Collaborative Research: CISE-MSI: DP: CPS: Cyber Resilient 5G Enabled Virtual Power System for Growing Power Demand

Proposal Description

1. Introduction

Distributed Generation (DG) is growing rapidly due to recent advancements in making more efficient networks of power generation plants. The demand for clean power is on the rise all over the world. The United States' Department of Energy has projected that demand for the electricity generated with solar power will increase by 33%. When photovoltaic (PV) systems are integrated into the distribution network, it can provide system stability, power reliability, and quality improvement, and can reduce energy losses [1]. Distributed Energy Resources (DERs), such as solar, wind and energy storage systems, today complement traditional power plants that are generating electricity centrally. Electricity produced from these energy resources can be coordinated intelligently like a "single utility-scale power station". Such a concept is known as a Virtual Power Plant (VPP) [2].

A VPP could have a single or centralized control system. When any decentralized unit produces, stores, and transfers power, it becomes a part of a VPP. There are technical constraints that arise due to the increasing penetration of PV systems in the distribution network, such as an under/over voltage, reverse power flow, overloading of feeders and transformers, and protection problems [3]-[5]. These constraints limit the maximum deployment of PVs in the distribution network, which is called the PV hosting capacity (PVHC) of the distribution network. The PVHC of the distribution network can be improved by voltage regulation. One of the most viable options is battery energy storage systems that can be used for voltage regulation, smoothing the intermittent power output of PVs, peak load shaving, and reducing power losses and line loading in distribution networks [6]-[7]. Battery storage systems can only provide active power control [8]. Hence, there is a need for a smart controller to control the PV system as well as the battery system. Artificial intelligence (AI) based switching systems for the smart inverter, or the PV and battery system reduces a lot of harmonics [9]. It has been observed that AI controllers are useful for integrating renewable energy systems into power grids because of the intermittent nature of DERs. AI controllers also can be useful for protecting the life span of expensive assets (such as batteries) and facilitating fairer ways to divide joint gains [10]. For instance, FUSE (Future Smart Energy) is an AI-enabled demand-side management system that improves the distribution grids' resilience to multi-energy applications [11].

The backbone of any centralized or decentralized system is its communication. To ensure uninterrupted power, the 5G communication [12] between the PV and Battery system, the controller, and the Supervisory Control and Data Acquisition (SCADA) needs to be ensured. 5G communication has ultra-low latency (1 millisecond) and a very high speed (10 times faster than 4G, which has 1 Gbps peak speed), sharing several attributes with Wi-Fi 6 [13]. However, the 5G communication network needs to be secured. VPP security needs are totally different from traditional information technology networks [14]. This research will design a smart and cyber resilient 5G-enabled AI controller for a pole mounted solar power system with an energy storage system to connect to low-voltage distribution networks to operate as a VPP.

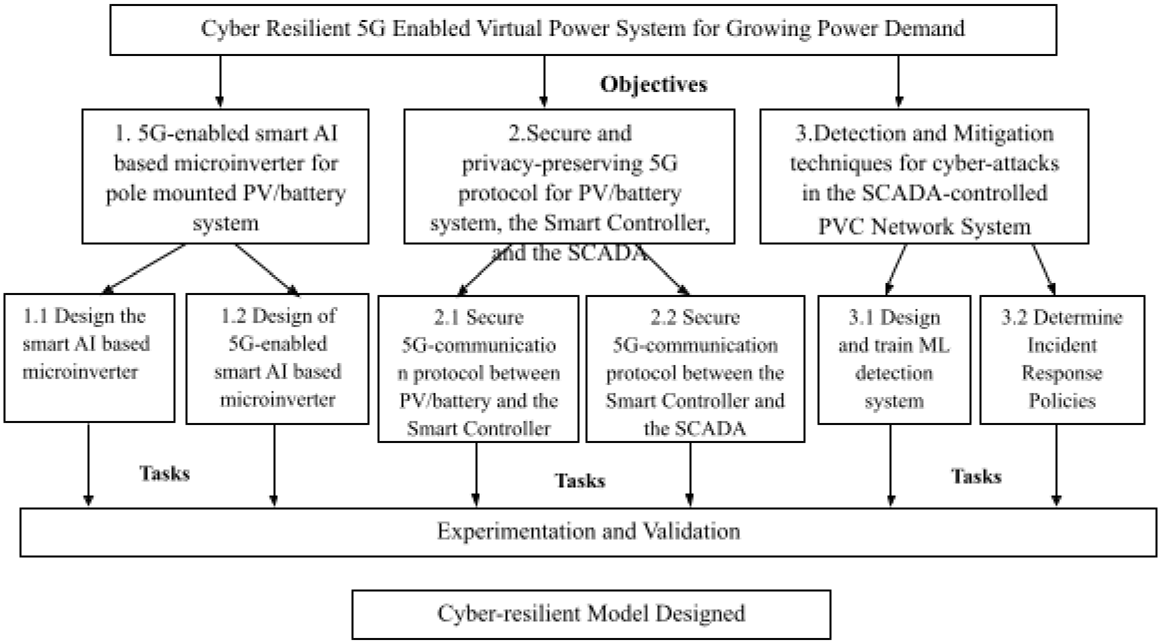
The current issue with 5G-enabled VPP systems is that they do not follow any cybersecurity standards and are connected to the internet, which causes vulnerabilities that hackers can exploit. Since solar energy is a vital method for providing clean energy in power grids, there's a need for PV owners and operators to be educated on cybersecurity standards and best practices. Therefore, data monitoring and control operations are essential to mitigate these risks. This research will design a secure and privacy-preserving protocol that will allow 5G communication between the PV/battery system, the Smart Controller, and the SCADA.

A VPP is susceptible to cyber threats, such as malware intrusion, SQL injection, compromised communication, replay attack, network unavailability, eavesdropping, and traffic analysis. Therefore, it is important to develop a cyber secure and reliable VPP control technique and 5G based communication protocol to connect to the SCADA system. This research will include designing a security framework based on Machine Learning (ML) models for the VPP system. The model will be based on prior cyber-attack datasets and will include continuous learning using the data collected from smart controllers and the SCADA system to detect cyber-attacks. Guidelines and procedures will be designed to help secure the physical systems while ensuring privacy and data protection by alerting administrators regarding security compromises of the VPP network to mitigate the risks and attacks.

1.2. Project Goal

The goal of the proposed research is to explore all technologies and design a secure and trustworthy approach for a 5G-enabled pole mounted Photovoltaic (PV) system for growing power demand. To achieve this goal, this project will have three main objectives:

1. Designing a 5G-enabled AI-based controller for pole mounted PV and battery storage system.
2. Investigating and establishing a secure and privacy-preserving 5G communication protocol for the PV/battery System, Smart controller, and SCADA.
3. Exploring different detection and mitigation techniques for cyber-attacks in a SCADA-Controlled VPP Network System.



Cyber Resilient 5G Enabled Virtual Power System for Growing Power Demand
Objectives
1. 5G-enabled smart AI based microinverter for pole mounted PV/battery system
2.Secure and privacy-preserving 5G protocol for PV/battery system, the Smart Controller, and the SCADA
3.Detection and Mitigation techniques for cyber-attacks in the SCADA-controlled PVC Network System
1.1 Design the smart AI based microinverter
1.2 Design of 5G-enabled smart AI based microinverter
2.1 Secure 5G-communicatio n protocol between PV/battery and the Smart Controller
2.2 Secure 5G-communication protocol between the Smart Controller and the SCADA
3.1 Design and train ML detection system
3.2 Determine Incident Response Policies
Tasks
Tasks
Tasks
Experimentation and Validation
Cyber-resilient Model Designed

Fig. 1. A block diagram highlighting various aspects of the overall project

To achieve these objectives, we will perform fundamental research necessary to address the cyber-resilient solutions for 5G-enabled AI-based controllers for the VPP. The proposed work of addressing the cyber-resilient solutions will be performed over a three-year period by a strategically selected team consisting of four partners, namely, Tennessee State University (TSU) as the Lead, California State University-Bakersfield, Stillman College, and Texas A&M University-Kingsville. Moreover, Schatz Energy Research Center will participate in an advisory role (see enclosed letter in supplementary document section). Fig.1 gives a pictorial view of various aspects of the proposed project.

The novelty of the proposed project stands on the fact that the 5G-enabled cyber secure and AI-based inverters for VPP have not been addressed so far and it is critical for successful deployment of this technology.

2. Proposed Research Methodologies:

To achieve the objectives of the proposed research, the team will undertake several tasks under three interlinked thrusts such as design of 5G-enabled AI-enabled controller, designing secure 5G communication protocols between the PV/battery system, the smart controller, and the SCADA system and explore different detection and mitigation techniques for cyber-attacks in a SCADA-Controlled VPP network system. Figure 2 shows the detailed structure of the proposed 5G-enabled AI based microinverter. Project thrusts, tasks along with their research challenges, and expected milestones are described below.

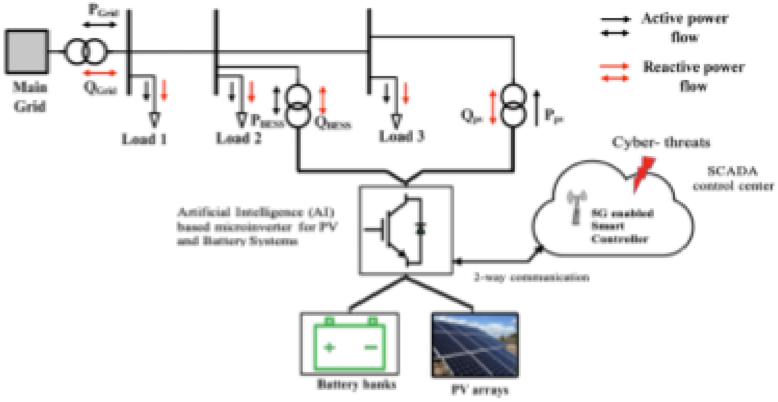


Fig. 2. Proposed 5G-enabled AI based microinverter control system.

Thrust 1: Design of 5G- enabled smart AI microinverter for the PV and battery System.

Background: State-of-the-art and problems

Centralized energy source is the classic standard power model for big power plants connected to the power system. There are typically four plant types associated with centralized energy sources, i.e., coal, gas, nuclear, and hydroelectric. The distributed energy sources consist of small to medium power plants typically, renewable sources, mainly wind and solar [15]. Distributed energy sources have power that is generated closer to the final users and allows the reduction of power traveling on the electrical line that results in loss reduction [15]. Other alternative power options include biogas, natural gas, solar thermal energy, and even wind energy.

Solar power is still one of the most expensive energy sources but has the advantage of being one of the cleanest sources of energy available. A PV system consists of many PV modules connected in series-parallel combination to attain the desired power level, and it is connected to the grid by a boost converter [16]-[17] and an equivalent aggregated DC to AC inverter [18]. A PV system connected to the grid consists of a PV array, a maximum power point tracking technique (MPPT), which is used to extract maximum power from the PV arrays. The perturb and observe (P&O) based MPPT [19] for the PV is implemented on the boost converter for extracting the maximum PV power at all environmental conditions. To maintain the efficient flow of power, utility operators must attempt to steady the supply and demand consistently to meet peak demand. The integration of renewable resources has helped serve the problem of demand. But the intermittent nature of these resources adds to the grid's need for frequency, power, and voltage regulations.

Energy storage can compensate for those fluctuations in power, frequency, and voltage, and thus deliver smoothed power to the customer. There are several types of energy storage available, battery energy storage being the most used because of its high energy density. There is a charging circuit that helps the battery storage system to store the energy and deliver the energy when need be. This circuit will be controlled by a controller. The charge controller delivers power from the PV array to the loads and the battery system. The controller regulates the charging current when the battery system is almost full and maintains the required voltage to fully charge the battery and keep it full. By being able to regulate the voltage, the solar controller protects the battery [20]. The battery system is protected by the charge controller from both overcharging and undercharging. In most PV and battery systems, separate inverters are used [21]. An inverter is used to interface the DC output of the distributed generations, such as the PVs and BESSs, into the AC grid. The inverter also includes reactive power functions to provide voltage regulation for the intermittent nature of the distributed generation resource.

The latest technology is the Photovoltaic AC Module (PV ACM) also known as a microinverter. It is a compact and modular structure for low power PV system applications. In short these are low power inverters in the range 100-350 W [22]. It offers the highest power optimization, design flexibility and avoids a single point of failure. It is less prone to shading effects. Nowadays a single stage flyback type utility interactive inverter is regarded as an attractive solution in PV ACM applications [23]. Most of the microinverters are Proportional Integral (PI) type control [24]-[30]. In [31], a zeta microinverter with a passive snubber is used to achieve higher bandwidth and good closed loop stability compared to flyback topologies [32]. The controller is used to regulate the gate pulses which are provided to the secondary of the transformer. The grid reference voltage is compared with the output of the microinverter to generate the error signal. The AI controller [33] is used to compensate for the error signal. The Levenberg Marquardt Back Propagation algorithm is used to train the system [34].

Some of the other challenges faced by the VPP system are proper communication with the charging control system, communication latency, etc. The charge controller in the charging circuit of the battery is one of the most important components. It is also challenging to design appropriate controllers for inverter and converter systems of the charging circuit of the PV/Battery System. It prevents the overcharging of the battery and protects the battery against over-voltage. The charging and discharging commands need to be relayed very fast and there should be as little latency as possible. 5G controllers are intelligent, fast, reliable, and cost-effective [S30]. The 5G system uses the concept of service-based architecture (SBA) and is deployed on a hyper-scalable containerized and virtualized infrastructure. Thus, it relies on common internet security protocols, commodity server hardware and cloud operating systems. Container orchestration manages containers with load balancing and scalability of applications while commodity hardware should be broadly compatible and have an easy plug-and-play nature. The infrastructure security component deals with 5G network operation with security for the underlying 5G infrastructure. LTE EPC (Evolved Packet Core) components are packaged and deployed as Virtualized Network Functions (VNFs). The secure infrastructure is expected to support 5G network functions, RAN components and related workloads. Due to the nature of RF-based communications, cellular networks are exposed to certain risks caused by impersonation of networks. They can be easily intercepted when devices transmit on the same frequency levels. Devices that utilize cellular connectivity are designed to connect to any network available.

The 5G-enabled communication system has not been used for the VPP aspects. Moreover, intelligent controllers for the PV and battery system were not considered. To overcome these challenges, drawbacks of existing control approaches, and fill in the technical gaps, it is important to design a robust control system using the benefits of 5G based communication technology for the VPP.

This thrust will answer some of the research questions like

1. What are the properties to be considered in the design of a smart AI controller for a PV/battery system?
2. What are the properties for 5G associated with the AI controller?
3. How can we design a low-latency communication protocol for AI controllers?

Proposed Research Tasks

This research proposes to design a 5G-enabled smart AI based microinverter for the PV/battery system which will be intelligent, fast, reliable, and cost-effective.

Research tasks 1.1: Design the smart AI based microinverter for the PV/battery system.

In this task, the proposed smart AI based microinverter for the PV/battery system will be designed. A microinverter consists of a boost converter, H-bridge inverter, and LC filter. Figure 2 shows the detailed structure of a microinverter. The booster converter is switched by Metal oxide semiconductor field-effect transistor (MOSFETS). A closed loop MPPT controller defines the duty cycle. Single phase micro inverters should be isolated at the end of the converter stage [37]. High Frequency (HF) transformer should be part of microinverter design. The H-bridge inverter consists of four MOSFETs and is controlled by PWM (pulse width modulation) with a PI controller. The LC filter is placed at the output of the inverter to reduce harmonics and generate pure sine wave [37]. Due to the intermittent nature of the PV and battery system, a non-linear controller is more suited.

Power generation management is one of the major concerns in contemporary smart power grids in order to provide just the right amount of power based on the demand or need, using artificial intelligence methods, like artificial neural networks, running on AI-based controllers. AI controllers can also manage incorporating eco-friendly power generation into the main electric network. AI controllers are also utilized for enhancing the reliability of eco-friendly power generation plants. Also, artificial neural networks and AI methods have been useful for regulating voltage and improving power efficiency. Along these lines, an AI controller will be utilized in this project to control the PWM, which regulates the switching of the H-bridge inverter. Figure 3 shows the proposed structure of the AI controller. The AI-based algorithm will address the resiliency of the power transfer between the PV/battery system and the low voltage distribution line. To generate the input to the controller, the reference voltage signal is compared with the output voltage signal which is used as a feedback signal. The difference between the two signals is the input of the AI controller and modulation index value is obtained. The modulation index is multiplied with the reference sinusoidal reference wave, and this is compared with the triangular wave. Thus, switching pulses (Q1, Q2, Q3, Q4) are generated for the H- bridge inverter. The circuit diagram for the H-bridge inverter is shown in Figure 5. With the help of the microinverter, the DC voltage of the PV panel is converted to AC voltage. Even though the solar irradiance changes, the output of the microinverter does not change. The AI controller helps to maintain the output voltage that is tracked at the reference value.

Milestone, M 1.1: This research task will result in designing of the smart AI based microinverter for the PV/battery system. The AI based microinverter addresses the resiliency of the power transfer.

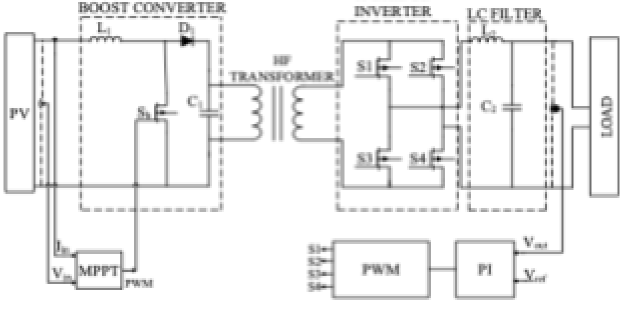


Fig. 3. The detailed structure of a micro inverter [37]

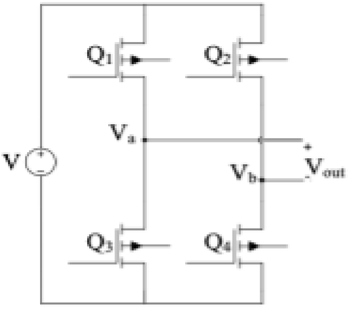


Fig. 5. Circuit of H-bridge inverter [37].

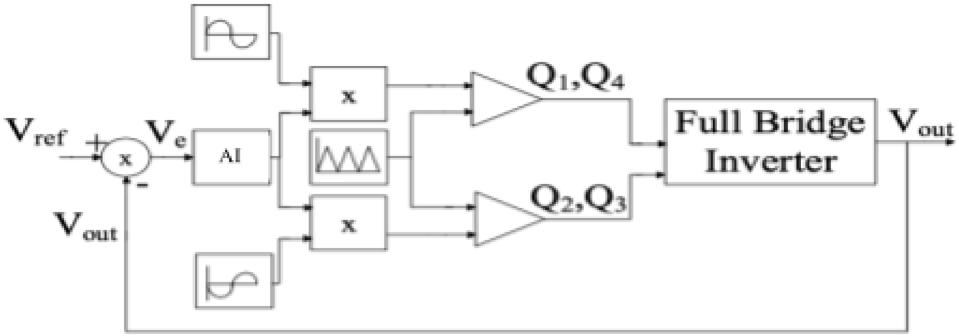


Fig. 4. Switching pulse generation with AI controller

Research tasks 1.2: 5G-enabling of the smart controller for the VPP.

For the development of an intelligent system, it is very important to realize the digitalization, information, automation, and interaction of the power grid. The four layers of the Power Internet of Things are perception layer, network layer, platform layer and application layer focused on data collection, transmission, management, and value creation [38] respectively. To facilitate the interconnection and intercommunication of grid components, one must adopt an open and plug-and-play communication network architecture, the command to and from the controller needs to be fast and efficient. As shown in Figure 2, there is two-way communication between the AI based microinverter and the SCADA system which is 5G-enabled.

Milestone, M 1.2: This research task will result in the successful design of a 5G-enabled AI based microinverter for the PV/battery system. This will enable fast, efficient and boosts data flow between the PV/battery system and the control system.

Research tasks 1.3: Performance Evaluation

To evaluate the effectiveness of the proposed 5G-enabled AI controller for the PV/battery system, simulations will be carried out by using NetSim and 5G simulator. The performance of the proposed 5G-based controller will be compared with that of the existing control approaches like fuzzy logic control, artificial neural network.

Milestone, M 1.3: Completion of performance evaluation for the 5G-enabled AI based microinverter for the VPP.

Performance Results

This is an ongoing work to design controllers and monitor systems for virtual power plants. This project was funded under the GridEd program by the Electric Power Research Institute (EPRI). The smart controller is successful in coordinating between the power demand and storing the power in the battery storage system.

Expected Outcomes

The expected outcome of this research thrust is to successfully design a 5G-enabled smart controller capable of interacting with the charging controller of the PV/battery system and the SCADA.

Thrust 2: Design a secure and privacy-preserving 5G communication protocol between the PV/battery system, the smart controller and SCADA.

Background: State-of-the-art and problems

The PVs are attached to the electrical grid via inverters and communicators with SCADA systems. Presently, the smaller PV systems are not following any cybersecurity standard and are connected to the internet, so data monitoring and control operations can be performed [39]. This is a vulnerability that the hackers can exploit.

In the US, solar energy is available in abundance, and is now becoming an essential part of the energy system. The small PVs are hosted by multiple small owners and operators. Such a PV system should be resilient to cyberattacks. The design of the PVs should be such that they are capable of detecting, identifying, responding to, recovering from, and preventing cyber-attacks. The PV owners and operators should be educated on cybersecurity standards and best practices to mitigate the risks. The PV system is a cyber-physical system (CPS), and any any cyberattack can steal data and can make it incapacitated, so we plan on designing a secure protocol for PV systems.

SCADA technology is of crucial importance to the electrical industry because it manages the extraordinary growth in renewable energy installations, while also ensuring the security and resilience of our nation's electrical grid. SCADA systems allow engineering technicians to control systems in real-time, and log monitoring data of system performance. SCADA data analytics allow for system optimization, preventive maintenance scheduling, rapid detection, and correction of faults and alarms to prevent or minimize system downtime. The project will have an enormous impact on the renewable energy sector, ultimately benefiting society by providing more reliable and lower energy costs to consumers, while creating a more resilient energy grid, and reducing the environmental impact on America's energy sector. Allowing SCADA systems to be controlled by a network can lead to unintended consequences of security risks. Security risks can come from external intruders or hackers, as well as internally from within the corporate Local Area Network (LAN) [40].

Network security refers to measures that are taken to protect the network and the data contained within it. The most common ways of securing a network include the use of firewalls, access control, intrusion detection systems and virtual private networks. Firewalls are the barrier between what gets in and out of a network. Firewalls are implemented in SCADA systems to keep unwanted traffic out of the network. Controlling access to the SCADA network is vital to its security; this is known as access control. Devices or users that are not known are given limited or no access to the network. Intrusion Detection Systems (IDS) are in place within SCADA systems to block malware or suspicious activity. Virtual Private Networks (VPN) allow data to be encrypted and to be sent over the internet. VPNs are a crucial network security tool that gives the user or operator the ability to have remote access to devices or information on the SCADA system [40].

Cyber Threats: There are several technical threats that could affect the digital infrastructure of the PV/battery system and SCADA because of the need to connect remotely. This involves unencrypted connections, technically known vulnerabilities, and exposures from systems on-site that could enable malware, backdoors, and many other techniques to affect current or future behaviors of digital components, or even worse botnets. Advanced persistent threats could disrupt the normal operation and affect the energy assets, as well. Internal technical threats may occur because of unsafe network designs.

Therefore, communication protocols and software dependencies are chosen. The lack of patch-management policy, or information errors because of bad human habits can make any cyber-protection system vulnerable. It is well known that a system is only as strong as its weakest link, and this includes people. Therefore, social engineering needs to be considered as an important threat [41]. In this thrust, we will address the following questions:

1. How can we securely have two-way communication between the smart controller and the Supervisory Control and Data Acquisition (SCADA) system?
2. What type of firewall is needed to protect data from the VPP to the controller?

Proposed Research Tasks

This research proposes to design a 5G-based interactive control system that will allow the microinverter to communicate with the control center and adaptively respond to the changes in demand, solar irradiance, and weather changes.

Research Task 2.1: Design a privacy-preserving 5G communication protocol between PV/Battery system and the Smart controller.

The methodology for this task is to use Location Based Services (LBS) to capture and secure the information being transmitted from the PV/Battery System to the Smart Controller. The application of the LBS system is to deploy sensing devices to monitor the rate of flow of basic and location information between the two sites. Single and continuous query scenarios will be constructed to monitor data flow [42]-[43].

The LBS privacy preserving techniques include rule-based protocol, encryption, heuristic techniques, and cache-based protocol. Rule-based protocol prevents an untrusted LBS server from accessing, storing, and using the user's location information through regulatory strategies [44]. Encryption-based techniques aim to make the information data flow in the network completely invisible to the LBS servers. The heuristic approaches can be classified in four categories: pseudonyms, cloaking, dummy, and perturbations [45]. Cache-based techniques are used to reduce the number of queries entering the LBS server. When fewer inquiries are sent to the server, less sensitive information is released. Hence, there is less chance of exposing the information that is flowing from the PV/Battery system to the Smart Controller [46].

Milestone, M 2.1: A secured link between the PV/Battery system and the Smart controller with appropriate bandwidth to handle 5G connectivity, using firewalls to protect data flow from the VPP to the controller.

Research Task 2.2: Design a privacy-preserving 5G communication protocol between the Smart controller and the SCADA.

The methodology for designing a privacy-preserving 5G communications protocol between the Smart Controller and the SCADA includes the same protocols used in task 2.1 above, with the addition of authentication and privacy-preserving schemes for the 5G network. Authentication for the network between the Smart Controller and the SCADA will include handover authentication, three-factor authentication, authentication and key agreement, radio frequency identification (RFID) authentication, deniable authentication, and mutual authentication [47].

Milestone, M 2.2: A secure two-way communication between the smart controller and the SCADA system.

Performance Results:

A previous project dealt with cybersecurity and was funded by the National Security Agency (NSA). The project involved conducting innovative cybersecurity research to help prevent connected vehicle theft using neoteric AI cybersecurity methods (e.g., deep learning, Neural/Bayesian networks, NLP, computer vision, computational sociology, etc.). The performance results of this current proposal reveal that the information flow between the Smart Controller and the SCADA is protected and preserved in the network, that attempted cyber-attacks are detected and thwarted prior to harmful impact on data and information, and that there is continuous power flow throughout the VPP system.

Expected Outcomes:

In paper [65] Dr. Gagneja has presented a new post-deployment pairwise key distribution scheme for two-tier sensor networks, where she has used a special tree structure for generating the addresses for the nodes in the network. Polynomial based key generating model is used for generating pairwise keys to be shared with neighbor nodes. Dr. Gagneja et al. [66] designed Voronoi-Tabu clustering technique over Improved Tree routing. Using simulations they compared it with directed diffusion, and LEACH, E-G, LEAP, and SBK methods and found that it performs better.

Research Thrust 3: Explore different detection and mitigation techniques for cyber-attacks in a SCADA-Controlled VPP Network System.

Background: State-of-the-art and problems

SCADA is nowadays incorporated in major crucial frameworks for supervising and managing technical and mechanized systems in the production of electricity, transportation, water supply, sewage treatment, etc. SCADA facilitates mechanics, technicians, and engineers to perform economical monitoring and functioning of mechanized systems for electricity transmission plants, which can be located far from each other. SCADA also helps to make sure that operators can work on the systems without harm and danger [48]. As an instance, a SCADA command center for an electrical grid with metering operation and energy measures can easily determine the cause of blackouts and implement stopgap solutions by safely issuing SCADA commands.

Previously, SCADA systems were using non-standard protocols and air-gapped networks as a defense against attack. More and more, the SCADA systems are now connected to the company's network and consequently the Internet [49]. When not connected to corporate or public networks over the Internet, SCADA networks remain secluded. However, SCADA systems can be connected to both wired and wireless technologies. SCADA systems can allow access over the Internet to facilitate the administrators to perform remote monitoring and control [50]. Because of this shift SCADA systems are more readily available, which is enticing for hackers to direct their attacks on them from anywhere in the world. This connection over the Internet allows remote access and monitoring, but it also makes the system vulnerable and susceptible to cyber intrusion and security attacks, which are even more dangerous when considering that interruptions to the SCADA network and system may cause critical operational and organizational issues, along with monetary and personnel problems. These factors combined have increased the number of attacks against SCADA systems. Thus, securing SCADA communication is crucial for the protection of the system and network and to avoid DoS (denial of service) attacks.

Manifestation of unanticipated attacks may be inevitable; however, their impacts can be mitigated by applying incidence response (IR). The main goal of incident response is to lay out a framework for a systematic and organized response while using suitable resources available to the organization.

This thrust will address the following research questions:

1. What are the best strategies for securing the PV, battery, SCADA system, and data? (In order to secure the data and SCADA systems there are three thrust areas: identify, protect, detect, respond, and recover [51].
2. Which supervised machine learning approach (anomaly-based, behavior-based, or signature-based) is going to be more effective for securing the infrastructure of a SCADA-controlled VPP network system? The goal is to determine which machine learning or artificial intelligence method will be most effective and robust for defending the infrastructure of a SCADA-controlled VPP network system.
3. To what extent is batch learning effective for training the models for intrusion detection in a SCADA-controlled VPP network system? The other approach that will be investigated is online continuous learning, which will continue training and improving the model while it is simultaneously making predictions and detecting intrusions or injections.
4. How would companies act in response to an incident?
5. Are distinctly identified processes in place to handle the unanticipated incidents?

Incident response (IR) is the steps used to prepare for, detect, contain, and recover from a data breach [52]. Generally, the workers/employees do not know if the attacker(s) is sitting on their system and for how long. So, the employees should be trained and there should be written procedural, legal, and ethical guidelines and procedures for the designed system on what to do if some incident takes place. According to the National Institute of Standards and Technology (NIST) [53], there are four key phases to IR:
Preparation: No one can spin up an effective incident response on a moment's notice. A plan must be in place to both prevent and respond to events.
Detection and analysis: The second phase of IR is to determine whether an incident occurred, its severity, and its type.
Containment and eradication: The purpose of the containment phase is to halt the effects of an incident before it can cause further damage.
Post-incident recovery: A lesson learned meeting, involving, all relevant parties should be mandatory after a major incident and desirable after less severe incidents with the goal of improving security as a whole and incident handling.

When some incident occurs, such as a cyber-attack or an intrusion is detected, to mitigate the effects, the evidence is gathered, including imaging of the hard drives using write blocker (Write Blocker is required hardware because it stops anything from being written back on the evidence machine). The FTK Imager would be used to take the images of the machines involved. System Artifacts would be checked manually to identify the cause or source of the attacks. The incident response date and time (metadata) of all the data/files is important. To maintain the state of the evidence, Write Blocker will be used. Cloning will also be used to prove that the data is sterile.

Proposed Research Tasks

The interactive nature of the AI-based controller and the SCADA control center and its dependency on the 5G communication protocols, however, makes it very vulnerable to cyber security threats and attacks which can lead to degradation of the system performance and even disruption of charging of the battery system. Therefore, it is important to develop a secure and reliable communication protocol between SCADA and the microinverter. To develop the proposed secure, private, and interactive control system, the following tasks will be performed.

Research Task 3.1: Design and train a ML intrusion detection system to detect any potential anomalous behavior and cyber-attacks.

The goal of this project is to detect intrusions in a photovoltaic cell (VPP) network system [54] that is controlled by supervisory control and data acquisition (SCADA) [55]. Different machine learning and artificial intelligence methods will be investigated, such as anomaly-based [56], behavior-based [57], and signature-based [58] detection. Statistical parameter calculations will be used for the investigation. Current state-of-the-art algorithms include Beta Hebbian Learning [59], classification and regression decision trees [60], and support vector machines in cyber-physical systems [61] for the detection of security attacks.

What needs to be explored is which approach, anomaly-based, behavior-based, or signature-based, is more suitable and effective for intrusion detection in the SCADA-controlled VPP network system. This research task is to investigate which machine learning or artificial intelligence algorithm will detect the intrusion attacks with the highest accuracy. Most research in the literature for intrusion detection in SCADA-controlled VPP network systems has used batch training. This project will compare both batch training and continuous online training approaches. This project will also investigate if continuous online training can continually keep improving the accuracy of intrusion detection, as it will be detecting attacks and training the model at the same time.

Milestone, M 3.1: The designed ML intrusion detection system identifies any anomalous behavior and sends an alert to the admin.

Research Task 3.2: Determine Incident response guidelines and procedures for mitigating cyber risks on the cyber-physical components of PV/Battery systems.

There are regulatory uncertainties in PV cyber security, and cyber threats are unpredictable and evolve faster than the industry's ability to develop and deploy countermeasures. Cybersecurity threats are evolving more rapidly than the implementation of defense measures. The response to any cyber-attack and mitigation process is delayed because of a lack of information-sharing among the entities involved and various challenges associated with different attacks. So, the response and recovery process should be resilient enough to handle system disturbances. The NIST recommends that the organization should provide for each stage of cyber incidents: identify, protect, detect, respond, and recover [39]. Identify and protect aims to enhance the security to harden PV communication to protect photovoltaic infrastructure such as by hardening the PV inverters by rigorous in-house testing. Detect advocates use of protective techniques that automatically identify and alert the user of any possible security breaches, such as sharing information with reliable resources to find if vulnerabilities detected in other commodities would affect PV devices. Respond and recover emphasize having a contingency plan to continue running critical operations and recover from cyber security attacks, such as designing PV devices to fail in a predictable and safe manner.

This research task is to design the guidelines and procedures in case of any cyberattack, such as, Distributed Denial of Service or Man in the middle, to mitigate the effects of the attack. The guidelines and procedures document would include the activities required in each phase of incident response, roles, and responsibilities for completing IR activities, communication pathways between the incident response team and the rest of the project team, and the metrics to capture the effectiveness of its IR capabilities. During the Identify and Protect stage, create standards or guideline recommendations for cyber-secure protocols, architectures, and certification procedures. Also, the stakeholders should share data and threat intelligence. During the Detect stage the grid operators should be aware of the capabilities of intrusion detection systems and how to use it on operational datasets for security analytics. During Respond and Recover stage the standardized PV/DER control network should be in use, and organizations should establish cyber response teams. They should also perform field tests for response and recovery.

Milestone, M 3.2: Comprehensive guidelines and procedures that should be followed to respond to any incident.

Performance Results

Dr. Gagneja in her paper [67] has explored how the industry should respond to an incident or cyberattack that takes place on them. Usually, it's the hackers' thinking process that triggers such attacks. So, knowing the hackers' intent would help the industry to resolve the incident quickly and efficiently.

Expected Outcomes

The expected outcome will be the design of an ML based intrusion detection in a SCADA-controlled VPP network system, which will be able to detect cyber-attacks and perform damage control by alerting admins regarding security compromises of the VPP network. The intrusion detection system will be able to identify any intrusive or malicious activity in the SCADA-controlled VPP network. The system will log any security breach for continuous training of the intrusion detection models. Incident response guidelines and procedures for mitigating cyber risks on the cyber-physical components of PV/Battery systems.

3. Institutional Data Narrative

Tennessee State University (TSU) a major urban, comprehensive institution is an 1890 land grant university and one of the Historically Black Colleges and Universities founded in 1912 as a normal school. This unique combination of characteristics distinguishes it from other academic institutions in the state of Tennessee. Tennessee State University displays a broad spectrum of sponsored research projects, ranging from basic to applied, and from single PI grants to major team collaborations. TSU has averaged approximately $40M annually in research and sponsored program awards. It has over 100,000 sq. ft. of floor space designated for scientific and technological research.

Stillman College (SC), located in Tuscaloosa, Alabama, is an "Institution of Emerging Excellence," as defined by USC 42 Section 283k. Founded in 1876, Stillman College is a private institution of higher education and 501 (c)(3) non-profit organization. Stillman College is a four-year educational, historically black liberal arts institution (HBCU), committed to fostering academic excellence and providing high quality educational opportunities for diverse populations with disparate levels of academic preparation, with a legacy of producing teachers, scientists, and researchers. Stillman College's 2019 student enrollment was 861 of which 408 (47%) were male and 453 (53%) were female students. Most students are from Alabama (597 / 76%) and identify as African American (87%); White (6%), Hispanic/Latino (2%), and the remainder unknown (5%).

California State University (CSUB), Bakersfield, in 1998, was designated a Hispanic-Serving Institution, as defined by the Higher Education Opportunity Act. CSUB works to meet the unique needs of Latina/o/x students, many of whom are first-generation. As of Fall 2019, CSUB reports 62.8 percent of undergraduates that are of Hispanic heritage. The total enrollment for Fall 2021, was 10,624 with race/ethnicity breakdown of 421 African Americans, 28 American Indians, 700 Asian Americans, 6,754 Hispanics, 268 Non-Resident Aliens, 18 Pacific Islanders, 225 with Two or More Races, 593 Unknowns, and 1,617 White, Non-Latino. In Fall 2021, out of all enrolled students 7,203 are URMs and 3,421 are non-URMs. First-Time, Full-Time Freshmen Graduation Rate for Fall 2017 is 27.60% for CSUB and 16.67% for the Computer and Electrical Engineering and Computer Science (CEECS) department.

Texas A&M University-Kingsville (TAMUK) is dedicated to serving an ethnically and culturally diverse population. The University is committed to its mission of teaching, research, and service in South Texas for the advancement of knowledge and of regional development. The university is in historic Kingsville, a friendly, safe city of 25,000 that is the home of the legendary King Ranch. Corpus Christi and its beaches are just 40 miles to the northeast, and the border with Mexico is 120 miles to the south at Brownsville or 119 miles to the west at Laredo. Most of Texas A&M-Kingsville's approximately 6,357 students come from South Texas, but there is wide diversity in the population, with students from 40 states and 35 countries. The student body is split almost equally between men and women. About 80 percent of students are undergraduates. Ethnically, the campus reflects the demographics of the area, with 69 percent of the students Hispanic, 15 percent white, and 4 percent African American. About 7 percent are international students.

4. Experimentation and Validation using Simulated and Real data

To validate the proposed research, in this work, simulations will be conducted by using various simulation software such as NetSim, ANSYS Maxwell Software, and MATLAB 5G toolbox. Additionally, a proof-of-concept smart controller will be designed with real-world 5G communication and wireless power transfer. To test the controller, Schartz Energy Institute will be subcontracted. The detailed experimentation plans for all three thrust areas are explained below.

a) For the validation of the 5G-enabled smart AI based microinverter, MATLAB/Simulink model will be used. The system will also be validated in real time with the help of Schatz Energy Research Institute. A 5G-based wireless communication module will be incorporated to allow the microinverter to communicate with a SCADA server based on the 5G communication standard. Networked Control Systems Windtunnel (NCSWT) is an integrated modeling and simulation tool for the evaluation of networked control systems (NCS). NCSWT integrates Matlab/Simulink and NS-2 with which Network Simulator 2 (NS-2) is regarded as a discrete event simulation tool and has proved its worth in research of dynamic communication networks. [62]-[63].

b) The evaluation process involves identifying how the system is supposed to work, then running experiments to make sure that it is working as intended with policies and procedures in place. Written policies and procedures for access control are based on the total number of employees or users in the organization, and facilitate implementation of policies and procedures by 1) identifying the type of organization and its responsibilities, 2) providing knowledge of fundamental concepts, 3) using standards such as National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, or International Organization for Standardization (ISO) 27001 [51], [64], 4) evaluating the security process (such as: social engineering, penetration testing, and others) following the best processes of NIST and using server software that is properly licensed. The ISO 27001 provides the specification for an Information Security Management System (ISMS), including requirements for the risk management process that should be followed to choose the security measures appropriate to the risks the organization faces.

c) For validation of the intrusion detection system, the artificial intelligence and machine learning models will be programmed in Python scripts. Past cyber-attack datasets will be collected and collated. The datasets will be loaded into the Python scripts, which will be programmed to create the artificial intelligence and machine learning models. The models will be trained using the cyber-attack datasets. The trained models will then subsequently be used for building the intrusion detection system. The implemented artificial intelligence and machine learning models for intrusion detection will be evaluated by assessing their performance parameters such as accuracy and precision using test data extracted from the datasets. Both the training and test accuracy will be calculated. Five-fold cross validation will also be employed to obtain a comprehensive assessment of each of the implemented artificial intelligence and machine learning models for intrusion detection. Guidelines and procedures will be designed to help secure the physical systems while ensuring privacy and data protection by alerting administrators regarding security compromises of the VPP network to mitigate the risks and attacks.

5. Project Schedule and Management

This project will be performed over a three-year period by the team members who are represented by two HSIs and two HBCUs from different states. The tasks shown in Table 1 are already described in section 2 and 3. For each task/subtask, one university will take the lead and the other universities will collaborate. The project lead Dr. Ghosh will conduct monthly meetings with the whole research team to review progress, discuss results and plan future directions. Research conducted by undergraduate and graduate students will constitute their capstone design project or master's thesis. Each university would hire either one undergraduate student or a graduate or both. Students will be recruited from computer science, electrical engineering, and software engineering. Research findings will be published in journals and will also be presented at conferences and standard meetings. The virtual/in-person workshop will be held during summer.

Our team's experience, outstanding research performance and record of publications are indications of commitment to success for the proposed project.

The Project Lead and **PI Dr. Sagnika Ghosh** is an Assistant Professor with the Electrical and Computer Engineering department of the Tennessee State University, Nashville (TSU). Her research interests include smart and microgrids, electric vehicles and cybersecurity issues and solutions for power grids. She teaches graduate and undergraduate courses at Tennessee State University. She is actively working on developing courses. She is a member of IEEE, ASEE, and SWE. She is also a member of IEEE Women in Engineering.

Co-PI Dr. Ayush Goyal is an Assistant Professor at the Electrical Engineering and Computer Science department at Texas A&M University - Kingsville (TAMUK). He has received funding from the Department of Homeland Security (DHS) Grant No. 21STSLA00011-01-00 for a project titled "Building Cyber Intelligence Workforce through AI-Based Cybersecurity Education and Training" in the amount of $466,324, for which he is an early-career faculty Co-PI. Dr. Goyal's research experience and publications are in machine learning and artificial intelligence applied towards cybersecurity, secure authentication, object detection, computer vision, and image processing applications.

Co-PI Dr. Kanwalinderjit Kaur is an Assistant Professor of Computer Science at California State University, Bakersfield. She has received a state funding of $45,000 from CyberFlorida Grant No. # 3910-1004-00-D 7/2017-6/2019 for a project titled "Curriculum and Lab/Technology Development on Digital Forensics". She has research experience working with graduate and undergraduate students. She has published over 40 conference and journal papers. Her research interests include Cyber Security, the Internet of Things (IoT), and blockchain. She works closely with other faculty, students, and industry partners to develop novel solutions to the cyber security problems related to the Internet, IoT devices, cloud, and Autonomous Vehicles (AV). She has received multiple institutional internal and industry grants to work on her research area. As an active researcher, she has developed a solid core of research skills and the ability to apply these skills to turn ideas into scientific contributions. She continuously reviews papers for various journals and conferences. She will use her expertise in designing AI-enabled controllers and to design a secure and privacy-preserving 5G communication protocol between the PV/battery system, the smart controller, and SCADA system. She will apply her expertise to design and train an ML intrusion detection system to detect any potential cyber-attack and will also design the guidelines and procedures to mitigate the effects of the cyber-attack.

Co-PI Maria Laurent-Rice is an Assistant Professor of Information Systems and the Director of the Cybersecurity Program at Stillman College (SC) in Tuscaloosa, Alabama. Professor Laurent-Rice has developed two research products that support Artificial Intelligence (AI) integration into the training the labor market workforce, researched and studied the labor market/workforce statistics for Alabama counties in and around Tuscaloosa commonly referred to as the Black Belt, and enhanced Stillman

College Dual-enrollment program with local high schools to provide cybersecurity training to meet the labor market demand for cybersecurity experts in Alabama. She has displayed exemplary collaborative skills in establishing collaborative partnerships with universities and businesses. Some examples of on-going collaborative efforts include the University of California at Los Angeles, California, Cypress Community College, California, Arizona State University, University of Tennessee at Chattanooga, Tougaloo College, Mississippi, WINTRIO Inc, Virginia, IBM, Microsoft, HumanTouch, LLC, Virginia, Women in CyberSecurity (WiCyS), National Center for Women & Information Technology (NCWIT), and NCWIT Mentoring Award for Undergraduate Research (MAUR).

4.1 Deliverables:

The deliverables of this project include,

i) Annual progress reports, and technical reports that will cover software and design documents from time to time.

ii) Publishing the outcomes of research in peer-reviewed journals and conferences as the project progresses.

iii) Demonstrating proof of concept with the simulation prototypes.

iv) Use cases for cyber-attack scenarios for VPP systems.

v) The Python AI and ML models and datasets for the cyber intrusion detection system will also be provided and shared with the larger research community.

vi) Comprehensive guidelines and procedures that should be followed to respond to any incident.

Table 1: Research Project timeline and Milestones

Task No.	Task Leader	Collaborators	Years			Resulting Milestones
			1	2	3	
1.1	TSU	SC, CSUB,	⬛			M 1.1
1.2	TSU	TAMUK, SC, CSUB	⬛	⬛		M 1.2
1.3	TSU	SC, CSUB, TAMUK	⬛		⬛	M 1.3
2.1	SC	CSUB, TSU, TAMUK	🟥	🟥		M 2.1
2.2	SC	TSU, CSUB, TAMUK		🟥	🟥	M 2.2
3.1	TAMUK	TSU, SC, CSUB	🟦	🟦	🟦	M 3.1
3.2	CSUB	TSU, SC, TAMUK	🟨	🟨	🟨	M 3.2

6. Intellectual Merit:

The overall goal of the proposed research aims to design a way to supply secure power during peak demand by the solar-powered and energy storage system created as a VPP. To achieve this goal, the project will have several objectives such as 1) designing 5G-enabled AI based microinverter for PV/battery system, 2) demonstrate a secure 5G wireless communication between PV/battery system, the smart controller, and the SCADA system, 3) designing a secure integrated data flow among the cyber-physical components of the PV/battery systems, smart controller, and the SCADA system, 4) detecting cyber-attacks and exploring mitigation solutions for 5G-enabled SCADA-controlled VPP network system. Our approach centers on designing a unique and potentially transformative cybersecure 5G-enabled VPP system. Equally important, the outcomes of this research will aid and provide inputs in the design of IEEE and IEC standards for 5G-enabled cyber-physical systems, especially for emerging cyber vulnerabilities and system resiliency.

7. Broader Impacts of the Proposed Research

This project will significantly impact industry, academia, and society at large particularly in securing the infrastructure of SCADA-controlled VPP network systems by designing more robust and effective, and Machine Learning (ML) enabled continuous continuously improving intrusion detection models. Research outcomes will help manufacturers design secure and resilient virtual power plants for growing demand. In academia, this work will impact the design of electrical engineering as well as computer science courses related to renewable power integration design and cybersecurity. The simulation models and controller prototypes designed for the secure VPP system as part of this project will expose students to the concepts of secure renewable resources integration, design of controllers for battery storage systems, and future design directions. The research results will be a model for other MSIs and will broaden the participation of URMs in cybersecurity programs nationwide. At a societal level, it will prepare cybersecurity experts and nonprofessionals alike to appropriately address the ever-increasing threats of cyberattacks and assist in meeting the demands of a national labor market that faces cyberattacks against them daily. In particular, the PIs plan to conduct innovative outreach educational activities to disseminate the findings of the proposed research. Some of the plans include:

i. Organize an annual virtual symposium for graduate and undergraduate students of the Engineering and Computer Science Departments. Through this workshop, the PIs will use hands-on demonstrations to convey the benefits of the secure 5G-enabled smart controller for the VPP and their cybersecurity issues. At the end of the workshop, handouts containing a description of the benefits of secure power systems and cybersecurity solutions will be distributed for reference.

ii. Expand efforts to expose middle and high school students to cybersecurity and renewable energy resources by demonstrating to them how 5G, VPP systems, and cybersecurity affects us. The school students would be presented with this information during the pre-summer interactive school. This annual event hosted by the College of Engineering at TSU draws more than 500 area middle and high school students and teachers. During the academic year CSUB hosts outreach events for high school students and encourages them to apply to the STEM field at the university. TAMUK and Stillman College will work on this effort by leveraging on existing initiatives such as AI, Robotics, and Sustainable Energy. Results from this research could be distributed to local high school STEM programs to better prepare their students for college level studies. This research project will greatly assist in closing the gaps in STEM education affecting underrepresented and minority students in colleges and universities across the United States. This project will be providing STEM research project experiences to minority students from marginalized and underrepresented backgrounds in the field of cybersecurity for virtual power plants, which will be a unique research opportunity for minority students. TAMUK is an HSI / MSI (largely Hispanic Minority Serving Institution) and the investigator from TAMUK will organize outreach events at the local South Texas high schools for attracting and recruiting the largely Hispanic, marginalized, and underrepresented students to STEM fields by showing them the application of artificial intelligence and machine learning for a cybersecurity application in virtual power plant networks.

iii. Collaboration will be expanded by submitting Research Experience for Undergraduates (REU) proposals to design a sustainable program to include MSI students.

iv. Disseminate research results via traditional publication venues as well as via a tutorial on cybersecurity issues to be offered at the IEEE PES General Meeting and/or at upcoming IEEE, ACM conferences. This activity will promote multidisciplinary research and training among power and cyber scientists.

8. Results from Prior NSF Support and Other

Dr. Maria Laurent-Rice (Co-PI from SC) had an NSF-Catalyst Collaborative project, (Award# 2107631, $175,000, 9/2022-9/2024) titled "Historically Black Colleges and Universities - Undergraduate Program (HBCU-UP)". *Intellectual Merit:* Our study is at the forefront of using interdisciplinary research by combining 1) self-regulated learning theory from educational psychology, 2) adaptive learning technology that leverages machine learning and data analytics to produce personalized learning paths and 3) culturally relevant pedagogy coupled with active learning to promote mathematics mastery in college algebra. *Broader Impacts*: The most immediate broader impact of this study is the potential for the theory- driven, hybrid, adaptive learning model for college algebra to be scaled up for use in other STEM courses. This innovative college algebra course also could serve as a model to be used at other HBCUs particularly smaller schools that welcome highly motivated students who enter college with some educational shortfalls e.g.- poor math placement.

Dr. Maria Laurent-Rice (Co-PI from SC) had an NSF-CEDI II, (Award # H9823-20-1-0331, $149,862.00, 9/2020-9/2022) titled "Peer-to-Peer Track and Trace Network", NCAE-C-003-2020 NCAE-C Cyber Curriculum and Research 2020 Program, CEDI II, Research. Intellectual Merit: Our study will conduct innovative cybersecurity research to help prevent connected vehicle theft using neoteric artificial intelligent (AI) cybersecurity methods. Broader Impacts: The proposed AI augmented cybersecurity for vehicle safety research may be expanded to apply advancements in AI methods (e.g., deep learning, Neural/Bayesian networks, NLP, computer vision, computational sociology, etc.) to provide safety decision, support services for vehicle owners and allow law enforcement to quickly respond and predict the likelihood of property crimes including, but not limited to, vehicle thefts/vandalisms, residential burglaries, and intentional violence against minority underserved and disadvantaged populations.