INL/RPT-22-67649

Cyber-Risk Management Feasibility Study

June 2022

Retrofitting Existing Solar with Emerging Technologies (RESET)

Megan J. Culler
Justin J. Welch
Jakob P. Meng
Dylan W. Reen
Kurt S. Myers

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance, LLC

INL/RPT-22-

Cyber-Risk Management Feasibility Study

Retrofitting Existing Solar with Emerging Technologies (RESET)

Megan J. Culler
Justin J. Welch
Jakob P. Meng
Dylan W. Reen
Kurt S. Myers

Idaho National Laboratory

June 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
Strategic Environmental Research and Development Program (ESTCP)
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

EXECUTIVE SUMMARY

The United States (U.S.) Department of Defense (DoD) maintains a globally networked force responsible for missions around the world—many of which rely on U.S. military installations. These military installations are often almost entirely reliant on the commercial electricity grid [1]. Cyber-attacks, aging infrastructure, increasing numbers of points for potential failures and system limitations, and extreme weather events exacerbated by climate change are causing more frequent and severe power interruptions, which threaten the success of critical military missions [2].

DoD has acquired—or purchases energy from—a large fleet of power plants located on, or nearby, its military installations during the past decade. These power-producing facilities include more than 2,000 renewable energy projects that generated 3,700 gigawatt hours (GWh) in 2020 in response to Congressional legislation and Executive Orders. DoD has installed more than 1,200 solar photovoltaic (PV) systems across the U.S., ranging in size from a few kilowatts (kW) to over 100 megawatts (MW). There are notable examples of solar PV systems that have been configured to provide resilience as part of microgrids. These include, for example, a 124 kW PV solar system at Kirtland Air Force Base, a 4.5 MW PV system at Naval Construction Battalion Center Gulfport in Mississippi, and a 30 MW PV system at Pacific Missile Range Facility Barking Sands in Hawaii [3, 4, 5]. However, DoD continues to rely overwhelmingly on backup diesel generators and limited uninterruptible power supply (UPS) systems to provide energy resilience and "much of the existing deployed solar PV on DoD installations is installed without islanding support or grid-forming capabilities, preventing use as a true resilience solution" [6]. DoD's fleet of existing renewable energy plants represents a significant, but largely untapped, energy resilience resource. DoD—and the federal government more broadly—lacks a process for assessing whether and how energy resilience capability can be added to existing renewable energy projects. This report specifically investigates the cyber-considerations related to energy resilience retrofits and summarizes the key questions that project proponents could ask when evaluating solar PV sites for resilience retrofit feasibility, preliminary design, and subsequent development processes.

Page intentionally left blank

CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

@DISCO	Annotated and Translated Disassembled Code
ACAS	Assured Compliance Assessment Solution
AI	artificial intelligence
AO	Authorizing Official
AO-DR	Authorizing Official Designated Representative
APT	advanced persistent threat
ATO	authorization to operate
AWS	Amazon Web Services
C3D	Constrained Communication Device
CAC	common access card
CCP	Common Control Provider
CIA	confidential integrity availability
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISA	Cybersecurity & Infrastructure Security Agency
CP	Contingency Plan
CVSS	Common Vulnerability Scoring System
CyPHAAR	Cyber-Physical Architecture for Automated Responses
DER	Distributed Energy Resources
DFD	data flow diagram
DHS	U.S. Department of Homeland Security
DNS	Domain Name Server
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
EAFB	Edwards Air Force Base
EMV	Exploit, Malware, and Vulnerability
ESTCP	Strategic Environmental Research and Development Program
GiG	Global Information Grid
GOTS	Government-off-the-shelf
HBSS	Host-Based Security System
HIDS	Host-based Intrusion Detection System
HTTP	Hypertext Transfer Protocol
ICS	industrial control system

IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
IO	Information Owner
IP	internet protocol
IPSec	internet protocol secure
IRP	Incident Response Plan
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	information technology
LCM	lifecycle management
MAC	media access control
MASTERRI	Modeling and Simulation for Target Electrical Resilience Improvement
MFA	multi-factor authentication
MSE	Master State Awareness Estimator
NERC	North American Electric Reliability Corporation
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
OT	operational technology
OUO	Official Use Only
PARROT	Plug-N-Play Appliance for Resilient Response of Operational Technologies
PLC	programable logic controller
PM	Program Manager
PMI	Project Management Institute
PSP	Personnel Security Program
PSSM	Ports, Protocols, and Service Management
PV	photovoltaic
RADIUS	Remote Authentication Dial-In User Service
RAR	risk assessment report
RBAC	Rule-Based Access Control
RESET	Retrofitting Existing Solar with Emerging Technologies
RMF	Risk Management Framework
SBOM	software bill-of-materials
SCA	Security Control Assessor

SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCE	Southern California Edison
SEL	Schweitzer Engineering Laboratories
SEMS	SPYRUS Enterprise Management System
SIEM	Security Information and Event Management
SIP	Security Implementation Platform
SISO	Senior Information Security Officer
SME	subject matter expert
SOAR	Security Orchestration Automation and Response
SPEMMCRA	Scalable, Physical Effects Measurable Microgrid for Cyber-Resilience Analysis
SSH	secure shell
SSP	System Security Plan
STAR	Structure Threat Automated Response
STEM	Smart Energy Storage and Energy Management
STIG	Structure Threat Intelligence Graph
STIX	Structured Threat Information eXpression
STOTS	Structure Threat Observable Tool Set
TCP	Transmission Control Protocol
U.S.	United States
UDP	User Datagram Protocol
UPS	uninterruptible power supply
UR	User Representative
VLAN	virtual local area network
VPN	virtual private network
WAPA	Western Area Power Administration
WiiBin	What is Binary

Page intentionally left blank

Cyber-Risk Management Feasibility Study

1 INTRODUCTION

1.1 Purpose

The Retrofitting Existing Solar with Emerging Technologies (RESET) project explores how the United States (U.S.) Department of Defense (DoD) can utilize its existing renewable energy assets to support its ambitious energy resilience goals. This project is funded by the Environmental Security Technology Certification Program (ESTCP) and consisted of a multi-disciplinary team where Converge Strategies acted as the principal investigator. This report specifically investigates the cyber-considerations related to energy resilience retrofits and summarizes the key questions that project proponents could ask when evaluating solar photovoltaic (PV) sites for resilience retrofit feasibility, preliminary design, and subsequent development processes. The questions and concepts in this report are intended to support initial site-screening and planning by energy personnel at installations, as well as by staff within the DoD energy program offices, engineering centers, and acquisition agencies. Similar questions could also be useful to private sector project developers or other energy project proponents.

1.2 Scope

This report focuses primarily on the following key areas:

- **Cyber-risk management**: The cyber-risk management considerations and assessment topics covered in this report are based on the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and are intended to provide a higher-level overview of key cyber-risk management practices that can be more easily and quickly implemented than a full RMF evaluation. The report covers key considerations such as network and equipment age, connected devices, network connections and protocols, and key personnel roles and knowledge.
- **Cyber-risk management assessment for solar retrofits**: An easy-to-follow assessment methodology for RESET is provided, which enables project proponents to systematically evaluate project and system risks in several key areas and loosely quantify the as-is risk to a particular system, and then the new risk if certain resilience improvements are made. Worksheets are provided in the appendixes to assist in the assessment process.
- **Lessons learned**: The inclusion of lessons learned early in the planning phase of projects is arguably the easiest and most cost-effective way to enhance the resilience and security of new or upgraded systems. A table of lessons learned is provided that includes inputs from cybersecurity subject matter experts (SMEs) and feedback from actual DoD energy-based projects and assessments.
- **Current and emerging cyber-risk management solutions**: Retrofitting a system allows an opportunity to add additional solutions to your system that could potentially decrease your risk. This report provides a non-exhaustive list of both currently available and new/emerging solutions that can be considered for RESET and system design architecture/developments for energy resilience projects.

A feasibility study for Edwards Air Force Base (EAFB) provides an example for how to apply the cyber-risk management considerations and assessment tool to a proposed resilience retrofit. The study demonstrates that although the cyber-risks to the system change when the retrofit is applied, following good risk management practices can reduce the risk to an acceptable level.

The appendixes provide additional information that can be used as a reference for conducting cyber-self-evaluations:

- Appendix A contains the worksheets for the cyber-risk management assessment.
- Appendix B contains a non-exhaustive list of NIST RMF questions most relevant to the cyber-assessment of an operational technology (OT) system.
- Appendix C contains a high-level view of resilience for cyber-systems that pushes users to think outside of checklist items for achieving cybersecurity and focus on cyber-resilience specific to each system and the hazards it may face.

2 CYBER-RISK MANAGEMENT BACKGROUND

Cyber-risk management focuses on protecting a computer system and networks from a loss of confidentiality, integrity, and availability, which is commonly called the confidential integrity availability (CIA) triad and is shown in Figure 1.

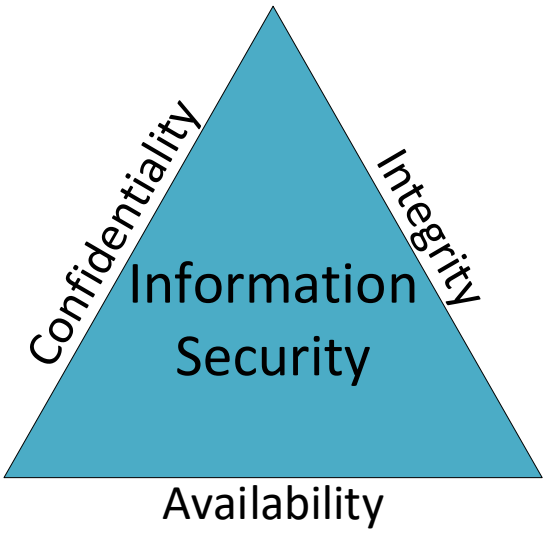


Figure 1. CIA triad.

NIST defines these as:

- Confidentiality: Preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.
- Integrity: Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
- Availability: Ensuring timely and reliable access to and use of information.

These definitions are important as they provide the context for what is being protected on a system and provides a common way to discuss cyber-risk management. Each system is unique and will need to be evaluated to understand the impacts that a loss of any aspect of the CIA triad would cause. For many OT systems, including energy systems, availability is often the highest priority. Security controls are designed to maintain the availability of the system, the ability to produce and deliver power, even while experiencing a disturbance. However, the other components cannot be neglected, and designers and operators should consider the specific security requirements of their system.

The NIST RMF provides details of how to systematically approach risk management for your organization [7]. However, this process is robust and time-consuming to complete. This document is intended to provide high-level considerations for cyber-risk management. It will not be an all-exhaustive look, but aims to provide enough details to understand your general risk posture as you consider retrofitting your existing solar with emerging technologies.

An important note is that it is common vernacular to use cybersecurity and cyber-risk management interchangeability. The authors of this report chose to use cyber-risk management to maintain a broader focus that includes things such as contingency planning and program management that sometimes do not get considered when using the term ‘cybersecurity’ exclusively. Additionally, cybersecurity can connotate active cyber-adversaries attacking the system, but cyber-risk management allows us to consider cyber-hazards, physical hazards, and failures that may affect the communications and control of a power system.

2.1 Cyber-Risk Management Considerations for Resilience Retrofits

Ensuring the cybersecurity of the resilience projects and the new systems is critical to ensure that the added resilience can be realized, particularly during natural or manmade hazard events.

Threats can pose challenges to resilience in several ways. We present a few examples here to motivate the key best practices that should be put in place:

- Disruptions during a hazard event where backup power is required could prevent the inverters from performing their grid-forming capabilities. This could happen even with an untargeted attack, like the denial-of-service attack against SPower in March 2019, which caused network routers to restart repeatedly over a 12-hour period, blocking operator visibility and control of renewable assets [8].
- Adversarial changes to smart inverter settings could make grid support functions unavailable, or even cause the inverters to reduce stability of the grid rather than support stability (e.g., inverted Volt-Var curves or frequency support curves). This would require a compromise of the device itself and the local or wireless control methods.
- Ransomware attacks could lock up resources directly or block visibility into and control of the system, preventing the active management of smart inverter functions. Often, ransomware is deployed against the most accessible systems, like the externally facing business network. However, ransomware can spread if there is poor network segmentation or management. Ransomware is increasingly being deployed against OT systems [9]. Adversaries recognize that the high requirement for availability of these systems may motivate asset owners to pay the ransom immediately rather than allow the system to experience more downtime as they try to remove the ransomware themselves.
- Mismanaged or adversarial managed storage levels could lead to battery power being unavailable when needed to provide backup power. Compromise of an onsite operator, third-party integrator, or electric utility could give access to an adversary to execute this attack.

The next sections take a deeper dive on the cybersecurity considerations identified in the considerations document produced for the RESET project [10].

2.1.1 Network Equipment

2.1.1.1 Equipment Age

Legacy OT systems were often not designed with cybersecurity in mind. Depending on the equipment being used, there may be updates or tools that can increase the cybersecurity posture to an acceptable level. On the reverse side, cybersecurity tools can break legacy equipment. For example, it has been documented that an active network scan from a common tool called Nessus has causes certain programable logic controllers (PLCs) to stop responding.

The other consideration is of course cost. Replacing a portion of legacy equipment might be more cost-effective in the long run.

Some questions to consider if you should replace existing equipment with new:

- Is my equipment so old that everyone is afraid to touch it as it might break?
- If equipment fails, can a replacement be bought?
- Do I have the expertise available to fix the device? New equipment usually comes with a warranty and support.
- Is the equipment compatible with other new equipment that would be added as part of the retrofit?

2.1.1.2 Ports and Connection Types

Network segmentation is the process of dividing a local network into multiple subnets. The topic is discussed more in Section 2.1.3.2, "Network Segmentation," but often it is advantageous to have one device in multiple segments. An example of this is to have a subnet that is dedicated to device management and configuration. If a device only has one physical communication port (e.g., a physical jack or a socket in which to plug the communication cable), it would be impossible for this to occur. There is a risk associated with allowing a device into multiple subnets as it allows an adversary a place to 'jump' subnets. However, proper configuration can significantly reduce this risk.

The Ports, Protocols, and Service Management (PPSM) is a required document for the RMF process that details what devices talk to each other and what protocol and ports they use. 'Port' in this case refers to a defined number associated with a network protocol that transmits and/or receives communication. For example, port 80 is used by Hypertext Transfer Protocol (HTTP) for the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocol.

Some questions to consider if you should replace the equipment with new:

- Does the device have multiple ports available?
- Does the device have a built-in management port that has cyber-controls already in place to prevent the jump risk?
- Do I have enough information to create a PPSM?

2.1.1.3 Proprietary Equipment and Operating Software

Project developers attempting to add cybersecurity to these systems will likely encounter proprietary equipment connections and operating software that may require individual vendors to connect to the systems as they are the only ones with the tool and knowledge to update the equipment. If a critical patch is needed, it could be costly to get the vendor to come quickly to patch it.

Another challenge with less commonplace equipment is that expertise and understanding in the configuration and management for that device may be lacking. Equipment vendors, such as CISCO, have their own certification programs ensuring that staff are properly trained.

In addition to the challenges above, proprietary protocols may make it unable to be integrated with other systems, including monitoring.

Some questions to consider for existing equipment or new equipment in consideration for purchase:

- Is there a robust training program in place for the equipment to train new users?
- Can you perform patches yourself or are you dependent on the vendor?
- Are there any examples of this equipment being used elsewhere that can be looked at through lessons learned to ensure there are no proprietary issues?

2.1.2 Connected Devices

Resilience retrofits will almost necessarily require new hardware to be installed. Whether this is information technology (IT) equipment to support new control protocols, sensors, and monitoring equipment to gather the data needed for efficient operation, or power system components including relays, batteries, or new inverters. For each of these devices, it is important to note what connection options are available for the device, who wants to connect to the device, and what capabilities or access the connection will allow.

2.1.2.1 Local Connectivity

Local connectivity is generally considered more secure than remote connectivity because that connection can only be accessed by the devices that are physically wired together. However, wired solutions do not guarantee the security of the connected devices. If the device on either end is compromised, it could send malformed or malicious payloads to a target device. Trust should not be assumed for directly connected devices, and methods of authorization and authentication should still be enforced:

- Asset managers should ensure that a bill-of-materials is maintained and updated for the system. This should include all devices with local connectivity.
- Local connections should use the highest security features available. One example is enabling multi-factor authentication (MFA).
- When multiple protocols are available for local communication, protocols with better security features—including encryption and authentication—should be used.
- Access control for local connectivity should be actively tracked and maintained. Users with the need for local connectivity should have unique credentials. Furthermore, those credentials should be revoked if a user's role changes or if they no longer need to use local connectivity.

2.1.2.2 Wireless Connectivity

Wireless connectivity is commonplace for renewable and distributed resources. This makes it easier to coordinate resources across a larger geographical area, which could be used, for example, to take advantage of maximum resource availability for wind and solar across a DoD base and wind and solar complementarity for enhanced resilience. However, as more devices are added to a local network, the impact of a potential cyber-attack may increase. Additionally, if there are wireless connections used to enable remote control, it is possible for those signals to be sniffed or even spoofed:

- Messages sent over wireless communications should be encrypted and authenticated.
- Whitelisting should be used for field devices. Only controllers that need direct access to field devices should be whitelisted.
- A data flow diagram (DFD) should be developed to track the flow of information and ensure that sensitive information is properly protected.
- When possible, a dedicated remote communications channel should be used. This can include sending all data through a virtual private network (VPN) or using dedicated cellular channels.

2.1.2.3 Lifecycle Management (LCM) Plan

LCM is an integrated system of people, tools, and processes that supervise a technology from its initial planning through retirement. Connected devices for resilience upgrades should have an LCM plan for both the physical device and any applications that run on the device. Part of the responsibility for an LCM falls on the vendor. The longer the vendor waits to implement an LCM, the more cost-prohibitive and resource-intensive upgrades, maintenance, and fixes become. It also inhibits the vendor's ability to respond to and address critical vulnerabilities, drastically increasing the time necessary for releasing security updates to customers. The LCM should include a plan for keeping software components updated, which by nature will require that a software bill-of-materials is maintained. Components that contain custom protocols or implementations may be difficult or impossible to patch. If the vendor does not have an LCM, the customer bears the cost of increased cybersecurity risk and expenses related to increased security, compliance, and audit requirements necessary to secure the vulnerable code.

DoD bases seeking to enhance power system resilience by retrofitting solar installations with upgrades should ensure that any new connected requirements for a system upgrade include an LCM. This can be negotiated with the vendor if necessary:

- DoD should require that a software bill-of-materials (SBOM) is included with the purchase of any new field devices that run applications. The SBOM should include a list of components and associated metadata.
- Vendors of new devices should provide a patch management plan, a vulnerability management/mitigation program, and an update process for the software, hardware, and firmware provided by the vendor.
- Patches provided by the vendor should include a published checksum to allow the customer to independently verify the integrity of the software and patches.
- The vendor should provide or arrange the provision of updates as necessary to remediate newly discovered vulnerabilities or weaknesses within 30 days. Updates to remediate critical vulnerabilities should be provided within a shorter period. If updates cannot be made available by the vendor in these time frames, the vendor should provide mitigations, methods of exploit detection, and/or workarounds within a reasonable time frame.
- Vendors should use reasonable effort to investigate whether computer viruses or malware are present in any software patches before providing them to customers. To the extent the vendor is supplying third-party software patches, the vendor will use reasonable effort to ensure that the third-party investigates whether computer viruses or malware are present before providing them to the customer.

2.1.2.4 Supply Chain Security

Supply chain security, while closely related to the LCM, deals more with the source and acquisition process for new devices and applications rather than the continued maintenance and security of the devices and applications. According to NIST, supply chain security risks include counterfeit hardware or embedded software, third-party data storage and acquisition, poor security practices by lower-tier suppliers, compromised or vulnerable software or hardware systems, and third-party service vendors and suppliers [11]. It can be difficult to assess a vendor's security practices, but it is worth discussing a vendor's design and manufacturing process to assess the documentation, management, monitoring, and production of a device from its conception to installation. The following questions, provided by NIST, can help guide an investigation into supply chain security of connected devices to ensure that the risk associated with the devices is acceptable:

- How is configuration management and quality assurance performed?
- What levels of malware protection and detection are performed?
- What steps are taken to 'tamper proof' products?
- Are all production and development back doors closed?
- What access controls are in place?
- How are the access controls documented and audited?
- What security practice expectations are set for upstream suppliers?
- How is adherence to security practice standards assessed?
- Have approved and authorized distribution channels been clearly documented?

2.1.3 Network Connections

The location of the system can mitigate some risks while creating others. A system not managed by DoD can cost less and may not need the full RMF process completed and maintained. However, putting a networked system in the control of a third-party limits the control that the DoD has over the system, and requires the trust of the third-party to maintain acceptable service levels for the desired resilience benefits.

Closed and isolated systems can prevent remote connections, but are also more difficult to apply patches and updates on.

2.1.3.1 Encryption and Authentication

Encryption standards exist for a reason. Networked devices should be using standard, up-to-date encryption standards and well-established implementations. Custom encryption implementation is prone to errors and security flaws, and security through obscurity, or security through 'novel' encryption or authentication, is never a recommended method.

Many OT protocols do not have encryption or an authentication feature. In these cases, if no alternatives are available, extra risk mitigation measures can be added to the network architecture, which could include using a VPN to add encryption, adding a firewall to allow only expected protocols through, and implementing internet protocol (IP) whitelisting to prevent any unknown or unauthorized devices from sending commands:

- Authentication can help ensure commands and data are not spoofed. Use authentication to communicate between networked devices where possible.
- Although confidentiality is generally considered less important in OT environments than in IT environments, it is still a best practice to use encryption where possible. Encryption does not usually add too large a computational burden, even on edge devices.
- When secure network communications are not available, consider adding additional risk mitigation measures like firewalls, IP whitelisting, and VPNs. These measures do not replace cryptographic authentication or encryption, and are often good practices to build into a communications architecture anyway.

2.1.3.2 Network Segmentation

Network segmentation is the process of dividing a local network into multiple subnets. It makes harder for devices to talk directly from one to another without going through a router, which can be outfitted with a firewall to ensure only valid traffic passes from one subnet to another:

- Apply the principle of least privilege when architecting subnets. Only devices that need to talk to each other should be permitted to do so.
- Limit third-party access. While third-party access may be required to manage certain devices, it is unlikely that third-parties need direct access to all devices in the system. Segment devices by vendor interactions where possible.
- Don't over-segment. Creating too many zones adds unnecessary complexity and makes the system more difficult to manage.

2.1.3.3 Cloud Connections

Vendors providing cloud-hosted solutions are becoming more and more common. Cloud solutions are well suited to renewable energy generation given the often geographically distributed nature of the resources. Cloud solutions are also cheaper than local installations of an energy management solution, and they can better support continuous upgrades and updates as opposed to relying on someone on site to perform this aspect of lifecycle management. However, cloud-based solutions are often shunned by risk-adverse organizations due to the perception that data and control capabilities may be more easily accessed

by remote adversaries. While there is some additional risk involved, well-managed solutions can provide additional benefits and efficiencies that would not otherwise be possible. Steps to ensure that risk from cloud connections is minimized include:

- Ensuring the cloud database is managed by a well-known and secure provider, such as Amazon Web Services (AWS).
- Requiring that the cloud connection use authentication and encryption.
- Not storing all data or control settings in the cloud. If the cloud connection or storage is compromised, local backups can be relied on to restore a minimum level or service faster.
- Developing a data privacy plan with the service provider.
- Ensuring proper network segmentation is implemented, allowing the cloud service to directly access only the data it needs to.

2.1.3.4 Network Monitoring

Monitoring and auditing a network is an effective way to ensure the network architecture is secure. Monitoring can aid in the rapid identification of traffic or security issues by:

- Ensuring sufficient network monitoring is deployed. At the very least, inbound and outgoing connections should be monitored.
- Monitoring logs should be stored securely, preferably outside of the system network. This will help ensure that if an adversary gains access, they cannot also manipulate the logs to hide their presence and activities.
- Backing up logs regularly.
- Providing intrusion detection systems (IDSs) that are customizable to industrial control networks. IDSs are not always necessary, but provide a valuable addition to monitor critical systems and quickly detect unusual activity.

2.1.4 Personnel Roles and Knowledge

2.1.4.1 DoD

The responsibility of cyber-risk management belongs to every single employee. However, there are some key roles that are defined by the RMF process. Is imperative that each of these roles has an active participant (in house or third-party) assigned to maintain an appropriate security posture. Table 1 provides a list of these roles and responsibilities.

Table 1. RMF roles and responsibilities.

Acronym	Role	Description
CIO	Chief Information Officer	Directs and oversees the cybersecurity risk. This is a high-level position and defines organizational policy, but the CIO doesn't get involved in the individual systems.
SISO	Senior Information Security Officer	Acts as the CIO's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

Acronym	Role	Description
AO	Authorizing Official	The AO is the senior official or executive with the authority to formally assume responsibility for operating a system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and national security.
AO-DR	Authorizing Official Designated Representative	Can act on behalf of AO.
SCA	Security Control Assessor	Independent validator.
CCP	Common Control Provider	A CCP is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls. For example, the U.S. Army may have rules and solutions that need to be used on their systems.
IO	Information Owner/ Steward	An IO is an organizational official with statutory, management, or operational authority for specific information. The IO position is occupied by a government employee with capital investment authority.
ISO/PM	Information System Owner/ Program Manager	The ISO (or cleared contractor PM) is primarily responsible for managing system development, operations, and maintenance at the program level.
ISSM	Information System Security Manager	The ISSM is primarily responsible for maintaining the overall security posture of the systems within their organization and are accountable for the implementation of the RMF.
ISSO	Information System Security Officer	An ISSO is an individual responsible for ensuring the appropriate operational security posture is maintained for a system.
UR	User Representative	A person representing actual users.

2.1.4.2 Third-party Integrator

In many cases, a third-party is contracted to perform upgrades and installs. Similarly, vendors of certain equipment may be involved in the process. An example of this would be Tesla providing support for their battery solutions. This is useful as DoD staff expertise and/or availability might not be high enough to tackle in house. However, this opens unique cyber-risk management concerns:

- The third-party integrator must provide clear and complete documentation:
    - This includes a password list where applicable. These passwords should be changed before the system goes live. However, if the contract changes during the installation process, the DoD user does not want to get locked out of their own system.
- If equipment is not Government-off-the-shelf (GOTS), the third-party must ensure that the company provides a reasonable level of maintenance and patching. Depending on install location, equipment may have to go through the DoD approval process before use.

- Third-parties and vendors sometimes try and leave the ability for them to gather information and make changes to the system. These access points should be allowed only if absolutely necessary (as determined by DoD, not the vendor) and they should be segmented off.

2.1.4.3 Electric Utility

An electric utility is a company in the electric power industry (often a public utility) that engages in electricity generation and distribution of electricity for sale generally in a regulated market. Depending on the use case, the electric utility may need access to data from the microgrid. This data should be protected as determined by the categorization of the system.

2.2 Cyber-Risk Management Assessment for Solar Retrofits

2.2.1 Risk Assessments Introduction

Risk assessments are important as they are used to identify, estimate, and prioritize risk for an organization's operations. NIST SP 800-30 provides guidance for conducting risk assessments. Many risk assessment models exist, but a commonly accepted one is shown in Figure 2.

		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Figure 2. Risk matrix classifies overall risk using likelihood and consequence.

This model defines risk as a function of the likelihood of the event occurring and the consequence to the system if that event were to happen.

Risk = Likelihood x Consequence

Consequences of certain events can usually be identified, but the likelihood of them occurring is often difficult to determine. One way to break down likelihood is to consider the threat itself, as well as the capabilities and security of the system.

Risk = Threat x Vulnerability x Consequence

Threats to information systems can include both adversarial physical- and cyber-attacks, as well as environmental disruptions, such as natural disasters and human errors. However, threat is still a nebulous concept to identify especially for adversarial attacks. Particularly for smaller power systems, asset owners

may take the perspective of ‘why would anyone want to attack my system in particular’ or ‘my system has a unique combination of technologies and controls; it would be difficult for anyone to customize an attack towards my system.’ By breaking down the concept of threat even further, it is easier to see how a credible threat is formed.

Risk = Adversary x Opportunity x Vulnerability x Consequence

Note that opportunity and vulnerability represent different concepts, although they can easily be conflated. Vulnerabilities are a weakness in the system, which can be exploited by a threat that causes a loss of CIA. It may be a flaw in the design or implementation of a component.

Opportunity is the access that a threat has to a target. For example, a system directly accessible from the internet provides far greater opportunity for an adversary than one protected by firewalls and VPNs, even if both systems are designed identically. A system built near a fault line has more opportunity for an earthquake to affect a system.

Additionally, opportunity is tied to the threat, while vulnerability is tied to the system. A disgruntled employee will have a greater opportunity to execute an attack than a financially motivated attacker from across the world, even though the systems they attack may have the same vulnerabilities.

Finally, there are a variety of different kinds of adversaries, which can be useful to classify.

Adversary = Intent x Capability

Adversaries may be intentional or unintentional with their actions. An employee who clicks on a phishing email that opens a backdoor for a hacker increases the overall risk, even though their actions were not malicious. Intentional adversaries may be motivated by financial gain, general disruption, or sociopolitical impacts. The other component to classify an adversary is their capability. This refers to the skills and funding they have available to execute an attack.

This extra granularity also helps when looking at environmental threats. Obviously, a natural disaster has no intent, but one can infer the capability of destruction it could have.

Risk = Adversary [Intent x Capability] x Opportunity x Vulnerability x Consequence

The components of the cybersecurity risk model (e.g., Adversary, Opportunity, Vulnerability, and Consequence) are difficult to quantitatively evaluate, but different system architectures can be qualitatively compared with this framework.

It can be helpful not just to evaluate the risk overall, but to see where the biggest parts of the risk lie so that mitigation measures can be prioritized.

In Figure 3, overall risk can be assessed as the shaded area shown inside the figure. Reducing any one of the risk components will reduce the overall risk. The ‘Adversary’ component cannot be directly controlled by the asset owner. However, measures taken for the other risk components can have an indirect effect on the adversary. Reducing the attack surface and vulnerability means that the adversary must have higher capabilities to successfully execute an attack. Reducing the potential consequences of an attack can make the system a less valuable target for an adversary with malicious intent (e.g., financial, political, destructive, or other). See Section 2.3.1.5, “Risk Evaluation,” for an example.

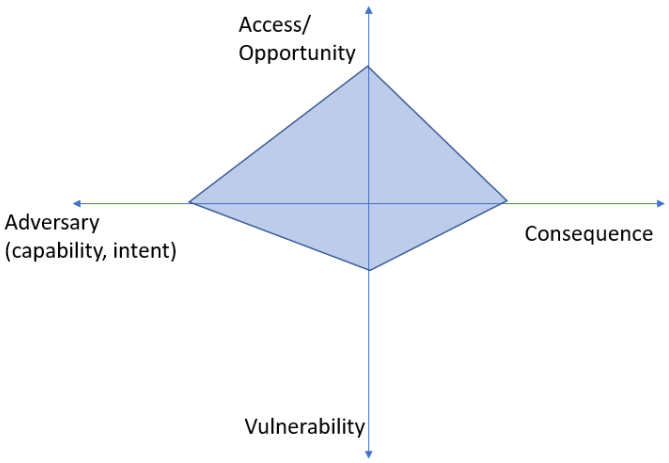


Figure 3. Example risk assessment diagram.

Each component of cybersecurity risk can be mitigated through resilience. It is nearly impossible to guarantee that there are no vulnerabilities, access points, and potential consequences of an adversarial attack. However, resilience in the context of power systems, "the ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to and/or rapidly recover from such an event [12]," is a quality that can reduce the overall risk. Idaho National Laboratory (INL) has developed a resilience framework for electric energy delivery systems, which breaks down resilience into five core functions: (1) identify; (2) prepare; (3) detect; (4) adapt; and (5) recover [13]. These core functions loosely align with the NIST cybersecurity framework, but are adapted to the considerations for a cyber-physical critical infrastructure system like energy delivery systems for a focus on overall resilience [14]. Appendix C contains specific examples of how to use each of the resilience core functions to mitigate each component of cyber-risk. Many of the resilience measures suggested aligning with risk assessment and RMF questions, but the visualization of how each mitigation is mapped to a specific resilience function can be useful for ensuring a comprehensive resilience plan is formed. Building these resilience functions into risk mitigation measures can help ensure that each stage in a potential disruption is mitigated to the extent possible.

2.2.2 High-Level RESET Risk Assessment Process

The following is a high-level risk assessment that can be performed for a system. The intent is to perform the assessment at least twice. The first is the system 'as-is' to get your baseline posture. The second is a repeat with the proposed upgrades. If the risk is not deemed acceptable, mitigation solutions can be considered, and step 3 can be performed. Even if the risk goes down during step 2, it still might be worthwhile to consider mitigations that bring it down even more.

Appendix A has three copies of the risk assessment. They are identical besides the title and contain the following three steps:

- Step 1: System as Operated
- Step 2: System with Proposed Upgrades
- Step 3: Mitigations Applied.

Each worksheet can be used to evaluate an iteration of the system as it progresses through the resilience retrofit. This iterative process allows for comparison of the system before and after the retrofit without using strict quantitative metrics for the assessment. The purpose of using these worksheets is not to certify a system against a certain cybersecurity, but rather to give bases considering resilience retrofits a way to evaluate the change in cyber-risk for their particular system.

There will be inherent biases in the selection of ratings, so it is recommended that the same person or same team conduct each iteration of the assessment so that these biases do not contribute to the change in the assessed cyber-risk.

Appendix B is designed to be a worksheet to aid in deciding which ranking best applies. Appendix B highlights elements of the risk management framework that are most relevant to the cyber-risk assessment for resilience retrofits. It does not represent every single consideration that may be important to an organization, but it provides concrete and specific questions that can help aid in the selection of a rating.

Section 2.1 is also a good reference for considerations to help evaluate each of these areas. Beyond evaluating the current position of the system, the best practices described in Section 2.1 are a good place to start to apply mitigations if the current risk level is higher than the organization wants to accept.

2.2.2.1 Evaluation Criteria

Pick the descriptor that best fits your posture in each risk category.

2.2.2.1.1 Adversary [Intent & Capability]

This category is one that organizations have the least control over. Please mark the highest ranking that it is likely the organization will be targeted by. Consider why an adversary would target this system (intent) and the capability of someone with this intent. For a naturally occurring cyber-'adversary,' consider how natural events, such as hurricanes or fires, could affect a system. While there is no intent associated with natural cyber-threats, the capability (i.e., strength) can be evaluated using Table 2.

Table 2. Adversary chart.

Hacker	Benign Insider	Organized Group	Malicious Insider	Hostile Nation-State or Terrorist
1	2	3	4	5

Hacker: A single entity or small group of individuals motivated by curiosity, notoriety, fame, or attention. They may or may not target specific organizations. The skill set of this group may not be advanced, but through the use of automated attack scripts and protocols that can be downloaded or purchased, they can orchestrate more sophisticated attacks.

Benign Insider: Benign insiders may not have intent to disrupt a system, but their familiarity with systems and granted access still pose a potential threat. This group may include third-parties or employees who may accidentally grant others access to the system (via phishing attacks or other mechanisms) or introduce malware via unintentional downloads.

Organized Group: This type of adversary is typically more organized and funded than hackers or insiders, creating the potential for higher capabilities. They often have a specific target, and can tailor their capabilities towards the target. Examples can include a corporate organization engaged in espionage, organized crime aimed at financial extortion (e.g., ransomware, financial theft, or blackmail), or hacktivists concerned with supporting political agendas.

Malicious Insider: Malicious insiders differ in their intent from benign insiders. They will leverage their access and knowledge of the system to target specific systems and specific outcomes. This could include individuals who are bribed or blackmailed by outside organizations, disgruntled employees, or others with outside agendas.

Hostile Nation-State or Terrorist: This type of adversary is often structured, sophisticated, and well-funded. Their capabilities allow them to launch advanced persistent threat (APT) campaigns, where an adversary gains unauthorized access and remains undetected for an extended period of time, pivoting into deeper and more sensitive networks before launching a targeted attack.

2.2.2.1.2 Access/Opportunity

Access or opportunity considers the setup of the system and its accessibility to the outside world. Consider the ability to access the system externally, as well as the difficulty to access the targeted subsystem if the internal network was compromised. For natural cyber-threats, consider the exposure of the hardware to naturally occurring hazards.

Table 3. Access/opportunity chart.

Air-Gapped/ Vetted Access	Controlled Access	Internal Access	Public, Limited Access	Public, Searchable Access
1	2	3	4	5

Air-Gapped/Vetted Access: Systems are air-gapped from external connections. All individuals with access to the systems are thoroughly vetted and trusted. No remote access is available.

Controlled Access: Firewalls, VPNs, session timeouts, and other controls are used to limit external and internal network access. If remote access is enabled, proper authentication and encryption is used. Role-based access control is implemented.

Internal Access: Controls are used to limit external access. From the internal network, the system is accessible by all users with no or weak credentials. Remote access is available and may or may not use protected protocols.

Public, Limited Access: The system can be accessed from any internet connection point if you know the correct IP address. All users on internal networks can access the system. External access requires proper credentials.

Public, Searchable Access: The system can be accessed from any internet connection point. The system is searchable using online tools. There are weak or no protections on the public interface.

2.2.2.1.3 Vulnerability

The selected vulnerability ranking should be at least the ranking of the highest individual known vulnerability. Multiple known vulnerabilities at one level may merit a higher overall system vulnerability ranking. Consider that vulnerabilities may be located in any layer of the system: hardware, firmware, software, network, and process. Consider also that vulnerabilities may be a flaw in either design or implementation of an individual component or the larger connected system. Known and reported vulnerabilities are assigned a score in the Common Vulnerability Scoring System (CVSS). These can be a useful reference for known software vulnerabilities, but keep in mind that not all vulnerabilities have been scored with this system, and some vulnerabilities may be related to software use or architecture implementation rather than code problems with software.

Table 4. Vulnerability chart.

Informational	Low	Medium	High	Critical
1	2	3	4	5

Informational: Informational (or potential) vulnerabilities refer to information that may be leveraged by an adversary that does not constitute a real risk on its own. This may include installed software, open ports, and general information about what a system is and how it operates. It may also specific bits of information that the end-user can see that was not designed to be released. Consider too how easy it would be for an adversary to discover this information.
CVSS Score: 0.0

Low: Low severity vulnerabilities usually result in information disclosure about users or application architecture that does not result in the compromise of sensitive information of the system. Vulnerabilities that require high privileges to exploit may also be classified as low.
CVSS Score: 0.0-3.9

Medium: Vulnerabilities may include denial-of-service vulnerabilities that are difficult to set up, exploits that require an attacker to reside on the same local network as the victim, exploitation that results in limited access, or vulnerabilities that require user privileges for successful exploitation.
CVSS Score: 4.0-6.9

High: The vulnerability is difficult to exploit, but exploitation could result in elevated privileges, significant data loss, or downtime.
CVSS Score: 7.0-8.9

Critical: Exploitation of these vulnerabilities likely results in root-level compromises of servers of infrastructure devices. Exploitation is usually straightforward, and does not need to persuade a target user into performing any special functions.
CVSS Score: 9.0-10.0

2.2.2.1.4 Consequence

This category considers the overall impact if the system were compromised. Consider the full cyber-physical implications. Can the solar system have an impact on the connected electrical system? Is the cyber-system tied to other critical systems on the network?

Table 5. Consequence chart.

Negligible	Minor	Moderate	Major	Catastrophic
1	2	3	4	5

Negligible: If the system is compromised, there is little to no impact on the power system functionality and no potential to pivot to other sensitive systems.

Minor: There may be minor impacts to the system if it is compromised. The system remains available and full control and operations can be quickly regained.

Moderate: There are noticeable impacts on system function if it is compromised. There may be short impacts to the availability of the system. Compromise of the system may expose other systems to potential access by the adversary.

Major: There are significant impacts on system function if it is compromised. There may be impacts to the availability of the system, including the potential for equipment damage and impact to the reliability of the connected electrical systems. Compromise of the system may expose other critical systems to potential access by the adversary.

Catastrophic: There is loss of control of the system and difficulty recovering control. There may be loss of availability of the system for an extended period of time, or significant impact to connected electrical systems. Compromise of the system may expose other critical systems to potential access by the adversary.

2.3 Edwards Air Force Base Example

Figure 4 is based on a conceptual communications diagram created by third-party battery integrator Smart Energy Storage and Energy Management (STEM)[a] for the RESET project. It represents a potential solution for retrofitting Edwards Existing Solar but does not contain any identifying information. The following is intended as a hypothetical feasibility study and should not be considered as an accurate representation of EAFB.

2.3.1.1 Network Equipment

2.3.1.1.1 Equipment Age

Legacy Schweitzer Engineering Laboratories (SEL) equipment in use at EAFB is still being supported by the vendor. While upgrades are possible, keeping this equipment in place is the most practical solution. One potential upgrade could be replacing the network switches with ones that support modern solutions, such as software-defined networking. For the size of this system though, other solutions might be more practical.

2.3.1.1.2 Ports and Connection Types

The computers used in this configuration can be ordered with multiple ports. This will aid in the network segmentation discussed later.

2.3.1.1.3 Proprietary Equipment and Operating Software

STEM's Athena software is proprietary. However, it is used as a monitoring and optimizing tool. Even if the software was removed, the system would continue working.

2.3.1.2 Connected Devices

2.3.1.2.1 Local Connectivity

Existing equipment at EAFB likely does not use MFA and uses local only passwords, which do not get changed regularly. A Remote Authentication Dial-In User Service (RADIUS) server could be set up as part of the upgrade, which would allow many devices to authenticate. In addition, RADIUS could be set up to use MFA, thus requiring and enforcing password requirements. With the correct mitigations in place, the DoD common access card (CAC) MFA could be incorporated.

2.3.1.2.2 Wireless Connectivity

In order to connect to the cloud service, STEM relies on a cellular connection. This risk is mitigated (but not negated) by:

a. Using an internet protocol secure (IPSec) VPN tunnel.

b. Using the firewall capabilities of the router to filter down to only allowing the connection(s) required by the cloud solution.

2.3.1.2.3 Lifecycle Management (LCM) Plan

One of the biggest challenges with LCM is the ability to keep the system up-to-date. Maintenance for the long-term must be factored into this upgrade. Contracting this out could be a better solution.

2.3.1.2.4 Supply Chain Security

Existing DoD policies should be followed for supply chain security on any new purchased equipment.

a. https://www.stem.com/.

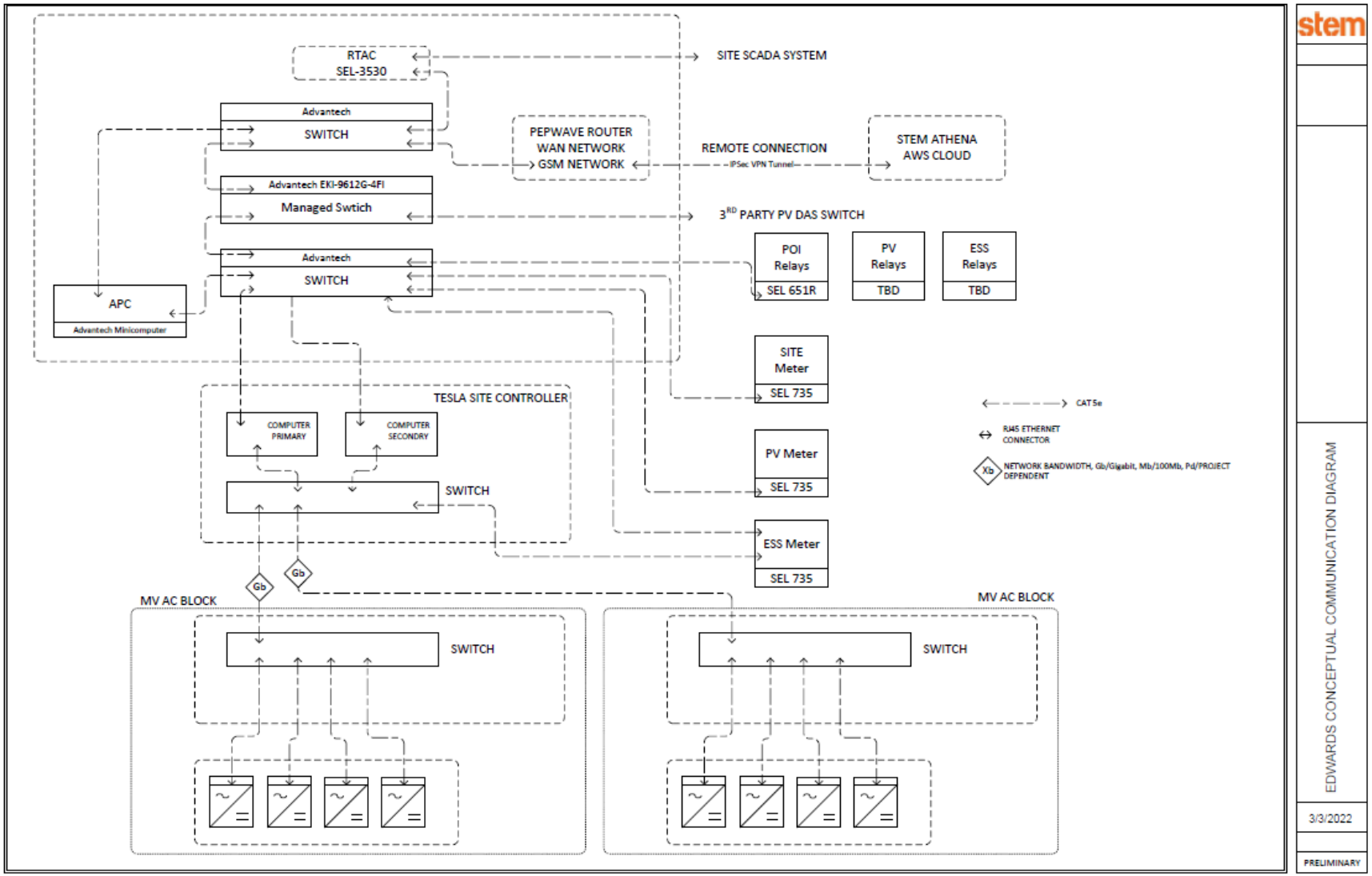


Figure 4. EAFB conceptual communication diagram.

2.3.1.3 Network Connections

2.3.1.3.1 Protocols

The STEM solution continues to use the existing ModBus communication. Devices should support more secure protocols if updating was desired. However, doing so would add time and cost to the upgrade, as well as increased the required training needed for engineers. For this system, other solutions to mitigate the risk might be more effective.

2.3.1.3.2 Encryption

The STEM solution uses a standard encryption when connecting through an IPSec VPN tunnel.

2.3.1.3.3 Network Segmentation

The STEM solution breaks out the system into logical subunits, which could be used to segment. While it would be easier to make this a flat network, architecting the network is a must. A less expensive solution of using virtual local area network (VLAN) switches to create logical (but not physical) separation is an ideal solution to keep costs down.

2.3.1.3.4 Cloud Connections

Like many solutions, STEM utilizes a cloud connection for their Athena Smart Energy Software. This cloud solution allows artificial intelligence (AI) to optimize energy resources. However, this increases the Access/Opportunity Risk. This risk is mitigated (but not negated) by:

a. Using an IPSec VPN tunnel.

b. Using a reputable cloud service, such as AWS.

c. Using MFA.

2.3.1.3.5 Network Monitoring

The DoD uses the Assured Compliance Assessment Solution (ACAS) for its network monitoring. This system must be Global Information Grid (GiG)-connected; however, it is no longer a closed, isolated network with the STEM cloud solution, so adding STEM to the ACAS only introduces a small amount of risk, which is easily negated by the benefit it provides.

2.3.1.4 Personnel Roles and Knowledge

2.3.1.4.1 DoD

The roles for this system should already be defined by EAFB and would only have minor changes for this upgrade.

2.3.1.4.2 Third-party Integrator

In this case, STEM would be the third-party integrator. As an experienced company, they should be able to provide the needed documentation and training to support the upgrade.

2.3.1.4.3 Electric Utility

EAFB is supplied medium voltage electrical power from Southern California Edison (SCE) with the Option D tariff rate at 34.5 kV through three service entrance switching stations, located at:

a. Main North Base - Switching Station-1.

b. South Base - Switching Station-3 and Switching Station-4.

c. AFRL - Switching Station-2.

Smaller portions are provided by a Western Area Power Administration (WAPA) hydropower allocation and its power purchase agreement for the output from the existing solar PV located on EAFB.

2.3.1.5 Risk Evaluation

2.3.1.5.1 Step 1: System as Operated

It is difficult to evaluate the original system since there was very limited information available. However, we make some base assumptions, and emphasize that the value in these risk evaluations is in comparing the cyber-risk of the new system to the cyber-risk of the old system in order to determine whether the change in cyber-risk of the resilience upgrades is acceptable:

Consequence: Most DoD bases will be backed up by reliable utility connections. Most onsite energy assets, even if networked, will be well-protected or isolated from the general DoD network. The consequence would likely be limited to the renewable generation.

Opportunity: Most onsite energy assets, even if networked, will be well-protected or isolated from the IT DoD network. Many renewable systems are not connected at all to the DoD systems and are instead managed by third-parties.

Adversary: DoD bases could generally be considered a valuable target for adversaries. However, it is unlikely that a nation-state would target a specific base's renewable energy assets, unless it was part of a larger attack. Organized insider adversaries are also possible, but unlikely, due to the vetting of DoD personnel. An organized group is likely the highest adversary that a DoD renewable energy installation would face.

Vulnerability: Given the fast development cycle and general lack of security considerations for OT and Distributed Energy Resources (DER) components, medium to high vulnerabilities may exist for the system.

List the selected rankings here:

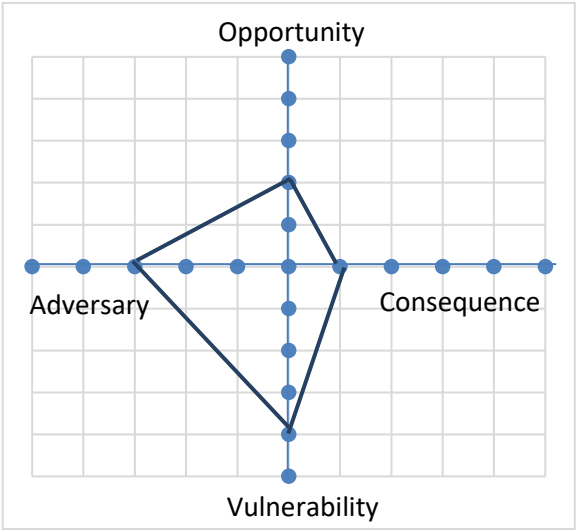
Consequence: 1

Opportunity: 2

Adversary: 3

Vulnerability: 4

Mark the rankings on the chart below:



Calculate the total risk as the area inside the quadrilateral:

Risk = ½ ((Consequence + Adversary) (Opportunity + Vulnerability)) = 12 (max risk score: 50).

2.3.1.5.2 Step 2: System with Proposed Upgrades

In this step, we particularly evaluate the changes to the system as proposed by STEM:

Consequence: Under the new proposed system, the solar + storage system would have the capability to contribute to ancillary services and the STEM controller would allow for optimal control of the system for maximum revenue. Given these increased capabilities, there is a greater consequence if the system were compromised, misused, or taken out of service by an attack. Reliability of connected systems should still be secure. Compromise of the system would not expose other systems to the adversary.

Opportunity: Due to the increased remote connectivity and cloud connection, there is a larger attack surface. Access from the local network is possible due to the use of insecure protocols, but external access is still well-protected.

Adversary: The changes to the system do not make it significantly more or less desirable for an adversary to attack, nor do they change the most likely type of adversary the system would face.

Vulnerability: Without a deep assessment of the technology used by STEM, it is difficult to say whether the severity of vulnerabilities for the overall system changes. Due to the increased complexity of the system and the requirements for a correct implementation of the network segmentation and communications architecture, we assess there is a possibility that the vulnerability level will increase.

List the selected rankings here:

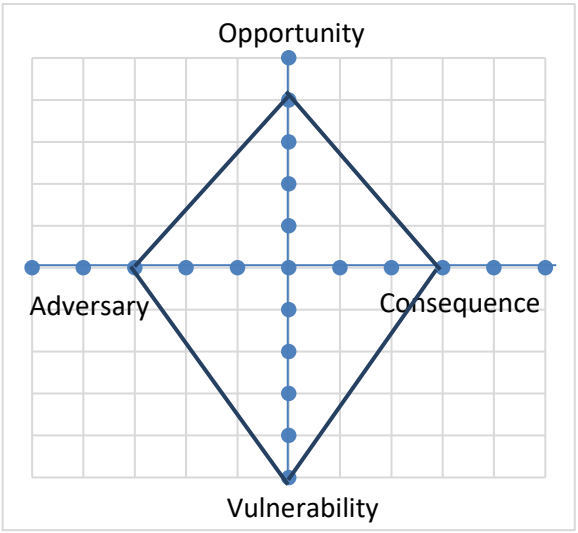
Consequence: 3

Opportunity: 4

Adversary: 3

Vulnerability: 5

Mark the rankings on the chart below:



Calculate the total risk as the area inside the quadrilateral:

Risk = ½ ((Consequence + Adversary) (Opportunity + Vulnerability)) = 27 (max risk score: 50).

2.3.1.5.3 Step 3: Mitigations Applied

In the final step, we assume that best practices, as discussed earlier, are applied:

Consequence: We assume that the system is still operating under a maximum revenue generating model. However, the consequence of a successful attack could be mitigated if the attack could be quickly corrected and stopped by using a network monitoring or intrusion detection system.

Opportunity: With an implemented RADIUS server and proper assurance of secure wireless connectivity using firewalls and VPNs, the opportunity and access to the system decreases.

Adversary: The risk mitigation measures do not change the type or capabilities of an adversary that might attack the system.

Vulnerability: Appropriate use of risk mitigation measures like network segmentation and patch management can help reduce the number and severity of vulnerabilities in the individual components and system architecture.

List the selected rankings here:

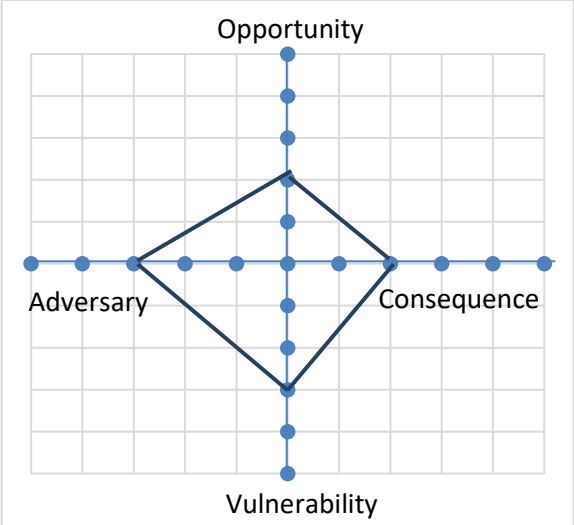
Consequence: 2

Opportunity: 3

Adversary: 3

Vulnerability: 3

Mark the rankings on the chart below:



Calculate the total risk as the area inside the quadrilateral:

Risk = ½ ((Consequence + Adversary) (Opportunity + Vulnerability)) = 15 (max risk score: 50).

2.3.1.5.4 Conclusion

The addition of the cloud-based controller and storage system will allow for more resilience and economic profit of the system. It also has the potential to significantly increase the cyber-risk of the system. However, using simple and cost-effective risk mitigation measures can bring the cyber-risk back down to near the original level of risk. Despite the many system changes, the final solution is one that does not significantly increase the cyber-risk. If the system owner/operators or DoD managers in charge of the system were comfortable with the original level of risk, they should be comfortable with the cyber-risk associated with the new system.

3 LESSONS LEARNED

3.1 Importance of Lessons Learned to Successful Project Planning and Execution

Inclusion of lessons learned early in the planning phase of projects is arguably the easiest and most cost-effective way to enhance the resilience and security of new or upgraded systems. Project planners should cast a wide net when looking for applicable lessons learned. Insights from past and present internal and external projects, whether directly or tangentially related to the project being planned, can provide valuable guidance that ultimately reduces project risk and increases security from day one.

Mistakes and incidents that are not adequately documented, studied, and used as learning material are almost assured to occur again. Likewise, successes should be documented and used as lessons learned to ensure that organizational best practices are continually upheld and improved. Organizations often do not look for and document lessons learned until after a project has been completed, which is a passive and delayed form of organizational learning and performance monitoring. Lessons can be identified at any point during a project. Continually being aware of these opportunities enables planners to more effectively implement and share potentially critical information.

Organizations should have formal procedures in place for the collection and processing of lessons learned. The U.S. Department of Energy (DOE) standard DOE-STD-7501-99 entitled "DOE Corporate Lessons Learned Program," is one such example of a federal lessons learned program. In addition, organizations like the Project Management Institute (PMI) produce educational materials that can help leaders and project planners implement effective lessons learned programs within their organizations. In addition to collecting lessons learned from within one's own organization, various avenues for obtaining lessons learned information from outside one's own organization exist. A contextually relevant example of such a resource is the North American Electric Reliability Corporation (NERC) Lessons Learned web page, which provides detailed descriptions and analysis of key lessons learned by various electric sector entities throughout the U.S. For industrial control systems (ICSs), specific lessons learned, and other useful information, the U.S. Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) ICS advisories and reports page (https://www.cisa.gov/uscert/ics) is an invaluable resource for DER and OT systems owner/operators.

In addition to more general methods of lessons learned collection, site specific evaluations and assessments should be conducted prior to operationalizing new or modified systems and at regular intervals during the lifecycle of an asset. Independent entities, both private and governmental, provide a variety of assessment and evaluation services that can help to identify potential risks and security issues of DER systems. A non-exhaustive list of lessons learned relevant to DERs and DoD installations has been compiled from previous INL field testing, research, and interviews with SMEs involved with/from the DoD. There may be redundancy from other sections, but the point here is to showcase lessons learned from actual installs to increase focus to these areas.

3.2 Cyber/DoD Facility Energy Lessons Learned

Table 6 provides a look at the Cyber/DoD facility energy lessons learned.

Table 6. Cyber/DoD facility energy lessons learned.

Number	Lesson	Additional Comments
1	Using an authenticated protocol provides a lot of protection, but that protection is eliminated if there is also an unauthenticated protocol that can be just as easily used.	To guarantee the protection from the authentication, use a firewall that filters out any traffic on unauthenticated or unapproved protocols. Also ensure that the other protocols are disabled on the device.
2	Authentication methods for authenticated processes/protocols (certificates, tokens, etc.) that are not implemented correctly can be easily evaded.	There can be a tendency to implement cyber-controls as just part of a checklist process. Just because a box is marked on a checklist does not mean that a cyber-control was configured properly. Special attention should be paid when implementing authentication methods.
3	Device whitelisting (e.g., what computer is allowed to talk to the field device) is effective at preventing spoofing from other devices on the network.	Many devices allow you to configure this in the device itself. If not, whitelisting also can potentially be done at the switch level.
4	Make sure it is known what ports on the device interfaces are open, what the purpose of each is, and if it is necessary for the port(s) to be open. Vendor maintenance or testing interfaces may not be closed before device commissioning.	The PPSM is a required document for the RMF process that details this information. Routine scanning should be done to verify ports. (Skipping equipment that can be potential broke by scanning.)
5	If secure shell (SSH) is used on a device, protect that interface with a key, not just a password that can be brute-forced. Using MFA is even better.	It doesn't matter if the protocol is secure if someone gains access to your username and password.
6	The legitimate interface of a device can be misused by someone who understands how the device works and what system it is connected to.	Implement secondary monitoring and backup sensors to detect if a device is behaving unexpectedly.
7	DoD often does not sufficiently self-assess incidents or near-mises to determine root-causes and implement remediations.	DoD should strive to become more of a learning organization.
8	DoD facilities often look to use existing or decommissioned equipment to help integrate new systems instead of purchasing equipment that is modern and best-suited for the task.	There is no way around cyber-risk management costs and there is only so much that can be done to protect legacy equipment.

Number	Lesson	Additional Comments
9	Bases often implement easier to manage flat networks for control systems when integrating DERs instead of implementing more secure layered network architectures.	Flat networks are easier to set up initially, but much harder to protect. Segmenting networks is a key practice to protecting networks.
10	Not accurately defining authorization to operate (ATO) boundaries can lead to not seeing or protecting internet connections that are on the fringe of the network.	Every entry and exit point of the network must be accounted for and an ATO boundary protection device used to limit traffic to only clearly defined traffic for the port in question.
11	Manufacturers with access to devices once they are deployed is something that is not well-monitored or controlled.	Special consideration should be made on whether to allow manufacturer access. If the decision is yes, proper controls should be put into place to monitor any access that is given.
12	DoD installations often lack good designs and/or architectural patterns for connecting on-base assets to off-base locations.	Project planning should address what security measures/designs need to be in place to enable on-base to off-base asset connections.
13	Installations often lack a plan for managing equipment and system updates once they are deployed.	Project planning should implement controls and procedures for completing manufacturer software/firmware updates.
14	Installations often don't follow/implement manufacturers recommendations regarding system hardening guidance or ask manufacturers if they have suggestions/guides to harden devices and systems.	Manufacturers often know their product best and have recommendations that should be followed.
15	Projects get deployed and taken to operational status before they are complete. Devices end up receiving updates to firmware and source code once they are operational, which makes it impossible to continuously assess the security of the systems.	Implement procedures for tracking system changes and continuously re-evaluating system security.
16	Independent risk/security validations and assessments don't get conducted early enough or often enough in project lifecycles (assessments by contracted personnel).	A risk assessment doesn't have to wait until the system is installed and running. For example, having the independent team view the conceptual design can catch things up front that will cost more money to find and fix later.
17	DER/OT assets cybersecurity managed by already overloaded IT personnel who don't possess the specific DER/OT experience and knowledge to effectively manage those assets/systems.	Ensure individuals tasked with configuration and/or management of DER/OT systems have sufficient bandwidth, training, and availability to effectively perform the tasks.
18	A dedicated Project Manager (PM) must be assigned to track scope, cost, and schedule.	Cybersecurity can be extremely expensive and time-consuming. Proper management of time and expenses can lead to a more successful and secure project.

Number	Lesson	Additional Comments
19	All team members should have adequate cyber-training to understand the RMF process.	There are many available options for training. One that comes highly recommended are ISC² certification courses. This training needs to be continuous and members of ISC² need to have access to continuous training courses.
20	The time required to prepare documentation, process, and input into eMASS will be greater than expected.	While it doesn't seem like documenting the required information should take long, it is a very tedious process. Be sure to account for this time in your budget.
21	Regular communication is critical.	It's easy for cyber-risk management to get pushed to the side in lieu of other project deadlines.
22	Use of local password-protected only devices can lead to challenges with storage, management, loss of passwords, and associated effects when passwords are lost or mismanaged.	Alternative authentication and protection methods may be more manageable, depending on the system. MFA, badge-access/pin systems, software-defined networks for control of which devices can utilize a network, etc., may be more effective.
23	The RMF process is owned by the installation or system owner, but the process in some cases can require others outside of the control of the system owners to review, assess, and approve. This can impact schedule and cost.	Ensure you know who is supporting and understand the review times before developing a tentative schedule.

4 CURRENT AND EMERGING CYBER-RISK MANAGEMENT SOLUTIONS

Retrofitting a system allows an opportunity to add additional solutions to your system that could potentially decrease the cyber-risk. These measures can add cyber-resilience to a system from the design phase, and are good to consider alongside the upgrades made to improve power resilience. This list is not intended to be exhaustive but focuses on more commonly used solutions, as well as a few emerging solutions.

4.1 Physical Security

The security standard for substations has always been physical security measures, such as barbed-wire fences, external security cameras, door and window alarms for all structures, and motion detectors within the parameters and structures. These security assets are typically viewable at the utility command center where the alarms will indicate if an unauthorized person has entered the premises. These are not only a strong deterrent for malicious intruders, but they serve as a strong defense for animals and keep the power generation and control equipment safe. In addition to security, a camera positioned at the meters and relays can be used as a ground truth system to verify readings without sending a technician. Even if the solar assets are on a military base that requires CAC badges for entrance, a defensive perimeter fence with video monitoring is highly recommended.

4.2 Phishing Detection

The most common cyber-events that regularly occur are email phishing events. The 2015 Ukraine power grid attacks that knocked out power to 30 substations and 230,000 people originated with successful phishing attempts. Phishing detection software can identify malicious emails, quarantine them, and identify the system administrator before they spread throughout the system.

Some common email security platforms are offered by Area1 Security, GreatHorn, Avana Cloud Email Security, and Cofense.

4.3 Firewalls

Firewalls can be a hardware or software security device that is installed on a network to monitor incoming and outgoing internet traffic. Firewalls can restrict access across a network with the aid of pre-determined rules that are implemented to reduce the likelihood of a cyber-attack. Firewalls can also be used to segment a network and add depths of defense depending on where they are installed on the network. Firewalls are a very passive system that can thwart a denial-of-service attack, but they do not perform packet inspection and they will not prevent a phishing attack or other common security threat.

For the energy sector, firewalls are generally installed at common points of connection to protect downstream equipment and keep attackers out by providing tunneling between networks for approved users. Figure 5 shows firewalls installed at the substation and the command center, this architecture helps in preventing an attacker from navigating to the intelligent electronic devices in the substation that could manipulate the flow of power. The substation monitoring the solar assets should have a firewall installed to limit access to unauthorized personnel and securely tunnel traffic back to the utility command center.

Some of the most common firewalls are the MSi Platform by Mission Secure, Wildfire by Palo Alto, Embedded Security CSP by Symantec, and BotHuter Malware Infection Diagnosis System by SRI International.

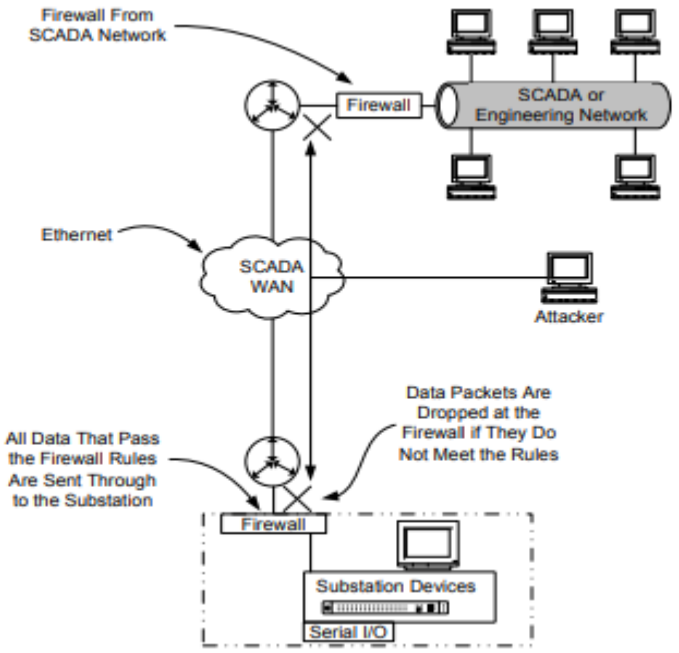


Figure 5. Example firewall installation, courtesy of SEL.[b]

4.4 Network-based Intrusion Detection Systems

Intrusion detection systems typically fall into one of two categories, network-based or host-based. Network-based detection systems are typically a stand-alone device placed on the network that monitors all data packets and attempts to prevent malicious activity before it arrives at the intended workstation. Host-based detection systems are a software security measure that is installed on each device individually to prevent attacks as they arrive on the host workstation. These systems can work simultaneously; in fact, many companies offer products that use both Host-based Intrusion Detection Systems (HIDSs) and Network-based Intrusion Detection Systems (NIDSs) to fully protect a system. Figure 6 shows the differences in the security setup.

b. https://cms-cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6427_ImplementFirewalls_DA-NK_20100224_Web2.pdf?v=20181015-211334.

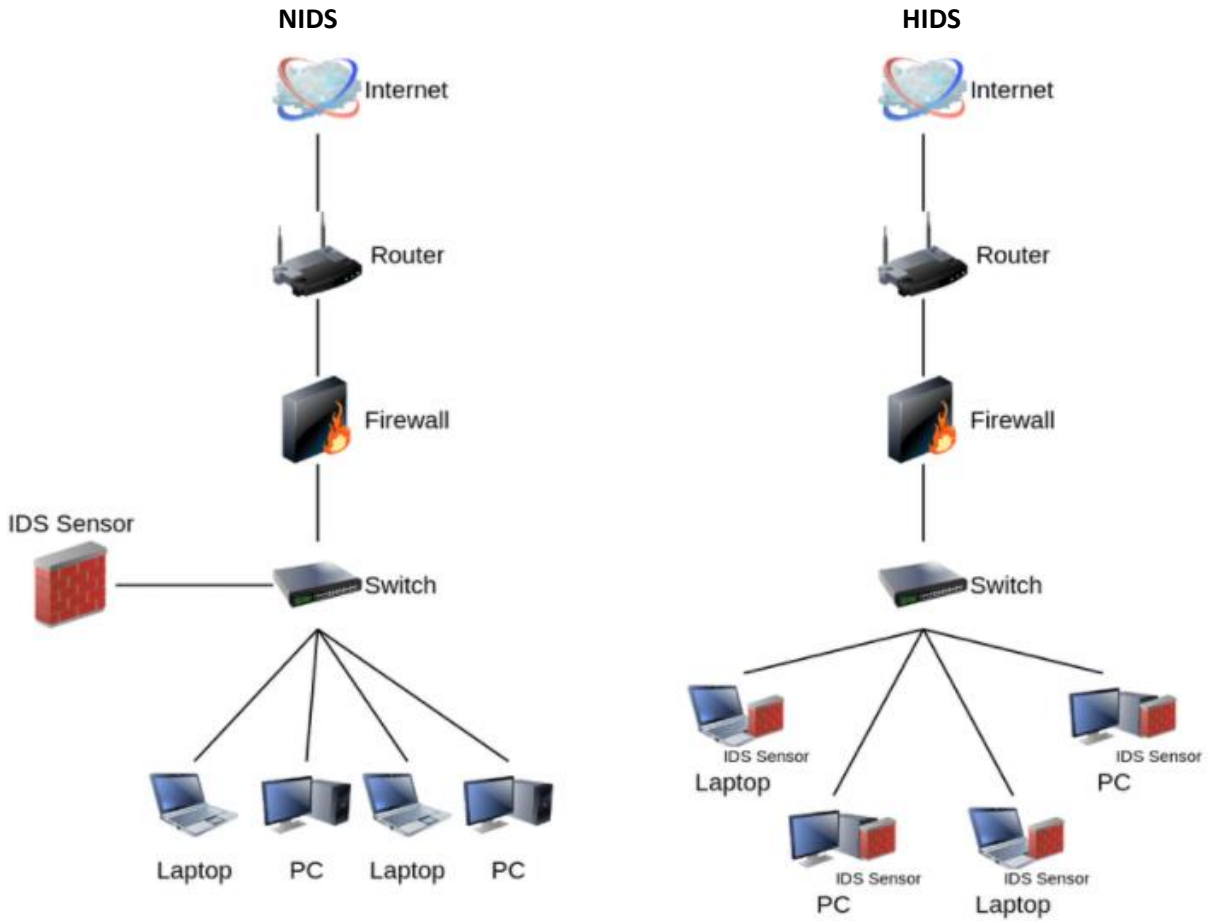


Figure 6. Comparison of a typical NIDS vs. a HIDS, courtesy of ResearchGate.[c]

4.4.1 Host-based Intrusion Detection System (HIDS)

HIDS were the first type of intrusion detection system and were originally developed for monitoring computing mainframes. This security software is installed on the host machine to analyze network packets and monitor the internals of the computing system. HIDS use object-database logs to find anomalies in the network traffic. These logs allow the HIDS software to track changes to the system and detect potentially malicious activities.

HIDS are considered a passive defense that will alert for malicious or anomalous activities. This alert can be local, or if on a network, it will alert the administrator. Typically, HIDS do not actively prevent unauthorized malicious activity.

When considering security for a solar site, HIDS are not a silver bullet. Many assets in a substation—such as power relays, meters, solar inverters, and other intelligent electronic devices—might not have the ability to support HIDS software. This security system is designed for security operation centers with a high concentration of workstations.

Some of the most common HIDS are Protect by Cylance, Fidelis Endpoint, Fidelis Elevate by Fidelis Cybersecurity, and McAfee's Host-Based Security System (HBSS).

c. https://www.researchgate.net/figure/Network-based-IDS-left-vs-Host-based-IDS-right_fig5_346499141.

4.4.2 Network-based Intrusion Detection System (NIDS)

NIDS are typically a physical device installed on a network, much like a firewall. NIDS differ from firewalls by how they operate. Firewalls are installed on the edge of the network and use rule-based routing to provide communication between devices. NIDS are installed inside the network where they can monitor all packets on the network. These packets are then compared against a library of known attacks. Once anomalous activities are identified, the NIDS can determine if the attacks are originating internally or externally on the network by packet inspection.

When considering security for a solar site, NIDS are a very good choice. Many assets in a substation such as power relays, meters, solar inverters, and other intelligent electronic devices might not have the ability to support HIDS software directly on their system, but a NIDS can monitor the traffic and alert at the first sign of malicious activity. This security system is designed to monitor the traffic between a high number of intelligent devices and works well in the utility industry.

Some of the most common NIDS are the Dragos Security Suite, the Supervisory Control and Data Acquisition (SCADA) Guardian by Fortinet-Nozomi Networks, Silent Defense by Security Matters, and Suricata IDS.

Some of the most common security platforms that offer both HIDS and NIDS are the Claroty Platform, the Indegy Platform, the CB Response by Carbon Black, the Open-Source Security Onion, and the CISCO Intrusion Prevention System Threat Response.

4.5 Security Information and Event Management (SIEM)

SIEM tools are essentially data aggregators that conduct event analysis in real time by monitoring log files and security alerts from other cybersecurity programs, such as NIDS, HIDS, firewalls, and email security systems to provide a response in real time. Figure 7 shows the SIEM as a data aggregator proving a simplified data feed to the security operations center. SIEMs can be set up to monitor other cybersecurity on the network like firewalls, email security systems, antivirus software, IDSs, and provide the security operations center with simplified feedback.

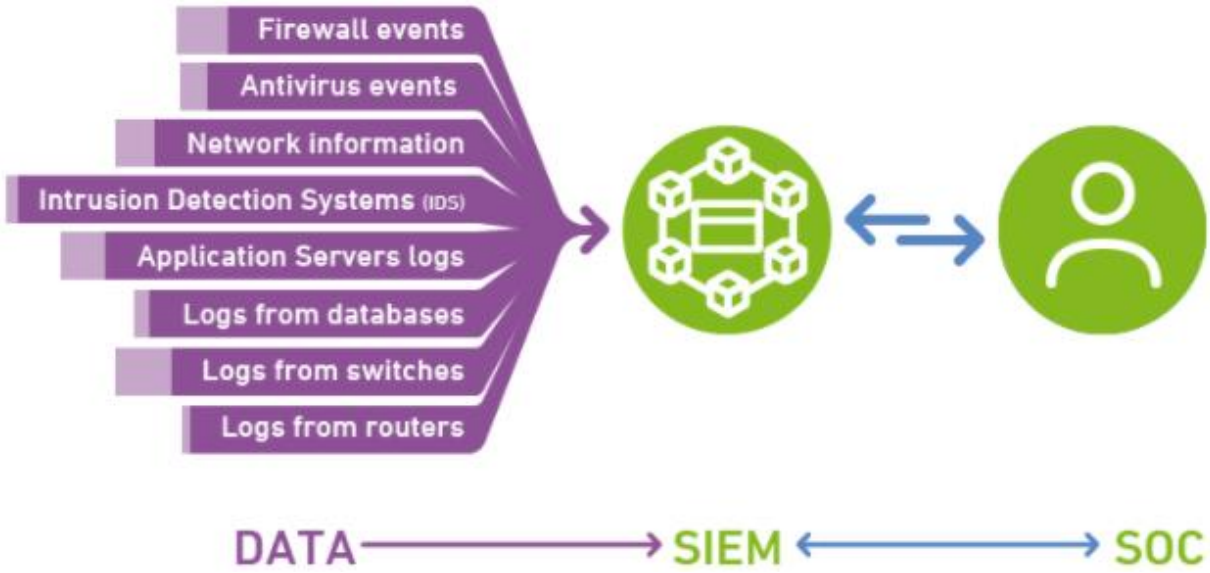


Figure 7. Example of a SIEM system conglomerating data from numerous cybersecurity assets, courtesy of LeaseWeb.[d]

d. https://www.leaseweb.com/cyber-security/managed-cyber-security (courtesy of LeaseWeb).

SIEMs work by learning what network traffic is normal. This learning session is completed in a controlled environment under normal operations with standard network traffic. Learning sessions vary by manufacturer, but a typical power system will need to operate normally to generate network traffic for a set period of time. While in the learning session, the command center would need to operate any relays or reclosers that are typically operated and log into access level two to perform settings changes and push downloads, as well as any other normal operations the utility might have. This will allow the SIEM to learn which computers and users can access devices and what types of commands are normal. Once the learning session is complete, any new devices on the network or unauthorized requests will generate an alert. If new events happen, such as new users or devices appearing on the network or if large amounts of data are being downloaded at odd hours, the SIEM will actively fight off the anomalous activity with its predesigned playbooks.

The playbooks are a set of responses designed by the user to thwart malicious activity. Playbooks are used for standard operations, such as identifying malicious links in phishing emails, preventing unauthorized software updates, or identifying new users and alerting the security operation center. If the type of attack was not programmed into the playbooks by the system administrators, it is possible that the SIEM system would not stop the attack.

The modern substation has many intelligent devices, such as power relays, meters, routers, and firewalls. This generates a lot of data for a security operations center. A SIEM system can reduce the amount of nuisance alarms and decrease operator fatigue. SIEMs are common in the utility sector and should be considered for solar asset monitoring and cybersecurity.

Some of the most common SIEMs are the Palantir Cyber, the XSense by CyberX, the SPYRUS Enterprise Management System (SEMS), the Verve Security Center, and the VNSOC360° by InfusionPoint.

4.6 Security Orchestration Automation and Response (SOAR)

SOAR tools are a new technology that uses machine learning to perfect cybersecurity alerts and mitigation. SOAR tools were built to bring all cybersecurity data to a single user interface to assist operators by reducing nuisance alerts. The SOAR software is based on custom playbooks a security team would need to program. These playbooks are the rules that govern the network for events such as adding a new user, adding a new device to the network, anomalous activity, or unauthorized downloads or uploads. To operate these playbooks, the SOAR receives input from other security devices on the system, such as firewalls, email security systems, antivirus software, intrusion detection systems, and web content. The results from these independent monitoring systems are combined in the SOAR, thus reducing the security interfaces the operator would have to monitor. When an anomalous event is detected, the SOAR can automatically operate the desired playbook to isolate and quell the cyber-event.

SOAR playbooks are much more advanced than SIEM playbooks. SOAR can create incident tickets and forward them to relevant teams, automatically add firewall rules to block new devices, and even disconnect workstations from the network if they show signs of malicious activity. SOAR architecture and software was designed based on SIEMS and therefore is a newer generation of orchestration. It does appear that SOARs eventually will replace SIEMs—especially on larger utility systems with dozens of substations. However, for small solar assets, a SOAR system might be too cumbersome to set up for what it has to offer.

Some of the most common SOARs are Metron by Apache, Verodin’s Security Implementation Platform (SIP), Cyber-Triage by Basis Technology, Demisto, and eyeShare by Ayeho.

4.7 Data Flow Reader

Data flow readers or data diodes are used to prevent the flow of data in one direction. This is a useful method for protecting power system equipment because it allows the security operations center to monitor the asset in real time, but it is impossible for the device to receive updates. This drastically reduces the attack space and prevents unwanted access, updates, or settings changes.

Figure 8 shows the OwlCyberDefense data diode that is currently in use. The source would be the solar assets or substation and the destination would be the security operation center. This setup would eliminate all updates, commands, and malicious activity to the substation without being physically present at the source to plug into the devices. This security feature, while very secure, would also require sending a utility team out to the substation for all settings changes. This can result in costly maintenance if the site regularly encounters faults. If the solar asset is easily accessible, this is a very secure option.

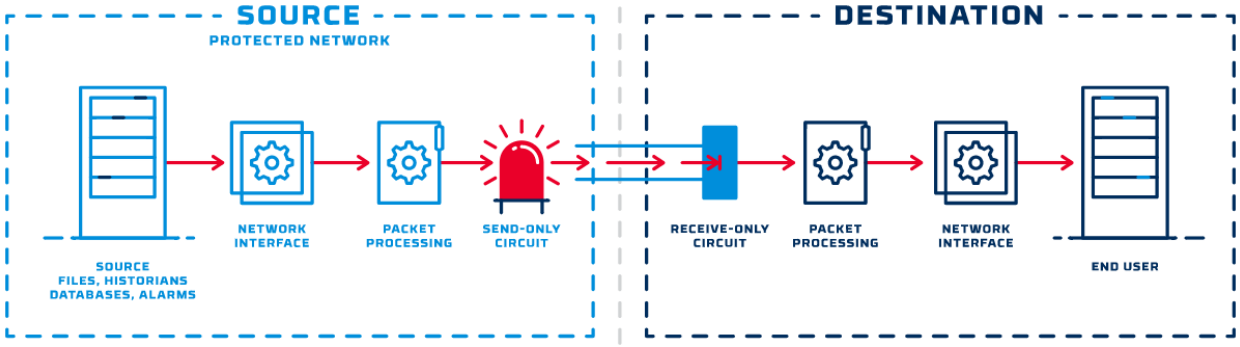


Figure 8. Installation of a data diode to block incoming data (courtesy of OwlCyberDefense).[e]

Some common data diodes are offered by Owl Cyber-Defense, FireEye, and Waterfall Security.

4.8 Vulnerability Scanner

A vulnerability scanner is a tool used to assess the vulnerability of a network. A scanner typically identifies all devices on a network by the media access control (MAC) address of the device. This MAC address contains a description of the devices that a scanner uses to check for known vulnerabilities. If a device is found to be vulnerable, the scanner then notifies the system administrator. A scanner can be network-based to identify potential security attacks, host-based to monitor a workstation, a wireless scan to identify unsecure access points, or based on a database to identify missing security patches.

The most common vulnerability scanner used by DoD is Nessus by Tenable, as shown in Figure 9.

e. https://owlcyberdefense.com/learn-about-data-diodes/.

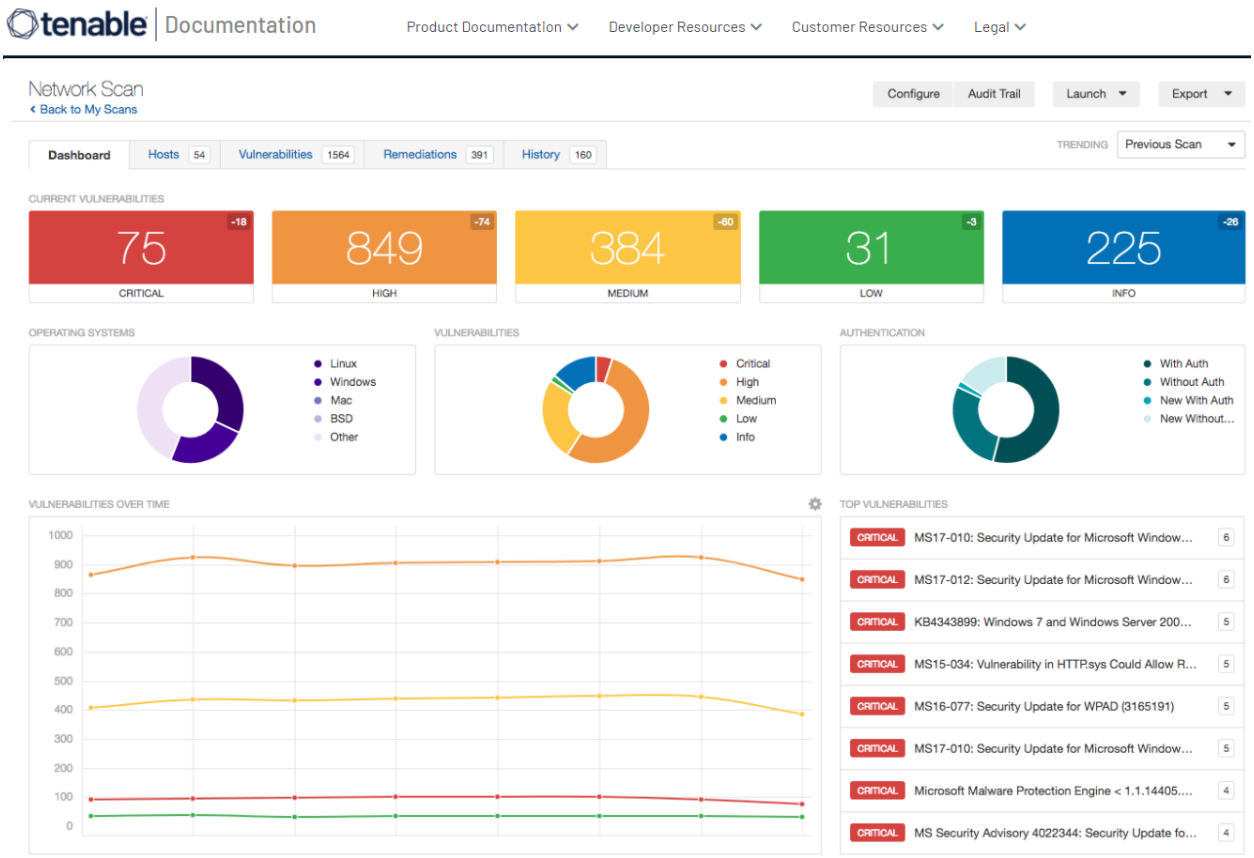


Figure 9. Nessus vulnerability scanner interface showing potential vulnerabilities on a network (courtesy of tenable).[f]

4.9 Cloud-Based Data

Small utilities are increasingly looking to cloud-based computing and analytics like AWS to process power system data. The driving force behind this is to alleviate the liability and cybersecurity infrastructure cost on small utilities and co-ops. As NERC Critical Infrastructure Protection (CIP) increases cybersecurity regulations, small utilities that might not have the expertise or manpower to meet the standards have started to look to cloud services. This is a new market segment and there is very little information on it. However, the DoD does have a classified cloud server and a military base could be an optimum test location.

4.10 Cybersecurity Defenses on the Horizon

4.10.1 Hardware

4.10.1.1 Master State Awareness Estimator (MSE)

The MSE is an out-of-band power monitoring and network security appliance that serves as a redundancy for normal operations. Power monitoring is completed with real-time state estimation that verifies typical SCADA power measurements. Network security is accomplished through a machine learning algorithm that detects anomalous data on the network. Together, the MSE system can detect a range of cyber- and/or physical-events in real-time.

f. https://docs.tenable.com/nessus/Content/Dashboard.htm.

4.10.1.2 OPDEFENDER

OPDEFENDER is an INL-tested and validated system that significantly reduces cyber-attacks to ICS through network switches to analyze/filter network traffic in real-time. The system deploys protective countermeasures by limiting network traffic and alerting users to abnormal and potentially malicious messages.

4.10.1.3 Plug-N-Play Appliance for Resilient Response of Operational Technologies (PARROT)

PARROT is a device that is inserted between the communications and power pins of any field control device to provide continuous operation while monitoring for anomalous behavior. PARROT is an extra layer of security from cyber-attacks on critical infrastructure operations by isolating cyber-attacks with automated responses while also maintaining operations. Moreover, the flexibility of the device can also provide legacy systems and device operators with the ability to upgrade security without having to replace older models.

4.10.1.4 Constrained Communication Device (C3D)

The C3D project was the result of a scenario put forth by industry to answer the question, 'how can legacy power monitoring equipment be protected if an attack is imminent?' The result was the development of the Constrained Communication Device (C3D) network security device. This device is controlled by an out-of-band network that can selectively terminate communication to devices that are at an increased risk of cyber-attacks. This can be helpful if an adversary is detected on the network or if a family of devices is known to have a vulnerability and is waiting to be patched.

4.10.2 Software

4.10.2.1 Annotated and Translated Disassembled Code (@DISCO)

@DISCO is a graph-based datastore designed as a highly scalable platform to organize firmware and enable automated binary software analysis. @DISCO is based on open-source software that empowers real-time efficiency and storage for machine learning. Moreover, users can make it easier to work together on understanding an executable file via graph database.

4.10.2.2 Visualization Tool for @DISCO (DISCOverFlow)

DISCOverFlow is a visualization tool that consist of tools that are used to generate visuals from data gathered by @DISCO. Therefore, allowing analysts to understand how a program provides software quality assurance by displaying connectivity amongst each program.

4.10.2.3 Cyber-Physical Architecture for Automated Responses (CyPHAAR)

CyPHAAR is a platform that can take intelligent automated responses in a two-part process of anomaly detection and response actions. The aim is to provide a decision-making support framework addressing challenges such as the identification of the network nodes that need to be monitored in priority, or the best choice of countermeasures after an attack.

4.10.2.4 Exploit, Malware, and Vulnerability (EMV) Scoring Application

The EMV Scoring Application provides a framework that scores exploits and identifies potential threat object characteristics; therefore, prioritizing and efficiently utilizing cybersecurity resources. This scoring schema allows users the ability to tune the application into what works best for their systems and equipment.

4.10.2.5 Modeling and Simulation for Target Electrical Resilience Improvement (MASTERRI)

MASTERRI is an integrated software suite that accurately calculates device dependencies and resiliency to provide recommendations and assist in quantifying system vulnerability, as well as quantifying the advantages of specific system upgrades.

4.10.2.6 Scalable, Physical Effects Measurable Microgrid for Cyber-Resilience Analysis (SPEMMCRA)

The SPEMMCRA framework was created as a cost-effective method to assess the true effectiveness of cybersecurity technology for microgrids. The SPEMMCRA framework uses custom written software, a raspberry pi (small computer), and a swing equation to simulate a microgrid. As a result, the SPEMMCRA framework can identify cyber-attacks moving through a microgrid, help stop the treat, and restore operations to a normal state.

4.10.2.7 Structure Threat Intelligence Graph (STIG)

STIG is a tool that translates dense analysis code into easy-to-understand visual icons through creating, editing, querying, analyzing, and visualizing threat intelligence. It uses Structured Threat Information eXpression (STIX), version 2, as its data format. STIG uses a graph database to store data and display abnormal behavior that can help solve issues in a couple of hours rather than having to take weeks.

4.10.2.8 Structure Threat Observable Tool Set (STOTS)

STOTS is a collection of tools that allows users in a test environment to create STIX, version 2, observable objects.

4.10.2.9 Structure Threat Automated Response (STAR)

STAR provides a flexible framework to automatically execute a course of action in response to receive cyber-observable data objects. STAR enables the execution of tailored responses to cyber-issues in an operational environment.

4.10.2.10 What is Binary (WiiBin)

WiiBin is an initial forensics triage tool for unknown binary systems using machine learning methods to discover endianness, architecture, and potential operation codes to aid reserve engineering.

5 REFERENCES

[1] U.S. Government Accountability Office (GAO), "Climate Resilience: DoD Coordinates with Communities, but Needs to Assess the Performance of Related Grand Programs (GAO-21-46)," U.S. GAO, Washington, D.C., 2020.

[2] P. N. Stockton and J. P. Paczkowski, "Strengthening Mission Assurance Against Emerging Threats: Critical Gaps and Opportunitie for Progress," *Joint Forces Quarterly,* vol. 95, pp. 22-31, 2019.

[3] C. Crowell, "Inside BlockEnergy's Military-Tested Microgri and the Future of Distributed Renewable Energy," Solar Builder Magazine, 29 June 2020. [Online]. Available: https://solarbuildermag.com/featured/blockenergy-military-tested-microgrid-is-the-future-of-distributed-renewable-energy/.

[4] W. Rickerson, M. Wu and M. Pringle, "Beyond the Fence Line: Strengthening Military Capabilities Through Energy Resilience Partnerships," Association of Defense Communities, Washington, D.C., 2018.

[5] W. Rickerson, E. Brousseau, M. Pringle, J. Monken, J. Graul, T. Calvert-Rosenberger and J. Barker, "Regulatory Considerations for Utility Investments in Defense Energy Resilience," National Association of Regulatory Utility Commissioners (NARUC), Washington, D.C., 2021.

[6] "Annual Energy Management and Resilience Report (AEMRR) Fiscal Year 2019," U.S. Department of Defense Office of the Assistant Secretary of Defense for Sustainment (ASD(S)), Washington, D.C., 2020.

[7] "About the Risk Mangement Framework," National Instutue of Standards and Technology, 30 November 2016. [Online]. Available: https://csrc.nist.gov/projects/risk-management/about-rmf.

[8] B. Sobczak, "First-of-a-kind U.S. grid cyberattack hit wind, solar," E&E News, 31 October 2019. [Online]. Available: https://subscriber.politicopro.com/article/eenews/1061421301.

[9] Cybersecurity and Infrastructure Security Agency (CISA), "Rising Ransomware THreat to Operational Technology Assets," June 2021. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf.

[10] "New Release: Considerations for Retrofitting Existing Solar with Emerging Technology [RESET]," Converge Strategies, 14 December 2021. [Online]. Available: https://convergestrategies.com/new-blog/considerations-for-retrofitting-existing-solar-with-emerging-technologies-reset.

[11] National Instittute of Standards and Technology, "Best Practices in Cyber-Supply Chain Risk Management: Conference Materials," [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf..

[12] FERC, "18 CRF Part 35 Docket No. RM18-1-000," 10 October 2017. [Online]. Available: https://www.govinfo.gov/content/pkg/FR-2017-10-10/pdf/2017-21396.pdf.

[13] M. J. Culler, B. A. Stephen, K. A. Hovland, S. Morash, A. F. Snyder, N. Placer and J. P. Gentle, "Resilience Framework for Electric Energy Delivery Systems," Idaho National Laboratory, Idaho Falls, 2021.

[14] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," April, Washington D.C., 2018.

Appendix A –
Risk Evaluation Charts

Step 1: System as Operated

Use the criteria above to evaluate the system as it is currently configured and operated.

List the selected rankings here:

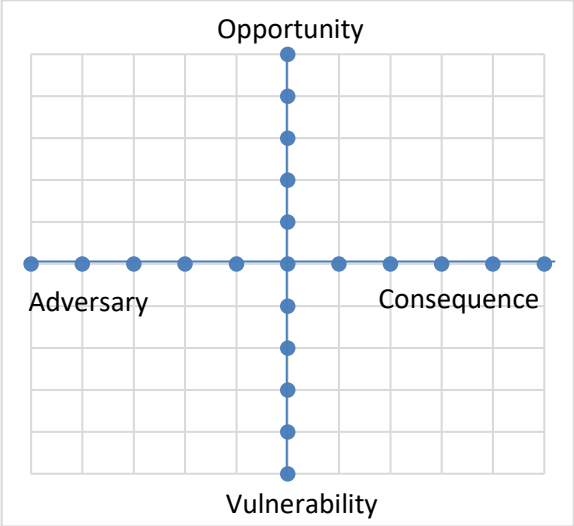
Consequence: _____

Opportunity: _____

Adversary: _____

Vulnerability: _____

Mark the rankings on the chart below:



Calculate the total risk as the area inside the quadrilateral:

Risk = ½ ((Consequence + Adversary) (Opportunity + Vulnerability)) = _____

Step 2: System with Proposed Upgrades

Use the criteria above to evaluate the system as it would be configured and operated with the proposed solar retrofits.

List the selected rankings here:

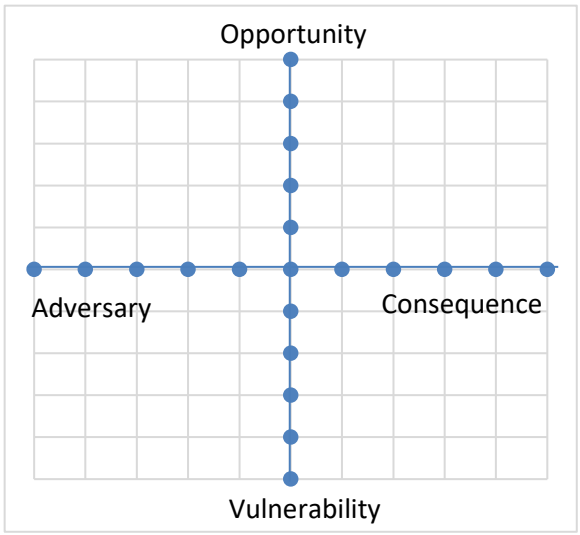
Consequence: _____

Opportunity: _____

Adversary: _____

Vulnerability: _____

Mark the rankings on the chart below:



Calculate the total risk as the area inside the quadrilateral:

Risk = ½ ((Consequence + Adversary) (Opportunity + Vulnerability)) = _____

Step 3: Mitigations Applied

Use the criteria above to evaluate the system with proposed upgrades and any mitigations enacted following Step 2. This evaluation should serve as a check that the proposed mitigations will reduce the cybersecurity risk to an acceptable level.

List the selected rankings here:

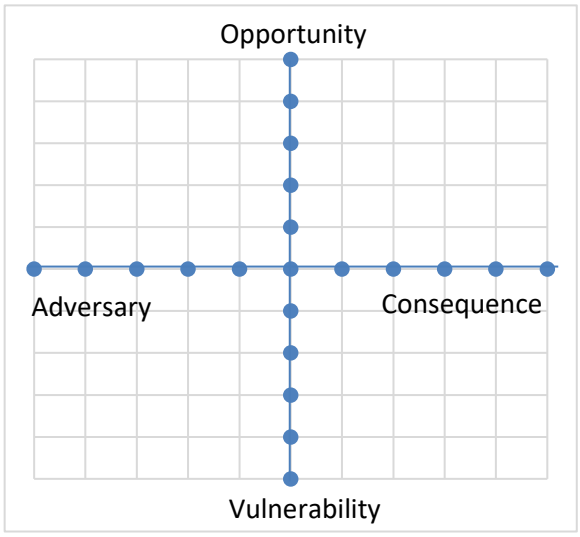
Consequence: _____

Opportunity: _____

Adversary: _____

Vulnerability: _____

Mark the rankings on the chart below:



Calculate the total risk as the area inside the quadrilateral:

Risk = ½ ((Consequence + Adversary) (Opportunity + Vulnerability)) = _____

Appendix B –
Risk Management Framework Questions

Adversary [Intent & Capability]

Risk Assessment

Component	Additional Comments	Response
Has a risk assessment report (RAR) been performed for the system?	RARs consider threats, vulnerabilities, likelihood, and impact to operations, assets, and individuals. Typically, an independent team is available to perform this assessment.	

Planning

Component	Additional Comments	Response
Is there an overarching document that details where to find all the related plans to the system, as well as an overview of the security requirements of the system?	One output of the RMF process is the System Security Plan (SSP). This helps to serve as the high-level overview of the security requirements and describe the controls in place or planned for meeting those requirements. If something similar already exists, the information from it can be utilized to place in the RMF format.	

Intent

Component	Additional Comments	Response
Has the system been evaluated by an external party to determine how valuable a target is to an adversary?	Independent reviewers provide a valuable outsider view.	

Capability

Component	Additional Comments	Response
Is information about the system concealed from public access?	Public access increased the risk of a system greatly.	

Access/Opportunity

Access Control

Component	Additional Comments	Response
Does the system have an automated account management solution (such as Microsoft Active Directory, AAA Server, Directory Server, or backend database, etc.)?	Having to individually manage account creations, account deletions, and password requirements can be complex and time-consuming. Having a centralized account makes it easier to meet these requirements.	
Is the system set up to audit account modifications and send those logs to a centralized location?	All account activities must be reviewed periodically to ensure that no suspicious activity has occurred. Manually reviewing these accounts would be complex and time-consuming.	
Is there an official system authorization access request process that is followed for all accounts?	Accounts should only be created for those individuals who need access to the system. A system authorization access request ensures that a record is kept of each user account that is created, that vets the user before access is granted, and that provides the rules that the user must follow.	
Is role-based access configured and enforced?	Only those who need administrator privileges should have them. This protects the system from harmful, deliberate, and accidental changes.	

Component	Additional Comments	Response
Is remote access allowed?	Remote access requires additional controls (e.g., monitoring, encryption, etc.) to be implemented. By not allowing remote access, the system is easier to manage.	
Is there any wireless access on the system (e.g., microwave, packet radio [UHF/VHF], 802.11x, Bluetooth)?	Wireless access required additional controls (monitoring, encryption, etc.) to be implemented. By not allowing wireless access, the system is easier to manage.	
Are external devices allowed to connect to the system?	External devices (such as a vendors maintenance laptop, or equipment from a different system) may not follow all the same risk management rules. As such, connection of any external device can create a vulnerability. Additional controls and processes are required to allow external devices to connect.	
Are session timeout, session locks, and system use notifications configured per STIG?	If system STIG requirements have been implemented, each of these requirements will be compliant.	

Awareness and Training

Component	Additional Comments	Response
Are users up-to-date with the required DoD cyber-trainings?	While this is a requirement to maintain ATO, the DoD trainings provide a solid foundation of cyber-training and is segmented by role to ensure the correct level of training.	

Component	Additional Comments	Response
Are any additional trainings needed to operate the documented system and are logs kept of who received them?	Depending on tribal knowledge regarding how to maintain and operate a system is a disaster waiting to happen. In other words, if something happens to a system when the normal experienced crew is unable to be on site, or mistakes happen because a complete training didn't take place, is something that should never be allowed.	
Are those who provide physical security up-to-date with their required DoD trainings?	Physical security is a critical part of maintaining a cyber-secure posture. Their eyes and ears often see and hear things that others do not. By making sure employees are adequately trained in cyber-risk management, they can be better utilized.	

Audit and Accountability

Component	Additional Comments	Response
Is the system configured to log access attempts at critical access points?	Knowing who and where systems were accessed can be invaluable during an incident and post-evaluation.	
Is the system configured to audit, analyze, and report events that could cause harm?	Systems can be configured to report information that can be used to alert regarding a cyber-incident. Newer tools can take actions to prevent that incident from escalating.	

Identification and Authentication

Component	Additional Comments	Response
Is MFA used?	MFA mitigates the chances of a user account being compromised even if the password is guessed/stolen.	
Are usernames set up to uniquely identify the user?	Unique usernames make it clear for audits and logs which user was logged in.	
Is password complexity enforced?	Password complexity settings help ensure passwords cannot be easily guessed or cracked using brute-force methods.	

Systems and Communications Protection

Component	Additional Comments	Response
If the system is not a stand-alone isolated system, does it have a boundary protection device?	Entry and exit points are the pinch point where all access must go through. This includes adversaries from getting in or unauthorized data from getting out.	
Is the system configured per STIG requirements?	Mobile code, domain name server (DNS), session authenticity, and protection on information at risk are elements of system and communication protection that are covered by being STIG compliant.	

Systems and Services Acquisition

Component	Additional Comments	Response
Is there a system development life cycle plan for the system?	Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). A software development life cycle plan makes sure that each of the phases have been considered.	
Are intrusion detection tools actively monitoring for breaches?	Intrusion detection tools are designed to look at the information being generated and quickly determine if a breach has occurred. However, they do not replace having experienced cyber-experts on your team.	

Vulnerability

Consider that vulnerabilities may be located in any layer of the system: hardware, firmware, software, network, and process. Consider also that vulnerabilities may be a flaw in either design or implementation of an individual component or the larger connected system.

Risk Assessment

Component	Additional Comments	Response
Is the system currently utilizing ACAS scanning?	Vulnerability scanning helps ensure that new or previously unknown vulnerabilities are found and fixed.	

Component	Additional Comments	Response
Is the system currently utilizing Security Content Automation Protocol (SCAP) scanning?	Vulnerability scanning helps ensure that new or previously unknown vulnerabilities are found and fixed.	

Security Assessment and Authorization

Component	Additional Comments	Response
Has an independent team validated the security of the system?	Security assessments will be performed to ensure that information security is built into the system; identify weaknesses and deficiencies; provide essential information needed to make risk-based decisions as part of security authorization processes; and ensure compliance to vulnerability mitigation procedures.	

Configuration Management

Component	Additional Comments	Response
Does the system currently follow a configuration management process?	Tracking and approving changes is an important part of risk management as it ensures the system remains in a known state.	
Is the system currently baselined?	To track changes, the current state of the system must be defined and documented.	
Is there the ability to test changes before going live?	If the system is required to stay operational, testing somewhere else prior to implementing changes is recommended.	

Maintenance

Component	Additional Comments	Response
Is there a maintenance plan for the system?	A maintenance plan ensures that all maintenance, diagnostic, and repair activities, whether performed on-site or remotely and whether the equipment is serviced on-site or removed to another location, are managed and monitored to preserve the confidentiality, integrity, and availability (CIA) of the system.	

Media Protection

Component	Additional Comments	Response
Is there any data on the system that must be protected before disposal or maintenance of equipment?	Classified or Official Use Only (OUO) data must be considered any time equipment leaves the system to ensure the data cannot be accessed by an adversary.	

System and Information Integrity

Component	Additional Comments	Response
If the system is GiG-connected, has it implemented HBSS?	HBSS monitors the system and is required if GiG-connected.	
Are there any intrusion detection tools on the system?	Traffic monitoring and prevention is key to knowing if an intrusion has occurred.	

Consequence

Physical and Environmental Protection

Component	Additional Comments	Response
Is there a physical security plan for—or that includes—the system?	A physical security plan helps to prevent unauthorized access to personnel, equipment, installations, information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.	
Is there a plan in place that addresses environmental concerns?	Fire, flood, temperature, and humidity are just some of the things that may affect a system. By addressing potential concerns and how to respond to these issues, the system can be resilient.	

Personnel Security

Component	Additional Comments	Response
Does anyone who have access to the system follow the DoD Personnel Security Program (PSP)?	The PSP has the established policies and procedures to ensure only trustworthy individuals have access to the system.	
Are safety measures in place to protect personnel health and safety if the system is compromised?	Making sure the health and safety of personnel is included and considered in all plans related to system compromise is crucial.	

Configuration Management

Component	Additional Comments	Response
Does the system currently follow a configuration management process?	Tracking and approving changes is an important part of risk management as it ensures the system remains in a known state.	
Is the system currently baselined?	To track changes, the current state of the system must be defined and documented.	
Does the system have the ability to test changes before going live?	If the system is required to stay operational, testing somewhere else prior to implementing changes is recommended.	
Can the system be rolled back to a previous configuration if the live process is compromised?	Backups and the ability to revert back to a previous configuration can help ensure a quick restoration to normal operations.	

Contingency Planning

Component	Additional Comments	Response
Is there a Contingency Plan (CP) in place for the system?	A CP is vital to continuing/restoring the systems operation/functions when the system goes down.	
Does the CP include multiple options depending on the event that occurs?	Tabletop exercises can be used to validate if the CP handles new scenarios.	
Does the CP ensure all critical loads will receive uninterrupted power from a UPS?	Critical loads must stay up for a system to maintain the critical operations.	

Component	Additional Comments	Response
Does the CP ensure all loads will receive uninterrupted power from a UPS?	While not always required as they are not critical, it can reduce risk to have uninterrupted power through a UPS system to all loads. For example, the human machine interface (HMI) may not be required, but using an HMI provides situational awareness.	

Incident Response

Component	Additional Comments	Response
Is there an Incident Response Plan (IRP) in place for the system?	An effective cyber-incident handling capability relies on disciplined processes, procedures, and correctly configured systems.	
Does the IRP designate specific personnel responsible for actions?	Personnel must know who is expected to do which task or that task will likely be missed.	
Does the IRP include specifications for limiting the impact of a cyber-intrusion?	Special considerations are often needed if the incident is a cyber-intrusion.	
Does the IRP include recovery plans for impacts to different parts of the system?	Being able to restore part of the system may be a quicker path to restoring critical operations.	

Appendix C – Recommendations for Cyber-Resilience

The following tables provide recommendations for enhancing cyber-resilience in each of the four risk areas. These recommendations, closely tied to steps evaluated in the RMF (see Appendix B), are broken down by the core functions of resilience, as identified in Section 2.2.1, "Risk Assessments Introduction." This breakdown of recommendations helps organizations identify exactly where in the resilience process there is room for improvement and achieve targeted improvement in a particular risk category. These recommendations are not an exhaustive list, but provide a starting point for closing gaps and following standard best practices for power system cybersecurity.

The following cybersecurity recommendations are based on the Institute of Electrical and Electronics Engineers (IEEE) P1547.3, "Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems." IEEE P1547.3 serves as basis for all DER, and it is recommended that this standard serve as a baseline for cybersecurity practices. However, there are additional considerations or points of emphasis particularly important for resilience upgrades to distributed solar systems discussed here.

Adversary [Intent & Capability]

Identify	Prepare	Detect	Adapt	Recover
Threat classification.	Add protections to systems that interest adversaries.	An IDS monitors for unusual activity.	Updates are made based on active threat bulletins.	Follow reporting requirements to ensure appropriate support is brought in to help with attack attribution and potential legal action against the perpetrator.

Access/Opportunity

Identify	Prepare	Detect	Adapt	Recover
Identify network and physical access points.	Enforce Rule-Based Access Control (RBAC) controls.	Collect and back up network logs.	Isolate infected systems.	Make sure the opportunity being exploited has been blocked.
List personnel that should have access to different tiers in the system.	Implement the principle of least privilege.	Update access lists as personnel gain, lose, or change organizational roles.	Revoke access to compromised accounts.	Run periodic checks for new access points to ensure protection.
Define the roles to be used in RBAC controls.	Ensure that passwords for local access should be different at each site.	Monitor for unusual personnel activity that may signal a compromised account.		

Identify	Prepare	Detect	Adapt	Recover
	Ensure that all hardware default passwords are changed to more secure passwords at commissioning.	Ensure all logs are timestamped.		

Vulnerability

Identify	Prepare	Detect	Adapt	Recover
Participate in information-sharing programs.	Ensure that known vulnerabilities are patched.	Track status of vulnerabilities through SBOM.	Implement workarounds for unpatched systems.	Upgrade and build security by design.
Identify all protocols used in system communications; note custom protocols and ensure they have been securely implemented.	Ensure third-party vendors can and do send out regular patches and updates	Perform periodic pen testing or external review of system architecture.		

Consequence

Identify	Prepare	Detect	Adapt	Recover
Identify critical systems and components.	Ensure that fail-safes and backups are successfully in place.	Ensure that network monitoring software is being used.	Isolate affected systems.	Restore service.
Consider impacts from environmental events (storms, extreme temperature, etc.) in addition to impacts from cyber-events.	Ensure that emergency response plans are in place.	Ensure that cyber-physical sensors are being used.	Maintain backups of control settings so that malicious changes can be undone.	