SAND2021-4954R

SANDIA REPORT
SAND20XX-XXXX
Printed March 2021

Sandia National Laboratories

New Jersey Transit Grid Distributed Generation Program

Cybersecurity Design Assurance Assessment

Benjamin Anderson, William Atkins, Jay Johnson, Timothy Ortiz, Steve Scott, Russell Shiplet
Sandia National Laboratories

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	https://classic.ntis.gov/help/order-methods/

ABSTRACT

Superstorm Sandy caused a major disruption to passenger-rail and other commuter systems throughout New York and New Jersey. To address this issue, New Jersey Transit (NJT) established the NJ TRANSITGRID project, an effort designed to power bus, ferry, and limited passenger-rail service during natural or man-made disasters. Given the importance of these transportation systems, NJT partnered with Sandia National Laboratories (Sandia) to assess the cyber-resilience of the information systems that monitor and control the electrical systems within the microgrid. The Sandia "tabletop" assessment is based on the most recent 20% design packages. From this assessment, the Sandia team identified several security areas that were undefined or did not implement industry best practices. Finally, the Sandia team presented possible follow-on assessment activities and recommended investigating multiple hardening technologies. Addressing these findings and adding state-of-the-art detection and mitigation technologies will help ensure the NJ TRANSITGRID is built with more comprehensive cyber-resilience features.

CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

Sandia National Laboratories assessed cyber-resilience microgrid technologies within the $570M NJ TRANSITGRID project, designed to power bus, ferry, and limited passenger-rail service within and adjacent to Northeast corridor rail operations between New York City and NJ during natural or man-made disasters, e.g., a future Superstorm Sandy. The NJ TRANSITGRID project consists of seven discrete Distributed Generation Facilities (DGF) in addition to the Microgrid Central Facility (MCF) that will support New Jersey Transit (NJT) and Amtrak train operations, the associated Newark Penn, Secaucus Junction, Newark Broad facilities, three bus garages, and the Port Imperial Ferry Terminal—which are used by more than 100,000 commuters daily. The MCF – the largest project component – consists of a 600 kW PV site, energy storage flywheels, and five natural gas fueled gensets that will operate NJT and Amtrak rail lines on a limited basis. As of early 2021, NJT has a 20% design of the electrical system but the security plan is not fully detailed.

This report summarizes the Sandia cybersecurity design assurance assessment performed on the 20% design packages for the NJ TRANSITGRID systems that were submitted to NJT by Jacobs Engineering and AECOM. This assessment was focused on the cybersecurity of the components (generator sets, switch gear, monitoring systems, etc.), systems (HMIs, workstations, etc.), and the various types of networks connecting these devices (SCADA, TCP/IP, etc.). However, the team also examined other aspects of the system that could directly impact cybersecurity – such as the physical security systems protecting the various components.

The design documentation provided by NJT related to the NJ TRANSITGRID project incorporated several security features and best practices that will help ensure the security and resiliency of the microgrid. However, since the system is early in the design phase, the Sandia team identified several potential vulnerabilities and areas that have not yet been defined and will need to be developed in accordance with industry best practices.

While the team recommends that all the findings listed in this report be reviewed and, if possible, mitigated, the team recommends that a review of the network architecture be prioritized. This includes examining the design for inconsistencies in security features such as having an air gap and utilizing data diodes, but then relying on external providers or services such as cellular connections. In addition to this review, the team recommends establishing a formal review process for any modifications in the network architecture that may impact assumptions or introduce inconsistencies.

The Sandia team would like to thank the personnel from NJT, Jacobs Engineering, and AECOM for their assistance with this assessment. Their cooperation and knowledge of the NJ TRANSITGRID project contributed greatly to the success of this effort.

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
ATS	NJ TRANSITGRID Distributed Generation Program Final Design, Construction and Commission Technical Specification
CASA	Cooperative Adversarial Security Assessment
CRADA	Cooperative Research and Development Agreement
DCM	Design Criteria Manual
HMI	Human Machine Interface
IAFC	Section 255000 – Integrated Automation Facility Controls
IDART	Information Design Assurance Red Team
IPSEC	Internet Protocol Security
ISSS	Integrated Site Security System
JEDP	Jacobs Engineering 20% Design Package
LAN	Local Area Network
MCF	Microgrid Central Facility
NJT	New Jersey Transit
PCS	Process Control System
PJM	PJM Interconnection LLC
PV	Photovoltaic (Solar Power)
SCADA	Supervisor Control and Data Acquisition
SDN	Software Defined Networking
SNL	Sandia National Laboratories
VLAN	Virtual Local Area Network
WAN	Wide Area Network

1. INTRODUCTION

This section provides the background and the scope for the assessment, and the layout for the rest of the report.

1.1. Background

Superstorm Sandy caused a major disruption to critical infrastructure – including passenger-rail and other commuter systems - throughout New York and New Jersey. To address this issue, New Jersey Transit (NJT) established the NJ TRANSITGRID project, a $570 million effort designed to power bus, ferry, and limited passenger-rail service within and adjacent to Northeast corridor rail operations between New York City and Newark during natural or man-made disasters, e.g., a future Superstorm Sandy. Given the critical importance of these transportation systems to the region's people and economy, NJT partnered with Sandia National Laboratories (Sandia) to assess the cyber-resilience of the microgrid technologies integrated into this project.

1.2. Scope

This assessment was focused on the security of the information systems – both analog and digital – that monitor and control the electrical systems described in the provided Jacobs Engineering and AECOM design documentation. However, the reliability, performance or capability of the proposed electrical systems – and the ability of the systems to meet the estimated power demand – was not considered. The systems were also not evaluated against other project objectives such as ensuring the site is raised to the FEMA 500-year flood elevation.

Physical security of the system was examined, but only as it related to preventing physical access to the electrical systems (generators, switch gear, etc.) and the monitoring and control systems (workstations, laptops, network equipment, cabling, etc.). The specific characteristics of these physical security components were not evaluated, but that physical security access controls that NJT considers sufficient were included in the design. For example, the team did not consider the resiliency of a specific type of door or lock to physical attacks, but would consider the presence of a locked door sufficient to secure an area to NJT standards.

Since the system is still in the early stages of design, policies and procedures related to the operation, maintenance, and physical security systems were not evaluated. However, the team identified several areas – such as defining which personnel (engineers, custodial staff, facility workers, etc.) would have authorized access to those areas – and included those in Section 0 as recommendations for future development.

1.3. Report Organization

The rest of this report is organized as follows: Section 2 provides an overview of the NJ TRANSITGRID project. Sections 3 and 4 describe the assessment methodology used by the Cooperative Adversarial Security Assessment (CASA) team and the team's assessment activities. The assessment results and the team's recommended mitigations are found in Section 5. Section 6 contains the conclusions of the Sandia team and recommended follow-on activities. Technologies that could be incorporated into the NJ TRANSITGRID to enhance its cybersecurity and resilience are included in Section 7.

2. SYSTEM OVERVIEW

The NJ TRANSITGRID project is designed to allow NJT to continue operations in the event of a major power outage such as that caused by Superstorm Sandy. To allow continuity of operations in the event of another disaster of this scale, the NJ TRANSITGRID project was developed to allow uninterrupted train service to the New Jersey and New York area.

The NJ TRANSITGRID project encompasses a variety of equipment and capabilities to be installed at a number of facilities with two main logical components – the Microgrid Central Facility (MCF) and the seven interconnected NJ TRANSITGRID Facilities. While all of these components are interconnected and together form a microgrid that can operate independently if grid power is lost, these two logical components have fundamentally different roles.

2.1. Microgrid Central Facility

The Microgrid Central Facility (MCF) will be located in Kearny, NJ and is being designed to provide up to 140 MW of power through a combination of gas turbines and steam generators. Gas turbines are considered to be resilient as natural gas transmission was not impacted by Superstorm Sandy. The MCF will provide power for the trains and will control the seven facilities discussed in Section 2.2.

In the event that grid power is lost, the MCF and participating facilities will disconnect from the grid (island) where they will use a combination of power generation at their location and power from the MCF to maintain operations. This will include establishing the necessary command and control systems to operate the microgrid when it is in island mode.

A central control room which will allow for monitoring, alarm response, and control of the microgrid will be established, and is expected to be located at the MCF. This will be manned 24/7 and will be equipped with the various workstations and displays to monitor and control the MCF, the distribution system, facilities, and other components that will make up the microgrid.

Various equipment – generators, switch gear, etc. – will have a local human-machine interface (HMI) available to engineering and maintenance personnel, as well as a remote user interface that can be accessed from the control room. The communication network for this will be a dedicated and redundant Ethernet ring loop using copper or fiber cabling. The design documentation also lays out a defense-in-depth strategy using industry best practices to protect the network, network devices, and other systems from a cyber attack.

There is some contradictory information in the design documentation related to the external connectivity of this network. In some areas, it called for an air-gapped network with dedicated fiber optic cables and data diodes. However, there are other areas that discuss cellular connections, connections to the internet, or the requirement for software to use online activation. (This has been called out as an area to be addressed in Section 0.)

The MCF will include an Integrated Site Security System (ISSS) which shall be a "stand-alone industrial grade system, separate from the CPP Plant Control System."[1] The ISSS will incorporate cybersecurity best practices similar to those of the NJ TRANSITGRID network. The ISSS design includes descriptions of fencing, gates, and other physical protection systems including video surveillance

[1] *NJ TRANSIT TRANSITGRID Phase II NJ TRANSIT Design Criteria Manual;* 09/10/2018

systems. The ISSS design also calls for card readers to access the MCF and other areas – but the kind of card readers to be used has not yet been determined.

2.2. NJ TRANSITGRID Facilities

There are seven facilities that will be part of the NJ TRANSITGRID project. These facilities are:

- Newark Penn Station
- Broad Street Station
- Secaucus Station
- Wayne Bus Garage
- Meadowlands Bus Garage
- Greenville Bus Garage
- Port Imperial Ferry Terminal

These facilities will have their own power generation and storage systems – with the generation primarily being done by natural gas generators, but also including PV systems where practical. Storage is primarily chemical battery systems, but a flywheel energy storage system capable of operating as an uninterruptible power supply will be included at the Wayne Bus Garage.

2.2.1. Facility Descriptions

Newark Penn Station

Located in Newark, NJ this is a four-story building with more than 217,000 square feet of space for waiting rooms, offices, platforms, etc. This facility hosts a number of rail and bus operators. This facility operates on a 24/7/365 schedule. By the number of passengers using a facility, this is the busiest of the facilities in the NJ TRANSITGRID project.

Broad Street Station

Also located in Newark, NJ this is a two-story building with 65,000 square feet of space for offices, retail spaces, and island platforms for passenger waiting and entry. This facility hosts both commuter rail and light rail. The commuter rail operates on a 24/7/365 schedule, while the light rail runs from 5:00 a.m. to midnight daily.

Secaucus Station

Located in Secaucus, NJ this is a three-story building with approximately 321,000 square feet of space for waiting rooms, retail spaces, offices, and utility rooms. This facility hosts both passenger rail and bus operations. The facility operates on a 24/7/365 schedule.

Wayne Bus Garage

Located in Wayne, NJ this is a single-story building with approximately 197,000 square feet of space for offices, maintenance/refueling/storage spaces, and utility rooms. This facility operates on a 24/7/365 schedule. Approximately 100 full-time staff and 300 drivers are employed at this facility.

Meadowlands Bus Garage

Located in Secaucus, NJ this is a single-story building with more than 266,000 square feet of space for offices, maintenance/refueling/storage spaces, and utility rooms. This facility operates on a 24/7/365 schedule. Approximately 100 full-time staff and 300 drivers are employed at this facility.

Greenville Bus Garage

Located in Jersey City, NJ this is a two-story building with approximately 85,000 square feet of space for offices, maintenance/refueling/storage spaces, and locker rooms. This facility also includes a separate parking lot (across the street) large enough to park 25-30 buses. This facility operates on a 24/7/365 schedule.

Port Imperial Ferry Terminal

Located in Weehawken, NJ this is a multi-modal station supporting ferry, light rail, and bus services. This facility operates 16 hours per day; with the passenger parking area open 24/7.

2.2.2. Facility System Characteristics

The requirements for the various facilities include that the generator controls shall be microprocessor based, and "provide automatic starting, monitoring, protection, and control functions for the unit."[2] The design also calls for appropriate displays so monitoring and control can be readily done by appropriate personnel. The design also calls for physical protections of this equipment (padlocking).

There will be two methods for conducting the monitoring and control operations: An HMI touchscreen interface and a remote workstation. The HMI will be co-located with the equipment to allow for local operation. However, the system will also include the necessary network infrastructure to allow a remote workstation to monitor and control the critical components of the system such as controlling breakers, switch gear, and operating the generators themselves. Security will include monitoring settings for any changes and requiring an appropriate password to make those changes. Support for two password-protected security levels is required.

To support remote operations, the system will have a supervisory control and data acquisition (SCADA) network, and interface with a standard IT network. Specifically, the design documentation calls for the Ethernet Modbus TCP/IP protocol for all critical plant control data. In addition, the documentation calls for "redundant, distributed systems to maximize system reliability and fault tolerance."[3] The design documentation calls for a dedicated network, however it also calls for integration with the building management system. (This contradiction has been called out as an area to be addressed in Section 0.)

The system design also calls for automatically maintaining the engine generators at 50-60% loaded by starting or stopping generators as necessary. However, this feature will be controllable by appropriate personnel.

[2] *NJ TRANSITGRID Distributed Generation Program Final Design, Construction and Commision Technical Specification, IFB No. 19-033X* (ATS)

[3] Ibid

3. METHODOLOGY

The base methodology used by the Sandia team for this assessment was the Information Design Assurance Red Team (IDART^{TM}) Methodology developed and maintained by Sandia National Laboratories. Since the system is currently at the 20% design stage, this methodology was selected for its flexibility and its primary focus of design assurance. This methodology is described below.

3.1. The IDART Methodology

The IDART Methodology was developed and refined by Sandia National Laboratories (Sandia) over a period of 15 years as Sandia assessors performed a variety of adversary-based security assessments. This methodology is intentionally designed to be adaptable, agile, and repeatable so as to apply broadly to any target system (i.e., system under assessment). The IDART Methodology has five primary phases: Planning, Data Collection, Characterization, Analysis, and Reporting. These phases are described in Sections 3.1.1 through 3.1.6 and are shown visually in Figure 1. Note that the Data Collection, Characterization, and Analysis phases are performed iteratively as long as the schedule and budget for the assessment support those phases.

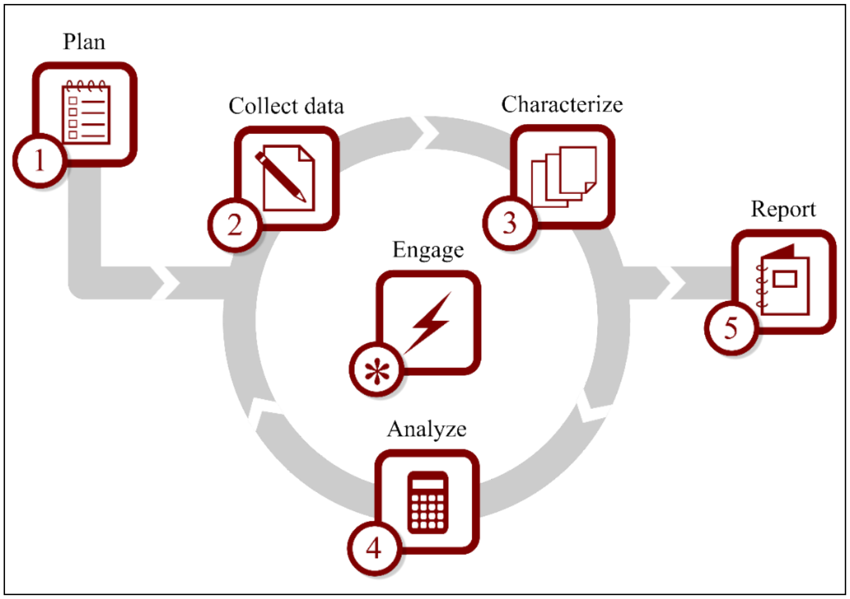

Figure 1: The IDART Methodology

3.1.1. Planning

The Planning phase of the IDART Methodology begins when a potential customer initially contacts the red team with a request for services. In this phase, the potential customer and the red team contact(s) discuss details of the work to be performed, determine an appropriate funding amount, develop a statement of work and execution plan, satisfy legal requirements, assemble a team of assessors and other resources for the project, and finalize project logistics (travel, deadlines, milestones, equipment purchases, classification/sensitivity, rules of engagement, non-disclosure agreements, etc.).

3.1.2. Data Collection

Once the project logistics are solidified in the Planning phase, the red team begins executing the Data Collection phase. During this phase, the red team engages with the customer and performs open-source (and closed-source, if the project allows) collections to amass as many details as possible about the target system, its operating environment, and its mission. As with all of the other phases of the IDART Methodology, the duration of the Data Collection phase is dependent upon the project schedule and funding level. As the assessors execute this phase, they form a solid grasp of the mission and the target system to provide for the customer. From this, the assessors can use their adversary emulation skills to derive possible attacker motivations and establish which sets of attackers would have an interest in the target system, what skills and capabilities such attackers would likely bring to bear against the target system, and what ultimate goals such attackers would hope to achieve when attempting to defeat the security protections of the target system.

3.1.3. Characterization

As the sizable quantity of data gathered in the Data Collection phase presents a steep learning curve and often contains unnecessary details to the red team, the Characterization phase aims to condense this data repository into a set of manageable, abbreviated artifacts that highlight critical aspects of the target system. These artifacts may take on many different forms based on the target system mission, possible attacker motivations/goals, and constraints on the project itself. Most often, however, the Characterization phase results in a set of "views" – concept graphics that highlight critical design, implementation, and/or operational aspects of the target system – that clearly depict how the target system actually functions (as opposed to how it is advertised or believed to function). Using these views, red team assessors can derive possible attacker opportunities. These views are also useful to arrive at "ground truth," as they are easily presentable to the customer and third parties to resolve conflicts in data gathered during the Data Collection phase.

3.1.4. Analysis

In the Analysis phase of the IDART Methodology, the red team project members use their collective expertise to discover viable attack paths that hypothetical attackers could take to achieve their goals in disrupting the mission of the target system. Furthermore, based on the mission of the target system, the red team can reach out across the entirety of their organization's technical staff to supplement their expertise with that of other experts that may deeply understand aspects of the target system that are unique or uncommon. At the conclusion of this phase for a typical red team project, an attack graph–a graph that guides its reader through the necessary steps an attacker would need to successfully execute to achieve a specific goal based on a specific starting state–and other analysis products are developed and, to some degree, vetted. These outputs are of tremendous use when developing mitigations, as the analysis identifies which attacks are easiest (and hence executable by a large number of potential attackers) and present the "lowest hanging fruit" to adversaries' intent on exploiting or attacking the target system.

3.1.5. Engagements

Whenever the red team must interact with the people, processes, or technologies that comprise the target system, this constitutes an engagement. Engagements can occur at any time during the Data Collection, Characterization, or Analysis phases of the project. For example, if a member of the red team were to contact a system administrator (either overtly or under the guise of cover) to ask a question about the security properties of the target system, an engagement supporting data collection would have occurred. Similarly, if an experiment or test were conducted against the target system, the results of such an engagement may support either data collection or analysis, depending on the type of test/experiment.

3.1.6. Reporting

The final phase of the IDART Methodology, Reporting, results in a project report and other deliverables that are tailored for and delivered to the customer. Often, the final project report includes or references all of the documents obtained or generated during the previous phases. Because it is common for a very large set of data to result from executing the Data Collection phase, supplements to the final report are often also delivered to the customer in electronic form to facilitate future security assessments. At the conclusion of the Reporting phase, the project is closed out, with the red team lead and their customer counterparts working intimately to ensure that all tasks in the statement of work were executed and all deliverables were received by the customer.

4. ASSESSMENT ACTIVITIES

The following high-level activities were performed by the assessment team. The observations and findings made during these activities are discussed in Section 0.

4.1. Jacobs Engineering Documentation Review

The CASA team reviewed the Jacobs Engineering 20% Design Package (JEDP) provided by NJT, which included their *Design Criteria Manual* (DCM), and *Section 255000 – Integrated Automation Facility Controls* (IAFC). In particular, the IAFC contained a specific section on Cyber Security that provided a description of their security strategy. These design documents were focused on the Microgrid Central Facility (MCF) and its interconnections with PJM and the NJ TRANSITGRID substations, transmission lines, and distribution infrastructure.

Review of these documents (and others in the JEDP) led to a number of follow-on questions that were provided to Jacobs Engineering. These questions were discussed on a number of teleconferences held with Sandia, NJT, Jacobs Engineering, and AECOM personnel. From these discussions, areas of concern were identified – along with multiple areas that meet or exceed industry best practice. These results are found in Section 0. In addition, many areas that were beyond the 20% design stage were identified, and the assessment team was able to provide input to Jacobs Engineering to ensure those areas were included, and followed best practices, when developed later in the lifecycle.

4.2. AECOM Documentation Review

The CASA team also reviewed the 20% Design Package from AECOM provided by NJT, which included the NJ TRANSITGRID Distributed Generation Program Final Design, Construction and Commission Technical Specification, IFB No. 19-033X (ATS). This document focused on the infrastructure for the various facilities that will be supported by the NJ TRANSITGRID project. While a number of information systems related to command and control were discussed in the documentation, further discussions with AECOM indicated that the specifics of their cybersecurity approach would be developed later in the system lifecycle.

5. ASSESSMENT RESULTS AND RECOMMENDATIONS

Results obtained from the activities described in Section 0 are provided in this section. These findings include strengths, weaknesses, and observations made by the team.

The team uses the following definitions for strengths, weaknesses, and observations:

- Strengths are the processes, procedures, or other aspects of the system that increase the difficulty of a successful attack, or limit/remove various attack vectors. These are included to ensure that these practices are continued as the systems evolves over time and are not disabled or discontinued as part of mitigation plans.
- Weaknesses are the procedures, controls, implementation details, or vulnerabilities that could provide an attack vector, contribute to successful attacks using other vectors, or prevent the timely detection of an attack. These enumerate the potential risks and vulnerabilities of the target system to enable corrective actions by the system owner.
- Observations include all other items of note observed by the assessment team that are not classified as strengths or weaknesses. These can include items outside the scope of the assessment, where not enough information was available to make that determination or are "non-actionable" items. Non-actionable items may be weaknesses that cannot be changed or modified due to external requirements such as laws or regulations.

In addition, weaknesses include a severity rating of HIGH, MODERATE, and LOW to represent the team's evaluation of the overall severity of that specific weakness. To perform this evaluation, the team begins by weighing the answers to the following questions:

- What level of damage could be expected from a successful attack?
- How widespread is the damage from the attack? (Single user/system, single facility, Domain-wide, etc.)
- How easy is it to reproduce the attack and result?
- What skill level is required to perform the attack?
- How difficult is it to detect the attack given current implemented protections?

However, the assessment team goes beyond these basic questions to apply a variety of additional rating systems that are based on any adversaries of concern; consequences of concern; adversary motivations and capabilities; potential for alternative attack targets that could achieve the same goal; and other reality filters that are informed by their experience and threat intelligence.

The outputs of these various rating systems are combined by the team members and relevant subject matter experts in a qualitative process to obtain the overall rating. The assessment team recommends that NJT primarily focus on mitigating issues in the order of severity. However, since implementing mitigations may require different levels of resources, these ratings should be used as a guide and not dictate mitigating actions.

5.1. Weaknesses

(High) Network architecture documentation is inconsistent regarding air gaps, possible use of data diodes, and use of external connections and services.

Justification: In Section 15.1 of the NJ TRANSITGRID Phase II: Design Criteria Manual, the document states: *This network shall not be connected to the Internet and no Cloud services are allowed – an air gap shall be maintained; communications to remote facilities shall be via dedicated fiber optic cables with data diode (one way communications) and/or firewalls for cyber security protection.*

However, in Section 1.3, Item B of the IAFC, it states: "The Plant Control System's Electrical Distribution can be controlled and monitored by a separate Supervisory Control and Data Acquisition (SCADA) System" and lists multiple facilities that will require bidirectional communication, preventing the use of data diodes. In addition, Item J in the same Section indicates that control room workstations will be able to *download software programs*. Section 2.2, Item D of the same document states: "The system shall integrate with components of each sub-system, sub-system to sub-system, control network to data network (LAN/WAN and intranet/internet), and third-party interfaces in a manner transparent to the operator." This seems to indicate that there will be external connectivity to the internet.

In addition, Section 2.5, Item I, bullet #10 states: "System must be able to function through periods of no internet access, no land line telephones service, and no cellular reception" which also indicates external connections into the network.

Finally, Item D, bullet #10 requires the firewall/security gateway to: "Configure VPN to restrict unauthorized access from the Internet", which implies that VPN access from the Internet will be possible.

These seemingly inconsistent requirements or statements may result in the assumption that some parts of the network are protected by an air gap or other architectural features when an external connection or configuration in another system or facility has compromised this protection.

Mitigations: To avoid potential vulnerabilities or unknown side effects from network configurations, it is recommended that a network diagram specifically illustrating the required directionality of the traffic (i.e., can a data diode be used), and color coded to indicate if a connection is using external resources such as a VPN, leased line, or cellular connection; or if it is going over dedicated network connections such as copper or fiber cabling. This diagram should then be reviewed by network architects to determine if vulnerabilities have been introduced.

In addition, the team recommends having a change process for the network architecture that specifically reviews proposed changes for the potential to change network connectivity or security assumptions. For example, changing copper cabling to fiber would not impact these assumptions; however, changing from dedicated fiber to a leased T1 line would introduce an external connection via the leased line provider.

(Moderate) The password protection for NJ TRANSITGRID Facility HMIs only requires support for numeric passwords instead of a full character set.

Justification: Item 10 in Section 2.15 HMI SCREEN LISTING, in the ATS document states: "Password entry screen that shall contain a numeric keypad for password entry" However, in *Section 5.1.1.1 Memorized Secret Authenticators in NIST Publication 800-63B, it states:*

> *Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber. Memorized secrets chosen randomly by the CSP or verifier SHALL be at least 6 characters in length and MAY be entirely numeric. If the CSP or verifier disallows a chosen memorized secret based on its appearance on a blacklist of compromised values, the subscriber SHALL be required to choose a different memorized secret. No other complexity requirements for memorized secrets SHOULD be imposed.*

While a numeric only password can meet NIST guidance if it is randomly generated, policies related to password creation and use have not yet been developed.

Mitigations: Ensure that the policies for the HMI interface passwords meet the NIST guidance for numeric-only passwords (i.e., they must be at least 6 characters in length and randomly generated).

(Moderate) Operating systems listed as minimum requirements are past end-of-life.

Justification: In Section 2.2 *Network Architecture* of the IFC, Item J states the OS shall be: "The Latest Windows Operating System compatible with the PCS hardware and software for process control and monitoring." This requirement is modified slightly in other areas of the document with Item M stating that the PCS workstations will use "Microsoft Windows 7 Professional 64 bit"; Item P has the same requirement for the wall-mount PCS view node. Item R states that the PCS servers have a requirement to use "Microsoft Windows Server 2012 R2."

These items do come with a caveat that the system shall "meet or exceed the requirements."

Windows 7 support ended on January 14, 2020 and, while Windows Server 2012 R2 is still in support, that ends January 10, 2023 – which may be prior to the deployment of these systems, or shortly after, preventing security updates from being received.

Mitigations: While process control and monitoring software may not work properly on the latest version of the Windows operating system available at deployment time, the team recommends that the requirement be to strictly use the latest OS version that is compatible with the software. In addition, the team recommends compatibility with an operating system that has several years of support remaining be considered during the procurement process.

(Moderate) The system administrator will be able to lockout any or all workstations from the NJ TRANSITGRID system.

Justification: If an attacker compromises the administrator account, or gains administrator privileges on a single system, they would be able to lockout all of the workstations providing monitoring and control of the microgrid. This would prevent authorized personnel from responding to or correcting any malicious activities taken by the attacker. Depending on the configuration of this feature, this may also include locking out the workstation that was compromised by the attacker. This would mean that, while authorized personnel could log into the workstations, they would no longer be able to exert control over the microgrid.

Mitigations: Configure the system such that the administrator or other account is always able to access the system regardless of the workstation they are logging in from. In addition, the administrator or other designated account should always have the ability to remove the lockouts.

(Low) Accounts are locked out after 3 failed logon attempts which could result in a denial-of-service attack (bullets 5 and 8)

Justification: In Section 2.5 of the IAFC, Item I, bullets 5 and 8 state that accounts are locked out after 3 attempts until reset by the System Administrator. This means that an attacker with a list of usernames could cycle through all of the users with incorrect passwords and lock out all of the valid users.

Mitigations: Instead of a hard retry limit, an increasing time delay progression (e.g., 2 seconds, 5 seconds, 10 seconds, and then 30 seconds) could be used to prevent brute force attacks. Alternatively, the account lockout could be temporary (e.g. 5 minutes) to ensure that authorized users will be able to access their accounts in a timely manner without the need for system administrator assistance.

(Low) The requirement for password deactivation is "as soon as possible" instead of a specific time requirement

Justification: In Section 2.5 of the IAFC, Item I, bullet 7 indicates that password deactivation should be done as soon as possible. However, this could result in passwords remaining active for some time after they are scheduled for deactivation. For example, if the system administrator has gone home for the weekend (or is on vacation) this could mean the password stays active for several days. This would provide a large window of time where an unauthorized individual could gain access to the system.

Mitigations: Change the verbiage to indicate a precise timeframe such as "same business day" or "next business day." Industry best practice is to disable these accounts at the same time the person is conducting their off-boarding process, but that may not be practical for the process control systems.

(Low) Backing up of log files is not listed as a requirement.

Justification: Log files are not listed as artifacts that need to be included in system backups. However, this could mean that valuable information related to malicious behavior or component failure is not preserved, preventing a root-cause analysis for a system failure or anomalous behavior, and would allow an attacker to delete evidence of their activity.

Mitigations: Use a centralized logging system such as syslog to ensure that any log entries related to a system failure or attacker actions are preserved. Ensure that the syslog server is also included in regular backup processes.

5.2. Observations

Exposed areas require using a galvanized steel conduit, but how areas are designated as exposed is unclear.

Description: An unprotected communication cable could be used as an attack vector into the network. However, an area that is not exposed, but is still generally unobserved, could provide an insider or an attacker who has gained physical access the opportunity to tap into the cable. The installation of a device with Wi-Fi, cellular, or other wireless communication would allow them to maintain access even after leaving the area.

Mitigations: For designating areas as exposed (or not exposed), establish a process that takes into account the ability of an attacker to remain unobserved long enough to tap into the cable and install a malicious device.

Policies related to physical access to the HMI systems should consider the insider threat.

Description: If custodians, facilities staff, maintenance contractors, or other personnel are given unrestricted, unescorted, or unobserved access to the HMI systems, then a malicious (or even curious) insider could interfere with or damage the system.

Mitigations: Ensure that policies reflect the necessary level of background checks or screening necessary for all personnel that have physical access to the HMI systems. If third parties are used for custodial activities, facilities work, or other activities, their screening processes should also be reviewed to ensure they provide the necessary assurance for their personnel. In the event the screening process for these other personnel does not meet security requirements, policies related to escorting workers should be developed. In addition, deterrent controls – such as signage indicating only authorized personnel should access the system – could be installed around the HMI systems.

Policies related to the existence, creation, maintenance, and use of manufacturer or third-party administrator accounts should be established.

Description: To ensure access in the event of a device error or software failure, some devices are configured to have an account that can always be accessed by maintenance personnel. This is sometimes done by having “secret” patterns to touch on a touchscreen, or hardcoded username/password combinations. In addition, third-party contractors may configure the devices to have their own accounts for maintenance purposes. The existence of these accounts can provide access to the device by individuals who are aware of these accounts and, if these accounts are shared by multiple individuals, prevent auditing and accountability.

Mitigations: If practical, devices should be selected that do not have backdoor accounts, or other universal username and password combinations. However, if a device does have these accounts, configuration policies should require the default passwords be changed once the device is deployed. In addition, if there are maintenance accounts that maintenance personnel will use for device access, these devices should use the same password policy as other systems in the network. For example, these policies should include defining the required password complexity, time period to change the password, and require the password to be changed if there is a change in personnel, suspected password compromise, or other event related to the security of the login credentials.

Policies related to the creation, maintenance, and use of shared accounts should be established.

Description: Standard best practice is for every user of a system to have their own account to allow for proper auditing and accountability. However, some devices do not support this ability. For example:

- A device may simply have a lock screen instead of supporting multiple users
- Authentication for a single user account across the entire system may not be available, resulting in prohibitive administration overhead
- The need for emergency actions may require users have a guaranteed method to gain access to the system to perform operations

Mitigations: Develop policies that govern the creation and maintenance of these accounts. At a minimum, these policies should define a process for approving these accounts, detail how these accounts will be maintained and updated, and how widespread these accounts will be. For example, will the account be used for all devices of the same type, or will they be limited to a specific NJ TRANSITGRID facility, or created and used based on job responsibilities? These policies should also identify the personnel, and from which organization, these accounts can be created and used by.

Policies governing how updates and patches will be transferred to the NJ TRANSITGRID network should be developed. This should include signature updates for intrusion detection/prevention systems.

Description: This item is dependent on the results of the network architecture review related to the use of air gaps, data diodes, etc. For example, if external connections are allowed, then a central proxy used by all systems in the microgrid to obtain updates could be configured. If there are no external connections, then any updates will have to be brought across on removable media.

Mitigations: Mitigations or policies will be dependent on the results of the overall network architecture. However, any point of interconnection should be considered a potential attack vector into the microgrid and protected and monitored appropriately.

Use of centralized services such as NTP and syslog should be considered.

Justification: Utilizing syslog is discussed in Section 0, however, in addition to preserving the logs, if the systems do not have synchronized clocks it is far more difficult to troubleshoot network issues or system failures. Lack of synchronization can also hinder incident response activities and investigations.

Mitigations: Establish an NTP server (and other centralized services) on the microgrid network and configure systems to utilize these services. To maintain network isolation, an NTP hardware appliance that gets its time from GPS could be used.

Best practices related to network equipment should be applied.

Justification: To ensure that a compromise of one system does not allow an attacker unrestricted access to the entire network, and to ensure that any intrusion detection devices are positioned to detect malicious activity, industry best practices related to network security should be applied.

Mitigations: After the final network architecture discussed in Section 0 is completed, VLANs, network segmentation, and other best practices should be applied to the network equipment configurations.

Given the expected use of third- party contractors, supply chain risk management processes should be used.

Justification: The design documentation explicitly calls out the use of sub-contractors (or third parties). These sub-contractors may use unknown or unexpected suppliers or vendors in their normal work processes, allowing malicious or inappropriate components to be integrated into construction.

Mitigations: The National Risk Management Center (NRMC), housed within the Cybersecurity and Infrastructure Security Agency (CISA), is one of the key components of CISA's risk advisory role. The NRMC has worked with government and industry partners to provide supply chain risk management guidelines, resources, and training for industry.[4] The CASA team recommends using this information to ensure that critical components of the NJ TRANSITGRID project are not stolen, replaced with inappropriate or counterfeit components, altered, or compromised prior to their use in the project.

5.3. Strengths

Network Architecture:

- The network design specifically calls for a physically separate network, using dedicated switches.
- The network is required to have redundancy to ensure there is no single point of failure. The supervisory networks are required to use a non-proprietary topology and use open source protocols.
- The supervisory network is required to be EMI and RFI noise tolerant.

[4] https://www.cisa.gov/supply-chain

Network Equipment and Capabilities:

- Network equipment is required to be capable of Virtual LAN segmentation.
- The firewall/security gateway is required to support IPsec, SSH, and TLS.
- The firewall/security gateway will perform stateful inspection.

Microgrid Systems and Configuration:

- The Emergency Power System Automation and Controls are required to be the same manufacturer as the switchgear and generator sets to avoid any compatibility issues.
- The system design calls for the hardware configuration to have 20% spare I/O points/modules, and 20% spare cabinet space.
- The system design specifically requires that manufacturer's default password must be changed prior to installation in the system.

Operations:

- Two-factor authentication is called out in the design documentation.
- The system design calls for off-site backups of critical data and configurations.
- The system design recommends using a double interlock preaction fire system for the main electrical room. (This allows manual cancellation in the event a fire is contained.)

Security Management:

- The design documentation requires the development of a network security plan.
- The design documentation requires the development of a change management program.
- The design documentation specifically calls out the requirement to immediately report any questions about the power system design (or other aspect) "At any time during engineering, design or construction".

Testing:

- Cybersecurity testing once the system is deployed is required to verify the defense-in-depth measures are effective.
- Redundancy testing is required to verify the system remains available, and can recover, in the event of a component failure.

6. CONCLUSIONS AND FOLLOW-ON ACTIVITIES

The design documentation provided by NJT related to the NJ TRANSITGRID project incorporated several security features and best practices that will help ensure the security and resiliency of the microgrid. However, since the system is early in the design phase, the Sandia team identified several potential vulnerabilities and areas that have not yet been defined and will need to be developed in accordance with industry best practices.

While the team recommends all the findings listed in this report be reviewed and, if possible, mitigated, the team recommends that a review of the network architecture be prioritized. This includes examining the design for inconsistencies in security features such as having an air gap, utilizing data diodes, and relying on external providers or services such as cellular connections. In addition to this review, the team recommends the establishment of a formal review process for any modifications in the network architecture that may impact assumptions or introduce inconsistencies.

The Sandia team would like to thank the personnel from NJT, Jacobs Engineering, and AECOM for their assistance with this assessment. Their cooperation and knowledge of the NJ TRANSITGRID project contributed greatly to the success effort.

For follow-on activities, the Sandia team recommends additional assessments as the system design matures and is implemented. At a minimum, the team recommends two additional assessments:

1) A design assurance assessment when the system reaches the 100% design point to ensure that design updates do not introduce additional vulnerabilities.
2) A vulnerability assessment once the system is operational and, ideally, prior to production operation so the difference between the as-designed and the as-built can be evaluated.

7. POTENTIAL HARDENING FEATURES

The Sandia team proposes working with NJT and NJ TRANSITGRID contractors participating in the architecture and design process to integrate state-of-the-art hardening elements into the NJ TRANSITGRID system.

These hardening features could include:

1. **Network Design**. The team could help support cyber-physical architecture planning using consequence-driven assessments to optimize cyber barriers (data diodes, proxies, firewalls, virtual local area networks (VLANs), air gaps, etc.) for the NJT internal OT network and external connections to other IT and OT systems.
2. **Network-based Intrusion Detection System (NIDS)**. The team would work with the NJT team to select the appropriate network monitoring points for network taps (e.g., SPAN ports), and then select the appropriate software package. Additionally, the team could investigate behavior-based anomaly detection (AD) technologies, refine machine learning-based AD technologies to secure the system, generation sources, and critical loads. These tools could be signature-based or behavior-based:
    a. **Signature-based** NIDS tools detect malware using deep packet inspection. Both open source and commercially available solutions are available for consumers in a variety of sectors, including Information Technology (IT), energy, financial, or government. Depending on the sector that the IDS is being applied, the signatures will be tailored to detect threats specific to those systems.
    b. **Behavior-based** techniques employ one or more algorithms to detect known and unknown patterns through inference. Various types of statistical learning and classification techniques have been used to solve this problem including supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning methods.
3. **Host-based Intrusion Detection System (HIDS)**. A host-based IDS inspects the integrity of the host itself by examining several host-based features such as system files, system calls, processes, and network communications. The IDS typically shares system resources with the host and can either be placed in-line or in parallel to the flow of traffic to and from the host. Host-based IDS technologies typically require elevated privileges on the host to track the state of system-level files and execute responsive actions. For this reason, it important that the IDS itself be secured and protected against attacks as compromises could lead to unauthorized administrator level access. Host-based IDS can monitor processes, executables, registry entries, RAM, processor utilization, memory utilization, or a variety of other host-based features to alert an operator to indicators of attacks. Host-based IDSs are useful when adversaries affect the features that are being monitored when an end device is compromised.
4. **Security Information and Event Management (SIEM)**. When an alert is detected by an IDS, typically an alert will be generated and communicated to a Security Information and Event Management (SIEM) system for operators to monitor. Several operators will monitor such alerts in a Security Operation Center (SOC) room dedicated to security personnel. Depending on the events detected, the role of an operator within a SOC would be to respond to mitigate any potential threats alerted by the IDS.
5. **Security Orchestration, Automation and Response (SOAR)**. SOAR technologies are software suites that augment SIEM tools to prioritize security events, automate responses to

low-level threats, and support incident response. There are commercial SOAR solutions from multiple vendors including LogRhythm, Rapid7, CyberSponse, DeMisto/XSOAR, Cyberbit, IBM, and others.

6. **Deception techniques**. The team proposes deploying honeypots within the NJ TRANSITGRID system using Sandia's High-Fidelity Adaptive Deception & Emulation System (HADES) technology. HADES platform is a deception environment that utilizes Software Defined Networks (SDN), cloud computing, dynamic deception, and agentless Virtual Machine Introspection (VMI). These elements fuse to not only create complex, high-fidelity deception networks, but also provide mechanisms to directly interact with the adversary—something current deception products do not facilitate. At the onset of an attack, adversaries are migrated into an emulated deception environment, where they can carry out their attacks on canary systems without any indication that they have been detected or are being observed. HADES then allows the defender to react to adversarial attacks in a methodical and proactive manner by modifying the environment, host attributes, files, and the network itself in real-time. Through a rich set of data and analytics, cybersecurity practitioners gain valuable information about the tools and techniques used by their adversaries, which can then be fed back to the network defender as threat intelligence.
7. **Moving Target Defense (MTD)**. Proactive defense technologies are just beginning to emerge. A R&D100-winning CEDS-funded project called Artificial Diversity and Defense Security (ADDSec) led by Sandia demonstrated moving target defense (MTD) using software defined networks was effective in military microgrid deployments. Similar technologies could be evaluated for the NJ TRANSITGRID project.

The NJ TRANSITGRID leadership are encouraged to consider these R&D areas and others for deployment on the microgrid networks to create a best-in-class cybersecurity defense system.

APPENDIX A. JACOBS' RESPONSES TO SANDIA REVIEW QUESTIONS

The tables in this section contain questions generated by the CASA team from the provided documentation, the response from Jacobs Engineering, documentation and other references pertaining to the questions and responses, and possible action items for Jacobs Engineering.

The Excel spreadsheet providing the source material for these tables were generated by Jacobs Engineering.

A.1. Physical Security

QUESTION	JACOBS RESPONSE	TEAM COMMENTS
What is considered tamper-proof cables?	This is listed in the Design Criteria Manual 15.3.4.6 & 21.5.1. Tamper proof cables achieved by having cable in conduit (vs open tray) and terminal boxes/panels with tamper alarm switches; pull boxes can use special security keyed screws/bolts. Design Criteria manual sections 21.6.6.5.d, 21.6.6.7.a, and 22.2.1.3 call out the use of tamper proof hardware and alarm switches. Also, Specification 283310, 3.4.O calls out: O. "Provide tamper resistant features and fasteners on all exposed junction boxes or enclosures."	Resolved
It is mentioned that cables will be placed in a galvanized steel conduit in exposed areas. What is considered an exposed area, and are any of these areas accessible to the public?	Spec 283318, 3.H calls out: H. "Security cable and signal wire shall be installed in separate conduit system or utilize armored cable."	

QUESTION	JACOBS RESPONSE	TEAM COMMENTS
Is the Weehawken tunnel considered an exposed area?	The Webster Definition of 'Exposed' is: open to view; not shielded or protected. The area is open to view, however, that area is posted and fenced for minimal protection.	Are there any security cameras on the tunnel? Any regular police patrols? Current NJT physical security specs, camera requirements? Minimize ease of access. DCM update for requirement to document survey of potential exposed areas and mitigating actions to preclude intrusion. Eventual Red Team evaluate for vulnerabilities. Probably during installation phase. Red Team during pre-installation/final design phase.
For exterior areas, what kind of fencing or barriers will be used?	Exact fencing to be installed will be determined in the final design. The Design Criteria Manual noted perimeter fence to be 8ft high with barbed wire at the top. Specification 283310 calls out the design requirements for a perimeter intrusion detection system on the CPP fence.	Resolved
Are physical keys/locks expected to be used to secure communication enclosures?	Physical keylocks will be used in the facilities and specific details of key lockers and use will be covered in the detailed design. Specification 283310, 1.3.I.15.b.3 notes that keys are a backup use, 1.5.C.27 refers to UL-437 for key locks; communication enclosures should have tamper proof designs and/or tamper switch alarms.	Resolved

QUESTION	JACOBS RESPONSE	TEAM COMMENTS
The Control Room floor plan shows three entrances/exits with two being protected by a card badging system. How will the third door be protected?	There are 3 doors in the Control Room: to the hallway, to the operating floor and to the Server room (the Server Room has another door to the hallway as shown on drawings PP-A-003. Dwg PP-SS-002 incudes a door schedule that shows the Control Room door to the hallway and the plant operating floor have card readers; the same schedule lists both server room doors as having card readers.	Server room details not yet designed.
If IP cameras are used, how will the network traffic for these be protected?	The Integrated Site Security System is shown on dwg SS-PP-051. the CPP site shall have video camera coverage. Specification 283310 addresses security network (which would include the camera system): 1.3.F.2 - incorporation of firewalls, segmentation and DMZs 1.4.A.1 - requires submittal for network configuration from going from 20% to final design. 3.7.R - requires cyber security testing of network intrusion 1.5.C.11 - invokes IEC-62443 requirements	Resolved

A.2. Control Room

QUESTION	JACOBS RESPONSE	ACTION REQUIRED	TEAM COMMENTS
How will physical access to the HMI be controlled? Is it expected that individuals who are not authorized to access the HMI will have unrestricted access to the secure space containing the HMI? (For example, custodial or facilities staff.)	The Owner/Operator entity will develop personnel HR policies and plant operating policies and procedures. Specification 255000, 2.5.E thru I call out system access details; 2.5.K calls for an Intrusion Detection System that would notify defined persons of intrusion detections.	Owner/Operator Policy & Procedures Required	Ongoing training for personnel in malicious threats, etc.
Will there be a single "maintenance account" or "maintenance functionality" for those trained by Jacobs Engineering to access the system if there are system problems?	This will be developed by the Owner/Operator during detailed design completion and contractual requirements.	Owner/Operator Policy & Procedures Required	Single sign-on account for maintenance staff (IC techs) to perform work on HMI/control room, each has own user account/password. Use CMMS to track (e.g. Maximo). Rights would need to be defined to track individual access.
Will there be a "maintenance account" or "maintenance functionality" specifically for technicians with Jacobs Engineering?	This will be developed by the Owner/Operator during detailed design completion and contractual requirements.F8	Owner/Operator Policy & Procedures Required	addressed above.
How will HMI updates be handled? Will they require signed updates – and will this be done by a vendor, on-site personnel, or will the system download them from the vendor website?	Specification 255000 calls out: "Anti-virus and Malware detection software updates shall be controlled by Engineering in conjunction with IT; no automatic updates." 1.6.B.4 requires a Patch management program submittal from the SBOM for review. 3.5 requires verification that the latest software version and patches are installed prior to the FAT		Resolved

QUESTION	JACOBS RESPONSE	ACTION REQUIRED	TEAM COMMENTS
	and SAT. The Design Criteria Manual section 15.1 also calls for a Patch management program.		

A.3. Backups and Data Storage

QUESTION	JACOBS RESPONSE	ACTION REQUIRED	TEAM COMMENTS
Will there be a possibility of cloud backups of historical data, reports, or system configurations?	it is possible but would have to be submitted upon for review during the design evolution from 20% to 100%. Specification 255000, 2.5.K requires the Intrusion Detection System to be on premises - not hosted in the cloud. Design Criterial Manual section 15.1: Network communications shall use a redundant Ethernet ring loop and gateways as needed to interface to multiple vendor equipment. This network shall not be connected to the Internet and no Cloud services are allowed – an air gap shall be maintained; communications to remote facilities shall be via dedicated fiber optic cables with data diode (one-way communications) and/or firewalls for cyber security protection."		Only one-way comms from remote station? Basically, set up currently as one-way data comms supplemented by vox for coordination. Plant monitored by ROC and plant. Need to id/define ROC-Plant data exchange. EMS located at MCF. How push data to EMS? Operational Plan to be developed. Specify performance characteristics/data requirements as part of RFP process. Ramp rate limitations a concern; batteries good solution.
If so, what protections will be considered?	See above.		
Will a version control system be used to allow access to previous configurations, documents, and files?	Question is not understood.	Sandia to clarify question	Version history to track/document issues/vulnerabilities. Assist with integrating new devices. Applicable to hardware and software. Share

QUESTION	JACOBS RESPONSE	ACTION REQUIRED	TEAM COMMENTS
			updates with Sandia as RFP developed.
Who will be allowed to initiate an off-site backup?	This will be defined as part of the 20 to 100% design evolution. Specification 255000, section 2.6 has backup criteria .		Resolved
Will designated ports be left open to plug in physical media to back up data?	Port controls are noted in specification 255000, sections: 1.2.M, 2.5.D ("Unused services in the operating system and device ports shall be disabled".), and 3.5.D.10.f.2, 7, & 8 address unused ports.		Resolved
What policies and procedures will be in place for records retention and deletion of archived data?	This will be developed by the Owner/Operator during detailed design completion and contractual requirements.	Owner/Operator Policy & Procedures Required	Resolved

A.4. Field Instruments & Control Valves

QUESTION	JACOBS RESPONSE	ACTION REQUIRED	TEAM COMMENTS
What protections will be put in place to protect the digital valves and positioners from being modified through Modbus TCP or HART	Owner/Operator will develop policies & procedures and train plant personnel in same for security as well as maintenance activities. This should include a Work Order management system that would be auditable and a supervisory check of all work activities by technicians or any manufacturer on site.	Owner/Operator Policy & Procedures Required	Beef up Inst spec.
How will updates to the HART Communicators be handled since licensing is done via the Web?	Discussions with local Emerson rep (TX) indicated that they could do updates via hard files (disc, thumb drive) in lieu of web. Remains to be verified.	Revise 253000 to follow 255000 more closely	How are malware scans handled - do onsite, kiosks recommended? Recommend burning to a disc versus thumb drives.
How will these updates be verified?	No ; will follow 255000, 2.5 that notes "no automatic updates".		
Will these updates be automatic?			
If possible, will the manufacturer's equipment default usernames be changed?	Yes, will need to update spec similar to specification 255000, 2.5.B: "Evaluate and incorporate equipment manufacturer security recommendations as applicable. Change manufacturer's equipment default passwords prior to installation in the system."		
Will the ICS Cert check be performed periodically? How long between checks?	The 255000 spec calls for ICS CERT checks and inventory list submittal in 1.4.A.2.f.6, performed per 2.5.C in design development/equipment selection. Frequency of checks will be an Owner/Operator developed policy & procedure.		

A.5. System Login Requirements

QUESTION	JACOBS RESPONSE	TEAM COMMENTS
What user encryption software will be used to store credentials?	That is beyond a 20% design and will be determined during design evolution to 100%.	
Who will have access to configurable password account?	See 255000 section 2.5	
Will user chosen passwords be compared to a blacklist of previously used/cracked passwords?	See 255000 section 2.5	Refine spec to address. Wiki article on most common passwords. NJT weighing guidance on password expiration timeframe.
What second means of user login authentication will be required?	See 255000 section 2.5.h.10; exact products will be determined, submitted, reviewed and approved during the 20 to 100% design evolution.	
Will password requirements be applied on all applicable machines across the plant?	Certain equipment, such as the combustion turbine generators have their own local control panels and were specified to meet cyber security requirements for passwords and access.	Contained in CTG spec.
Is there any guidance for password complexity or how often passwords need to be changed?	See 255000 section 2.5	Addressed.

A.6. Remote Monitoring & Control

QUESTION	JACOBS RESPONSE	ACTION REQUIRED	TEAM COMMENTS
Will the remote locations be rooms on-site, or will there also be a location off-site that can be accessed from?	See 255000 section 2.5.H.10 & 11; also 2.7.D.17 requires a Network Security Plan as part of the 20 to 100% design evolution		TBD
Who can connect remotely and where are these connections allowed from? Operator home offices? Jacobs Engineering offices?	See Dwg PP-IC-051, PP-CM-051. See Design Criteria Manual section 15.1. Specification 255000, 1.3.P, 2.7.E calls out use of data diodes for remote sites		TBD
What type of hybrid firewalls will be implemented?	See specification 255000, 2.7.D for firewall details; firewalls to be tested per 3.5.C.10		
Will a combination of blacklisting and whitelisting be used?	Spec 255000, 2.7.D.5 calls for whitelist anti-virus and malware protection		
Site Communication Block Diagram shows a singular router and communications switch serving what appears to be both the IT and OT portions of the plant. This router is also shown to be connected to the internet via a dedicated fiber through a firewall. Is this correct? If correct, is there a reason for having the IT/OT sides managed by the same switch?	Dwg PP-CM-01 is for Emergency point to point/conference calls between associated rail entities dependent upon the power plant. System requirements are called out in Specification 273010.		intended for voice comms
Will the proposed intrusion detection system/intrusion prevention system be able to detect changes in values passed to PLCs, remote I/O, etc.?	The IDS requirements are called out in 255000, 2.5.K and notes monitoring the network for unauthorized or abnormal traffic.	Add wording to clearly include network traffic from PLCs and remote I/O	

QUESTION	JACOBS RESPONSE	ACTION REQUIRED	TEAM COMMENTS
Is it possible to get a physical diagram that shows where remote monitoring, and control workstations/sites are physically located in relation to each other? In particular, will leased lines or ISPs be required to connect the various sites to the remote monitoring and control locations?	The full design drawing package has this physical information. The OWS are shown in the control room of the CPP on PP-IC-051.		
How are the remote monitoring and control workstations secured?	CPP OWS are with the control room which is card key access or by plant management authorization. OWS access is by user login and passwords. Local OWS, such as the combustion turbine is at the local panel that also requires login and passwords.		Beef up engineering laptop security access
Will this system have an internet connection for external communication and/or information access? (Ex. Access other New Jersey Government websites or email accounts.)	There is to be a separate Corporate IT computer structure for plant personnel that would have access via ISP to internet; but this network is isolated from the plant controls, security, and emergency comms.		Clarify computer access operational control vs personal

A.7. Maintenance & Troubleshooting

QUESTION	JACOBS RESPONSE	ACTION REQUIRED	TEAM COMMENTS
How will maintenance and troubleshooting of the various systems be performed?	This will be developed by the Owner/Operator during detailed design completion and contractual requirements.	Owner/Operator Policy & Procedures Required	
Will the technicians use the Engineer laptop to plug into the systems or will there be use of outside laptops?	This will be developed by the Owner/Operator during detailed design completion and contractual requirements. The Engineering laptop should be kept in a secured location with a sign out access log.	Owner/Operator Policy & Procedures Required	see 38 above, vendor equipment laptops too
Are the systems expected to have an external connection and/or "phone home" to report diagnostic information? If so, how is this connection monitored and secured?	No, specification 255000, 2.7.D.17 requires a Network Security Plan as part of the 20 to 100% design evolution.		
Will version control be used to facilitate rolling back any system changes?	System back up and patch management are discussed in Specification 255000.		check details for system backups/frequency?
Is the time to perform maintenance or repair operations in-line with the maximum outage/failure time that can be tolerated?	The plant is an N+1 design. The plant operator will be in control of maintenance & repair activities & schedules. This is beyond a 20% design package	Owner/Operator Policy & Procedures Required	Post event spare parts
What is the estimated time between receiving a software update for anti-virus and/or malware detection software and installation since automatic updates are disabled?	This is beyond an engineering design package. It is dependent on what systems and equipment are actually selected and installed as well as the respective manufacturers. The Operator will manage this activity.		
How will the signature list for the signature-based IDS/IPS be kept up to date? **Will this be automatic or manual as in the case of the anti-virus/malware updates?**	The design basis does not allow automatic updates; this is to allow another step in the process to control/monitor such activities. Specification 255000, 2.5.K.5 calls for: Provide a list of signatures and define the means as to how		

QUESTION	JACOBS RESPONSE	ACTION REQUIRED	TEAM COMMENTS
	this list shall be kept current; update means shall be coordinated with Owner.		

A.8. IT/OT Networking

QUESTION	JACOBS RESPONSE
If there are additional external connections from the remote monitoring and control workstations can a network diagram of those systems, connections, protocols, and encryption also be provided?	The known connections at this time are shown on the dwg set
Is it possible to get a physical layout diagram showing where the physical control and network cables will be located? If any of these locations are outside of a secured area?	This is a 20% design package; additional drawings will be developed in the evolution between 20 to 100% design by the DBOM
If communication or network cables (serial, Ethernet, fiber) are disconnected is this detected, and is an alarm raised?	This should generate a loss of communication alarm. Specifiation255000, 2.4.O.6.a.1 calls for loss of communications alarms.
Is there any information regarding cybersecurity services being integrated into the IT/OT network such as centralized logging (ex. syslog), authentication, time synchronization (NTP), and use of VLANs or other network separation techniques?	The OT network is separate from the IT network for the CPP. Power glitch, lightning

A.9. Other

QUESTION	JACOBS RESPONSE	ACTION REQUIRED	TEAM COMMENTS
What type of cyber security training will be required to be taken by the Operator in order for them to be able to develop cyber security policies and procedures for plant personnel and training of staff?	This will be developed by the Owner/Operator during detailed design completion and contractual requirements.	Owner/Operator Policy & Procedures Required	We developed policies plans and procedures for many clients. However, I think it will require funding. (Adi) Check network security plan details.
Will a 3rd party cyber security expert be considered to aide in development of said procedures and policies?	This will be developed by the Owner/Operator during detailed design completion and contractual requirements.	Owner/Operator Policy & Procedures Required	We developed policies plans and procedures for many clients. However, I think it will require funding. (Adi)
What physical hardening tactics will be used to prevent unauthorized access to device ports?	Exact means to physically disable a port will be determined in the design evolution from 20% to 100% final configuration. Specification 255000, 2.5.D requires unused ports and services be disabled; and this is to be tested during FAT and SAT per 3.5.C and D.		We probably need to add element of network monitoring. (Adi) Address trigger VLAN
How will a virus scan of portable media be verified?	This will be developed by the Owner/Operator during detailed design completion and contractual requirements.	Revise 255000 to add requirement for freestanding portable media kiosk to meet NERC CIP 003-7 and NIST-800-53 requirements.	
How will privacy, integrity and authenticity be guaranteed to remote login sessions to the system?	This will be developed by the Owner/Operator during detailed design completion and contractual requirements.	Owner/Operator Policy & Procedures Required	We need details to understand why and the design for remote connectivity - it could affect some cyber aspects (Adi)
Will a data diode be used anywhere in this network?	Data diodes are listed in specification 255000 and may be used as the design progresses rm		We deployed data diodes several times - but it will be design dependent. (Adi)

QUESTION	JACOBS RESPONSE	ACTION REQUIRED	TEAM COMMENTS
	20% to 100% final configuration.		
What cyber security checks will be conducted during self-diagnostics of the system?	Not sure what the expectation is in the question? Specification 255000 calls out diagnostics with respect to the actual process control system operations. The IDS is in place as noted below and plant operators monitor the system alarms.	Sandia to clarify question	If we design proper OT management and monitoring, there will be 100& monitoring, check and vulnerability analysis 100% of the time. (ADI)
For systems that use external media for updates or to control settings, other than physical access, are there any protections to prevent the removal or modification of this media?	The design does not allow external media to control the system; updates are to be vetted and controlled such as noted above for patch management.		There are a variety of options to accomplish this; need to understand intent. (Adi)
Will any of the systems, HMIs, or remote workstations use secure boot techniques, or require digitally signed firmware or software updates?	Not sure what the expectation is in the question?	Sandia to clarify question	This is vague. Needs to be clarified (Adi) Don't currently reference "secure boot" techniques. Avoid installation of bugs without digital sig.
What is the process to ensure configuration values are correct, and are not modified in a manner that could impact operations or damage the system? (Ex. Would the system prevent a cooldown period of a generator to be set to 60,000 minutes?)	The Intrusion Detection System shall use both signature list and anomaly means to detect unauthorized traffic. The control system also has built in alarms and setpoint limitations that are monitored by the plant operators 24/7.		Call out hart communicator lockup

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Benjamin Anderson	05681	brander@sandia.gov
William Atkins	09373	wdatkin@sandia.gov
Robert Broderick	08812	rbroder@sandia.gov
Jay Johnson	08812	jjohns2@sandia.gov
Mike Lopez	05681	mrlope@sandia.gov
Timothy Ortiz	08851	tortiz@sandia.gov
Steve Scott	03648	stescot@sandia.gov
Russell Shiplet	05681	rshiple@sandia.gov
Technical Library	01977	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Nicholas L. Marton	NMarton@njtransit.com	New Jersey Transit
Roderick Schwass	Roderick.Schwass@jacobs.com	Jacobs Engineering

Sandia National Laboratories