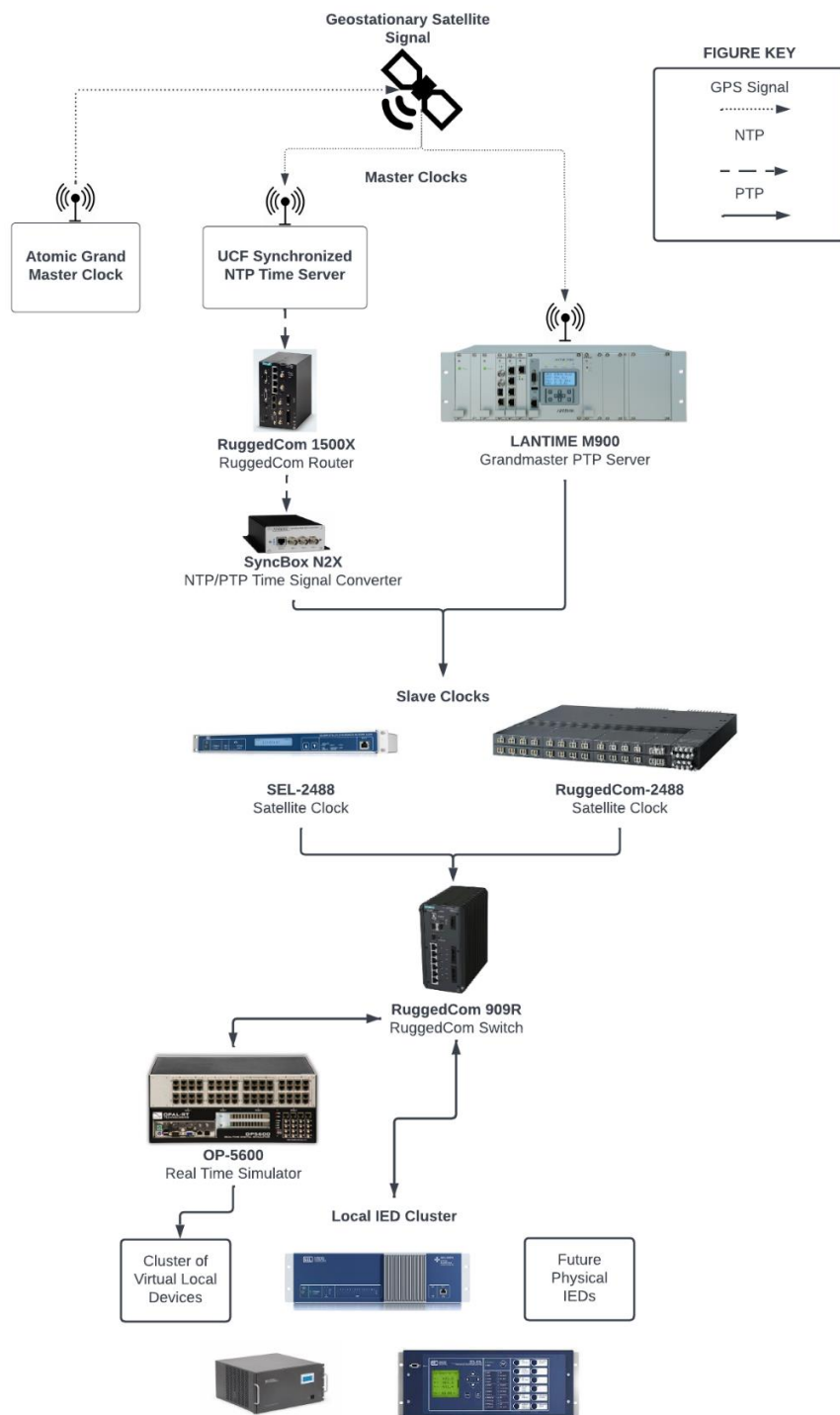


Figure 20. CN-PTP Digital Grid Lab Proposed Experimental Topology

[37][38][39][40][41][42][43][44][45]

Resilient control of a cooperative system through embedded dynamic encoding and decoding requires one significant enhancement to IEDs relative to what is present within standard industry equipment in chaotic oscillation. Nonlinear transfer functions will output signals scrambled from the inputted signals to states that would be impossible to decipher and replicate given the digitally modulated nature of the input signal and the analog transformation it then undergoes. Hypothetically and proven within MATLAB simulation, decoding these signals with a complementary nonlinear circuit would output a stable residual component, while ulterior inputs would quickly raise red flags.

To test this hypothesis, the simulated performance within MATLAB that introduce stealthy integrity attacks would be replicated results for the four test cases outlined in Section 2.2. This would occur by observing a control group of the experiment with no attack, an uncoordinated attack with a typically observed control, a stealthy coordinated attack with typical control, and a stealthy coordinated attack against the protection scheme. Ideal designated attack vectors would be relays that would have the most impactful service disruption. These targets would stem from SEL and Siemens relays or synchronization technology within the RISES testbed. The resulting false data points could include key measurables such as voltage and current or critical vectors such as the accurate time stamps. In either case, successful integrity attacks could result in unintended disruption of service or catastrophic damage to critical components of the energy sector. This being the case, the RISES testbed benefits from its ability to simulate these devastating results without dire consequences and can continually improve response against failed defenses of attacks in future simulations. Labs such as the Smart Protection and Control Lab have many of these physical relays that resemble the configuration of

protection for a substation. On the other hand, labs with the OPAL-RT systems' real-time capabilities can extrapolate digitally cloned devices, allowing for added testing that can be realized through the testbed's interconnection across labs.

With the attack scheme introduced, determining best practices for introducing chaotic oscillation is crucial. This goal can be achieved through three mechanisms: simulated nonlinear mathematical functions, simulated nonlinear circuits, and physical chaotic circuits. With a common goal of producing a nonlinear transfer function for both delivery and reception of signals, it is key to experiment with each of these approaches to measure their viability level against standard integrity attacks and additional penetration testing. The same circuit equations derived from the physical circuits such as the Chua oscillator described in Section 2.2 can be applied to simulate the proper chaotic circuits. Subsequently, any proposed nonlinear equation and its inverse can be used to mimic these characteristics in MATLAB or, if possible, on the IED itself. An additional experiment that could prove valuable for future industry adoption is using a chaotic physical circuit such as the Chua oscillator built into the IEDs to enhance the industrial design of devices like relays. Utilizing the oscillator at the sending and receiving end of a control loop between devices would offer a peek into how building such circuits into future relays may benefit security and yield an improved practice in the realm of device encryption. The remaining construct for this examination relies on utilizing output measurement residual-based attack detection, which relies on accurate models to validate the physical accuracy of received data.

Distributed resilient consensus by the use of competitive interaction among IEDs in a system has the potential to be a precious tool within cooperative systems and critical infrastructure. OPAL-RT highlights this very concept within their cybersecurity pitch for real-

time simulation. [47] Citing the value in utilizing digital twins through their technology to bolster resilience against attacks, the company points to the lessons learned from the grid attack against Ukraine's power grid in 2015 and how this methodology of digital clones can assist in preventing such disruptions in the future. For this reason, the proposed experimental construct for examining this cooperative system defense mechanism has the OPAL-RT devices as its focal point.

With OPAL-RT at the core of these experiments, any lab device can be used in conjunction with the OPAL-RT within either the Siemens Digital Grid Lab or the Microgrid Control Lab to create digital clones of the devices. Three proposed setups shall be examined: no digital clones, one layer of digital clones, and two layers of digital clones. In addition to this device configuration, alterations to the proposed gain  $\beta$  (used in the standard practice of compensating against potential attacks) should be deployed to determine the optimal gain across experimental responses to attacks. Within previous simulation data at UCF, the gain response was measured across several cases. More rapid approaches to a steady state were seen for the followers' state at different gain values. [3] Future research would aim to examine the optimized response across varying gains and attack situations to determine which setup produces viable resilience for the least computational cost and vulnerability. An additional variable to examine would be measuring the draw on computation runtime and space constraints caused by adding  $n$ th order layers of clones. This analysis could better understand how this mechanism can be best optimized and where its limitations could falter its defenses. With these future experiments proposed for deployment within the UCF RISES testbed, the examination of industry-grade practices does not end with their application. Examination of their viability starts with honing

their practice within the controlled testbed, yet examining their weaknesses further following their deployment will be crucial for warranting recommendations of practices for industry adoption.

Cybersecurity is a constantly evolving domain, and the focus of this research is on examining methods that can evolve along with the industry. The flow of ingenuity does not stop with these proposed ideas, however. While these methods seek to patch holes within the power grid's digitalized control, numerous other vulnerabilities may be sought after and discovered by assailants. Additional cooperative system algorithms should be examined for integration within this interface to continue the adaptation of defenses. Given that cooperative system OT enhancements often increase the robust and dynamic defenses of a system, observing combinations, altered orientations, and completely new forms of these enhancements could lead to more improvements in the industry's defense against attacks.

### 3.4 Future Vulnerability Assessment

Assessment of the RISES testbed if required in multiple extents. At a foundational level, the basis for industry technology deployed, the testbed's setup, and the system's permissions for users needs to be examined. Upon validation of this setup, the system then requires more rigorous probing by experts in the knowledge of the power sector, devices specific to the system, and an understanding of the implemented defenses. Combining these approaches allows for a future examination that can return results easily interpreted by the industry.

Vulnerability analysis at face value can be approached from several standpoints. Traditional software that simply scans a system can be a good starting point but has numerous shortcomings. These include missing unknown weaknesses, raising false-positive weaknesses, and, most importantly, only looking for previously considered vulnerabilities. [48] A common assessment approach garners an initial benefit in discovering and prioritizing the assets within a scope and then often focuses on rigorous examination of results and continued security moving forward. [49] However, these traditional methods revert to the initially proposed limitation of traditional cybersecurity in its static approach to problems that looks for lessons from the past. At the same time, the keys to the future lie in the prophesized exploitation mechanisms of today. This research proposes the exploitation of experts in cyber security and specialization within the power industry/critical infrastructure to examine the previously discussed vulnerabilities of a system such as the RISES testbed. In the preliminary stages, standard practices will be deployed. These often include penetration testing, user phishing, DoS attacks, social engineering, and security scanning [25].

Penetration testing involves white hat hackers utilizing their skills and knowledge set to determine potential entry points for vulnerabilities and test their viability within a network. This examination can be performed within our system from varying vectors, including server access, client access, direct device access, etc. Both phishing and social engineering rely on the exploitation of human behavior. Where common practices may exist by users, there is a chance for an advantage to be swung by garnering an understanding of these patterns. Whether it is the day-to-day behavior of how a user logs into a service or the malware their client-hosted device has just received, understanding their impacts and how their loopholes can be closed is crucial



for preventing disaster to an overall system. Attempts at denial-of-service attacks may seem rudimentary. However, emulating characteristics that can slow the performance of a system can result in both degraded performance of a device, and the response time from both automated and human-based course correction can be hindered. Testing the bandwidth of a system against these attacks is another fundamental building block to a resilient cooperative network. Automated searches for vulnerabilities can be rather mundane and limited. However, if deployed with purpose and solid knowledge of a system, security scanning can go a long way in finding the flaws the human eye is blind to.

While these preliminary examinations do bolster the IT security of a system quite a bit in nipping inconveniences prior to them becoming fatal flaws of a system, the value of specialized individuals in examining a system is priceless. Proper cybersecurity examiners for a testbed of this scale should be equipped with a wealth of knowledge on topics such as the energy sector's design, common trends amongst the digital equipment deployed, mindsets of potential attackers, and the repercussions at stake for failure to uphold the sanctity of the grid's infrastructure. Balanced candidates for this role would hold extensive knowledge of general cybersecurity, understanding of government and private efforts in this field, and practice of attempting to exploit and defend given the constraints commonly deployed across the power grid.

Bolstered security is the mission upon which this research is built. With these vulnerabilities in mind, analyzing them is crucial for delivering meaningful results for standards of cybersecurity, best practices of system integration, and individual device improvements. The above steps must be taken to arrive at meaningful conclusions. With certain standards in place

for experimentation, industry adoption is a possibility that could be realized and could guide the energy sector to a safer state.

### 3.5 Desired Outcomes

While the RISES testbed has seen significant progress through connecting these laboratories and edging closer to a fully simulated power grid, further development is still required for accurate industry models to be deployed. Deploying a shift to new industry protocols compared to widely adopted UCF standards has taken time and still needs continued improvement. The Crossbow interface seeks to take over and bolster a more secure and practical interface of centralized control and monitoring of every device across the testbed. As experiments progress and more is discovered about its future potential, the RISES testbed has the potential to expand further with more devices and labs on the horizon of the current research scope's full integration and completion.

Experimental deliverables are a must for a pathway to commercialization to be possible. With a wide-spanning research scope, many projects at play, and several disciplines at the forefront, the RISES testbed has the potential to make quite a splash moving into the next iteration of intelligent devices in cooperative structures. Proving the viability across these experiments requires a team of various skilled individuals, detailed timelines, and thresholds for success compared to already existing practices,

Disciplines spanning from the cooperative system resilient responses are centered on electrical engineering and computer science core concepts, and thus require experts in both fields

for future endeavors in this scope. For simulation schemes that integrate MATLAB simulations of control systems, commonly seen as power grid concepts such as IEEE standard busses, complex circuit orientations, and proficiency in communication protocols, knowledge from multiple electrical engineering industries is required. As is currently the case, the RISES Cluster works directly with numerous Ph.D. students conducting research in each subsection of the testbed and their subsequent subsection of the grid. This yields valuable insight into how each of the proposed applications and experiments can reach its potential within the industry. When it comes to the computer science field, the algorithms and their efficiency are proven by using many core theorems within the discipline. Computer networking is also at the root of the entire testbed's setup, and knowledge of underlying flaws and good practices from this perspective is a needed baseline. Experts in the field of cybersecurity, as previously described, are required to test the vulnerabilities of the designed system. For this cause, the RISES Cluster is currently working with members of the cybersecurity faction of the world-renowned UCF Programming Team. Under the guidance of the leading professors in the field, the experience of completing these experiments is present and capable of doing such. Having a small group of undergraduate students focused on continued monitoring and expanding the testbed's core operations is a valuable asset. The continued progress of this interface allows for the edge nodes that most of the labs focus on to be integrated and expanded to larger scales. As the industry continues to upgrade, operations deployed in the testbed can also continue to be patched, and yield added convenience.

In terms of future experimental results, thresholds for the success or failure of a hypothesis are a gray area. Ideally, results show complete robustness against attacks similar to

simulated case studies. However, confounding variables can contribute to certain edge cases, leading to unforeseen results tipping the scale and rejecting a proposed design. These iterations allow for a reexamination, possible edge cases to be examined to be noted, and improvements to design to be integrated moving forward. Truly robust algorithms require perfection at a minimum with the current realm of present problems. Confidence in the ability to ward off any future form of an attack that these procedures are aimed at defending against must be broken down to the construct of how the attack is physically possible. If all bases are covered in this realm, it passes an initial check and can be thrown into more testing orientations to examine the universality of the mechanisms.

Fortunately, research developed for enhancements for the energy sector does not stop with the power grid. As previously discussed, a cooperative system architecture can be deployed to several alternate industries. Some of these will require reliance on devices near perfection such as autonomous driving and any critical infrastructure disciplines that house the IED and centralized control characteristics necessary to idealize a cooperative structure. These same defenses can be extrapolated to respective alternative industries in cases such as these. The importance of robust defenses shines once again due to this factor. Attack vectors and interfaces change correspondingly as we change the industrial lens in which our systems are understood. If enhancements can be deployed that can inherently prevent integrity attacks, then manipulating the setups to deliver the same results as our OT integrity defenses would ease the transition between industries. Transitioning cybersecurity to more replicable defenses that present insurmountable obstacles to attacks can be an avenue for safer, more reliable technology that instills the continued exponential growth of technological advancements.

## 4. CONCLUSION

As the power sector continues to trek into the realm of a smart, decentralized grid, many vulnerabilities have been exposed across the branches of grid-edge devices. Critical infrastructure has garnered a large target across the global stage, and malicious parties have set their sights on the biggest of prizes in the electrical grid. With numerous cases of integrity attacks being deployed across various industries, the defense of critical infrastructure has become the top priority of utilities and government agencies alike. Fortunately, along with these developing problems, pathways for bolstered security have developed that surpass the static approaches of response-oriented defense mechanisms and instead deploy dynamic enhancements that negate future attacks rather than respond to previously flagged vulnerabilities.

This thesis sets the stage for future research to examine proposed operational technology enhancements to operating grid mechanics and opens the door for future research that further enhances the same vulnerable sectors. The UCF RISES testbed environment is introduced, and standard practices that can be deployed throughout it and the industry are outlined. Three OT enhancements are examined, and experimental settings to assess their efficacy are outlined. The future research outlined within this thesis can be used as a blueprint for determining the validity of the proposed defenses and lays out the framework for developing future experiments and testbed expansions that will continue to evolve along with the ever-changing industry.

Industry is developing at ever faster rates. There must be a methodology in place that will keep the participants of those industries safe from malicious actors and naïve to the idea that vulnerabilities are present in the first place.

## REFERENCES

- [1] H. Rui, W. Yao and B. Gemsjaeger, "Planning of Digitalization and Smartness for Industrial Infrastructures," 2020 10th Smart Grid Conference (SGC), Kashan, Iran, 2020, pp. 1-6, doi: 10.1109/SGC52076.2020.9335731.
- [2] D. Liu et al., "Research on Technology Application and Security Threat of Internet of Things for Smart Grid," 2018 5th International Conference on Information Science and Control Engineering (ICISCE), Zhengzhou, China, 2018, pp. 496-499, doi: 10.1109/ICISCE.2018.00110.
- [3] Y. Joo, Z. Qu and T. Namerikawa, "Resilient Control of Cyber-Physical System Using Nonlinear Encoding Signal Against System Integrity Attacks," in *IEEE Transactions on Automatic Control*, doi: 10.1109/TAC.2020.3034195.
- [4] "Critical Infrastructure Sectors." *Cybersecurity and Infrastructure Security Agency CISA*, CISA, <https://www.cisa.gov/critical-infrastructure-sectors>.
- [5] "Cyber-Physical Systems." *Cyber-Physical Systems - a Concept Map*, University of California Berkeley, <https://ptolemy.berkeley.edu/projects/cps/>.
- [6] A. Gusrialdi, Z. Qu and M. A. Simaan, "Competitive Interaction Design of Cooperative Systems Against Attacks," in *IEEE Transactions on Automatic Control*, vol. 63, no. 9, pp. 3159-3166, Sept. 2018, doi: 10.1109/TAC.2018.2793164.
- [7] D. Kushner, "The Real Story of Stuxnet," in *IEEE Spectrum*, vol. 50, no. 3, pp. 48-53, March 2013, doi: 10.1109/MSPEC.2013.6471059.

- [8] Beaumont, Peter. "Natanz 'Sabotage' Highlights Iran's Vulnerability to Cyber-Attacks." *The Guardian*, 12 Apr. 2021.
- [9] Ferman, Mitchell. "Texas Power Grid, Energy Sectors Facing Elevated Russian Cyber Threats during War in Ukraine." *The Texas Tribune*, The Texas Tribune, 31 Mar. 2022, <https://www.texastribune.org/2022/03/31/texas-energy-grid-russia-cyberattack-hackers/>.
- [10] Sanger, David E., and Nicole Perlroth. "U.S. Escalates Online Attacks on Russia's Power Grid." *The New York Times*, The New York Times, 15 June 2019, <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.
- [11] Lancelot, Jonathan F. "Cyber-Diplomacy: Cyberwarfare and the Rules of Engagement." *Taylor & Francis*, Journal of Cyber Security Technologi, 31 Dec. 2020, <https://www.tandfonline.com/doi/abs/10.1080/23742917.2020.1798155>.
- [12] Lundqvist, Bertil. *100 Years of Relay Protection, the Swedish ABB Relay History*. ABB Automation Products, [https://library.e.abb.com/public/c1256d32004634bac1256e19006fd705/PAPER\\_2001\\_08\\_en\\_100\\_Years\\_of\\_Relay\\_Protection\\_\\_the\\_Swedish\\_ABB\\_Relay\\_History.pdf](https://library.e.abb.com/public/c1256d32004634bac1256e19006fd705/PAPER_2001_08_en_100_Years_of_Relay_Protection__the_Swedish_ABB_Relay_History.pdf).
- [13] Solutions, Process. "A Brief History of the SCADA System." *Process Solutions, Inc.*, 8 Oct. 2020, <https://processsolutions.com/a-brief-history-of-the-scada-system/>.

- [14] Rehman, Abdur. "SCADA and Its Application in Electrical Power Systems." *AllumiaX Engineering*, <https://www.allumiax.com/blog/scada-and-its-application-in-electrical-power-systems>.
- [15] LaMonica, Martin. "Inside a Power Grid Control Room (Photos)." *CNET*, 24 Aug. 2010, <https://www.cnet.com/pictures/inside-a-power-grid-control-room-photos/>.
- [16] "Centralized Generation of Electricity and Its Impacts on the Environment." *EPA*, Environmental Protection Agency, <https://www.epa.gov/energy/centralized-generation-electricity-and-its-impacts-environment>.
- [17] "From the Bottom up: Designing a Decentralized Power System." *NREL*, National Renewable Energy Laboratory, <https://www.nrel.gov/news/features/2019/from-the-bottom-up-designing-a-decentralized-power-system.html>.
- [18] Zyxel, Team. "Does the Internet of Things Increase the Likelihood of Cyber Attack?" *Does the Internet of Things Increase the Likelihood of Cyber Attack?*, Zyxel Networks, <https://blog.zyxel.com/does-the-internet-of-things-increase-the-likelihood-of-cyber-attack>.
- [19] Martin, Maurice, et al. *Power Sector Cybersecurity Building Blocks - NREL*. National Renewable Energy Laboratory, Mar. 2021, <https://www.nrel.gov/docs/fy21osti/79396.pdf>.
- [20] Thompson, Kristy. "Cybersecurity for Smart Grid Systems." *NIST*, 4 May 2021, <https://www.nist.gov/programs-projects/cybersecurity-smart-grid->



systems#:~:text=The%20Cybersecurity%20for%20Smart%20Grid,cryptography%20a  
nd%20cybersecurity%20for%20microgrids.

[21] *Cyber Defense Strategy for Power Equipment | Eaton*. Eaton, <https://www.eaton.com/us/en-us/products/backup-power-ups-surge-it-power-distribution/power-management-software/cyber-defense-strategy.html>.

[22] Jibilian, Isabella. “The US Is Readying Sanctions against Russia over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal.” *Business Insider*, Business Insider, 15 Apr. 2021, <https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12>.

[23] “What Is a Cyberattack? - Most Common Types.” *Cisco*, Cisco, 6 Apr. 2022, <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>.

[24] “Study Reveals Growing Cybersecurity Risks Driven by Remote Work.” *Security Magazine* RSS, Security Magazine, 12 May 2021, <https://www.securitymagazine.com/articles/95177-study-reveals-growing-cybersecurity-risks-driven-by-remote-work>.

[25] Froehlich, Andrew, and Madelyn Bacon. “What Is a White Hat Hacker?” *SearchSecurity*, TechTarget, 29 Dec. 2021, <https://www.techtarget.com/searchsecurity/definition/white-hat>.

- [26] A. Gusrialdi, Z. Qu and M. A. Simaan, "Robust design of cooperative systems against attacks," *2014 American Control Conference*, 2014, pp. 1456-1462, doi: 10.1109/ACC.2014.6858789.
- [27] McGahan, Anita M. *How Industries Change*. Harvard Business Review, Oct. 2004, <https://hbr.org/2004/10/how-industries-change>.
- [28] Qu, Zhihua, et al. *GPS-Free Cooperative Precision Timing for Large Infrastructure Systems*.
- [29] Dagle, Jeff. *Precision Timing Needs in the Electric Power Grid - Rntfnd.org*. Pacific Northwest National Laboratory, 19 June 2018, [https://rntfnd.org/wp-content/uploads/PNNL\\_Dagle\\_Timing-in-Power.pdf](https://rntfnd.org/wp-content/uploads/PNNL_Dagle_Timing-in-Power.pdf).
- [30] Minati, Ludovico, and Mattia Frasca. "Transistor-Based Chaotic Oscillator." *Scholarpedia*, [http://www.scholarpedia.org/article/Transistor-based\\_chaotic\\_oscillator](http://www.scholarpedia.org/article/Transistor-based_chaotic_oscillator).
- [31] *RISES Cluster*, RISES Cluster Resilient, Intelligent and Sustainable Energy Systems, <http://rises.ece.ucf.edu/>.
- [32] "Microgrid Control Laboratory." *Microgrid Control Laboratory – Dr. Zhihua Qu*, <https://www.ece.ucf.edu/~qu/labs/microgrid-control-laboratory/>.
- [33] "Home." *Smart Infrastructure Data Analytics Lab*, University of Central Florida, 6 Jan. 2020, <http://www.smartinfralab.com/>.
- [34] "Digital Grid Lab." *Wei Sun - Group*, University of Central Florida, <https://www.eecs.ucf.edu/~weisun/lab.php>.

- [35] “Power System Simulation Software | Power System Solutions.” *OPAL*, 15 July 2021, <https://www.opal-rt.com/power-systems-overview/>.
- [36] Lichvar, Miroslav. “Combining PTP with NTP to Get the Best of Both Worlds.” *Red Hat*, Red Hat, 20 July 2016, <https://www.redhat.com/en/blog/combining-ntp-ntp-get-best-both-worlds>.
- [37] Meinberg. “IEEE-1588 Grandmaster: PTPv2 Time Server.” *Products*, Meinberg, <https://www.meinbergglobal.com/english/products/grandmaster-clocks.htm>.
- [38] Meinberg. “SyncBox/N2X: Converts NTP or IEEE-1588 to IRIG, 10MHz, PPS, DCF77 and Serial Time Telegrams.” *Products*, Meinberg, <https://www.meinbergglobal.com/english/products/ntp-ntp-signal-converter.htm>.
- [39] “RUGGEDCOM RX1400.” *Rugged Communications for Harsh Environments*, Siemens USA, <https://new.siemens.com/us/en/products/automation/industrial-communication/rugged-communications/ruggedcom-portfolio/wireless/rx1400.html>.
- [40] “RUGGEDCOM RSG909R - Managed Ethernet Switch by Siemens Industrial Communication: .” *Directindustry*, Siemens, <https://www.directindustry.com/prod/siemens-industrial-communication/product-50160-2291864.html>.
- [41] “RUGGEDCOM RSG2488 - Managed Ethernet Switch by Siemens Industrial Communication.” *Directindustry*, Siemens,

<https://www.directindustry.com/prod/siemens-industrial-communication/product-50160-1353071.html>.

[42] “Satellite-Synchronized Network Clock.” *SEL-2488*, Schweitzer Engineering Laboratories, <https://selinc.com/products/2488/>.

[43] “Station Phasor Data Concentrator (PDC).” *SEL-3373*, Schweitzer Engineering Laboratories, <https://selinc.com/products/3373/>.

[44] “Advanced Line Differential Protection, Automation, and Control System.” *SEL-411L*, Schweitzer Engineering Laboratories, <https://selinc.com/products/411L/>.

[45] “NI Announces PMU Application for Grid Automation System.” *Business Wire*, National Instruments, 2 Feb. 2015, <https://www.businesswire.com/news/home/20150202005115/en/NI-Announces-PMU-Application-for-Grid-Automation-System>.

[46] *Ensuring the Security of Electric Power Grids*. OPAL, 4 Mar. 2022, <https://www.opal-rt.com/cybersecurity-overview/>.

[47] *Ensuring the Security of Electric Power Grids*. OPAL, 4 Mar. 2022, <https://www.opal-rt.com/cybersecurity-overview/>.

[48] Irwin, Luke. “The Pros and Cons of Vulnerability Scanning.” *IT Governance UK Blog*, 28 May 2022, <https://www.itgovernance.co.uk/blog/the-pros-and-cons-of-vulnerability-scanning>.

- [49] “How to Perform a Vulnerability Assessment: A Step-by-Step Guide.” *Intruder*,  
<https://www.intruder.io/guides/vulnerability-assessment-made-simple-a-step-by-step-guide>.
- [50] R. S. Singh, H. Hooshyar and L. Vanfretti, "Assessment of time synchronization requirements for Phasor Measurement Units," *2015 IEEE Eindhoven PowerTech*, 2015, pp. 1-6, doi: 10.1109/PTC.2015.7232728.
- [51] “Precision Time Protocol.” *Precision Time Protocol | Junos OS | Juniper Networks*, 2021,  
[https://www.juniper.net/documentation/us/en/software/junos/time-mgmt/topics/topic-map/precision-time-protocol.html#id\\_bpx\\_2ch\\_lrb](https://www.juniper.net/documentation/us/en/software/junos/time-mgmt/topics/topic-map/precision-time-protocol.html#id_bpx_2ch_lrb).
- [52] Labus, Helga. “The Massive Impact of Vulnerabilities in Critical Infrastructure.” *Help Net Security*, 15 Mar. 2022, <https://www.helpnetsecurity.com/2022/03/15/critical-infrastructure-security/>.
- [53] D. An, F. Zhang, Q. Yang and C. Zhang, "Data Integrity Attack in Dynamic State Estimation of Smart Grid: Attack Model and Countermeasures," in *IEEE Transactions on Automation Science and Engineering*, doi: 10.1109/TASE.2022.3149764.
- [54] Y. Luo, L. Cheng, Y. Liang, J. Fu and G. Peng, "Deepnoise: Learning sensor and process noise to detect data integrity attacks in CPS," in *China Communications*, vol. 18, no. 9, pp. 192-209, Sept. 2021, doi: 10.23919/JCC.2021.09.015.

- [55] A. Gusrialdi, Z. Qu and M. A. Simaan, "Competitive Interaction Design of Cooperative Systems Against Attacks," in *IEEE Transactions on Automatic Control*, vol. 63, no. 9, pp. 31593166, Sept. 2018, doi: 10.1109/TAC.2018.2793164.
- [56] "RUGGEDCOM Crossbow." *Siemens.com Global Website*,  
<https://new.siemens.com/global/en/products/automation/industrial-communication/rugged-communications/ruggedcom-portfolio/software/crossbow.html>.
- [57] Lantero, Allison. "How Microgrids Work." *Energy.gov*, 17 June 2014,  
<https://www.energy.gov/articles/how-microgrids-work>.
- [58] Giraldo, Jairo, et al. "A Survey of Physics-Based Attack Detection in Cyber-Physical Systems." *ACM Computing Surveys*, U.S. National Library of Medicine, 13 May 2019,  
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6512826/>.
- [59] "Operational Technology Cybersecurity for Energy Systems." *Energy.gov*, U.S. Department of Energy, <https://www.energy.gov/eere/femp/operational-technology-cybersecurity-energy-systems>.
- [60] P. Fairley, "Cybersecurity at U.S. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory [News]," in *IEEE Spectrum*, vol. 53, no. 5, pp. 11-13, May 2016, doi: 10.1109/MSPEC.2016.7459104.
- [61] Sanger, David Sanger E., and Emily Schmall. "China Appears to Warn India: Push Too Hard and the Lights Could Go Out." *The New York Times*, 28 Feb. 2021.

- [62] P. S. Kumar, W. Emfinger and G. Karsai, “A testbed to simulate and analyze resilient cyber-physical systems,” 2015 International Symposium on Rapid System Prototyping (RSP), Amsterdam, Netherlands, 2015, pp. 97-103, doi: 10.1109/RSP.2015.7416553.
- [63] Mekkanen, Mike. Vaasan Yliopisto, 2020, *Developments of the Cyber Physical Security CPS*.
- [64] Siemens. *Deploying RUGGEDCOM CROSSBOW as an Intermediate Remote Access Solution*, Siemens Canada Ltd., 2016.
- [65] Siemens AG. *RUGGEDCOM CROSSBOW: Secure Access and Management Solution*, Siemens AG, 2016.