ANNEX B

NASEO
National Association of
State Energy Officials

National Association of Regulatory Utility Commissioners
Dedicated to Public Service
1889

Photovoltaic Solar Engineering and System Overview

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

Photovoltaic Solar Engineering and System Overview

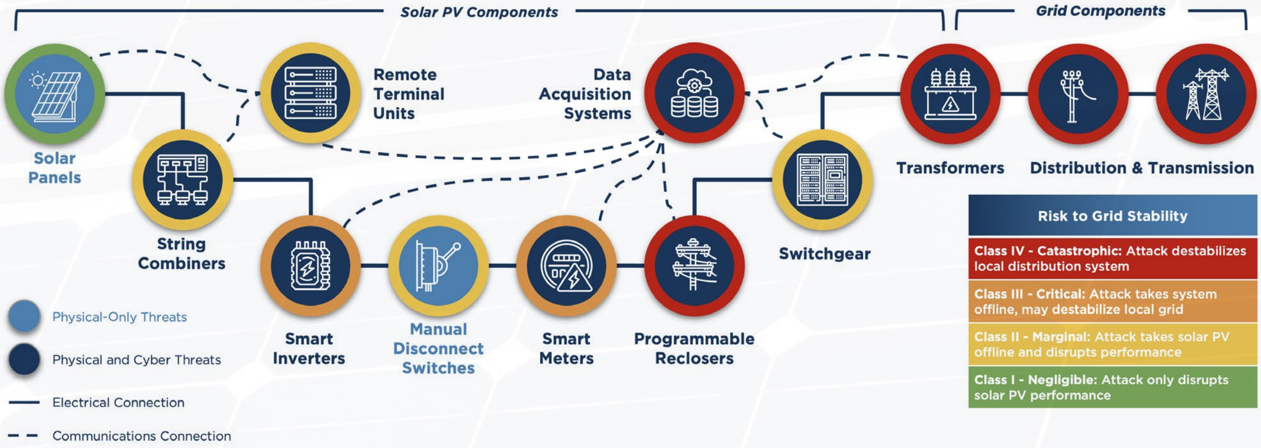
A Cybersecurity Advisory Team for State Solar (CATSS) Tool

Disclaimer:
The CATSS Toolkit is designed to provide states with basic education on cybersecurity issues for solar and enable their efforts to support cybersecurity enhancements efforts for solar. Cybersecurity challenges for solar should not be viewed as unique. All electricity generation technologies are, to varying degrees of potential severity and vulnerability, susceptible to cyberattacks and disruption. As interconnected electricity generation technologies, solar systems—and DERs generally—have a unique advantage to ensure that cybersecurity is incorporated by-design and prior to deployment, rather than applied ex post facto. The recommendations provided within the CATSS Toolkit/this tool were developed to meet the expressed needs of State Energy Offices and Public Utility Commissions during the project, and their respective purviews, priorities, and directives to support cyber-secure solar deployment in their states. While many industry and federal partners were included in the CATSS Advisory Group, it must be noted that neither the states' nor other stakeholders' perspectives collected are exhaustive. The Toolkit represents a snapshot of a quickly evolving and complex area, and should not be treated as a definitive guide, but rather a basis for continued discussion and adaptation of public-private partnerships for solar cybersecurity.

This material is based upon work supported by the U.S. Department of Energy (DOE) under award number DE-EE0009004. This report was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or any agency thereof.

Simplified Schematic of Grid-Scale Solar PV Components

This simplified schematic depicts local solar PV components, interdependencies with the grid, and local two-way communication pathways. It identifies physical and virtual risks, and delineates between solar PV and grid scale components. There may be additional components, communication pathways, connections, risks, and vulnerabilities not depicted for illustrative simplicity.



Risk to Grid Stability
Class IV - Catastrophic: Attack destabilizes local distribution system
Class III - Critical: Attack takes system offline, may destabilize local grid
Class II - Marginal: Attack takes solar PV offline and disrupts performance
Class I - Negligible: Attack only disrupts solar PV performance

Data Acquisition Systems (DAS)

Owner: Project Developer in Non-vertically Integrated Market, Utility Provider in Vertically Integrated Market

Background: Data acquisition systems (DAS) are a critical component of any distributed generation (DG) system. Various sensors and controls are installed in the equipment listed below that collect data that is aggregated by the DAS system and delivered wirelessly to a remote server. The owner of the DG system and their operations and management partners can log into a website or smartphone app to see the data collected on the solar PV in real time, and remotely control certain solar PV components. The DAS can be accessed through a local area network (i.e., private intranet) or a wide area network (i.e., public internet).

Vulnerability: This internet interface presents a level of risk for a cyberattack that could potentially alter system data or disable the flow of data, removing visibility and control of the DG system.

Risk to Grid Stability - Class IV - Catastrophic: DAS systems will generally monitor and provide controls over transformers, switchgear, inverters, and string combiners. A cyber attack on the DAS has the potential to take the solar PV offline and impact the stability of the local distribution system.

Remote Terminal Units (RTU)

Owner: Project Developer in Non-vertically Integrated Market, Utility Provider in Vertically Integrated Market.

Background: A small computer located in a weatherproof box near the solar PV, that collects data such as how much electricity it is generating, and aggregates that data for delivery over a wired or wireless data link to a central authority like the local electric utility or the regional transmission organization.

Vulnerability: Similar to the recloser, the data connection for remote terminal units (RTUs) makes it potentially vulnerable to a cyberattack that could alter or halt the flow of data, thereby hindering the local electric utility or regional transmission operator from having visibility of the electricity in their systems.

Risk to Grid Stability - Class II - Marginal: This can disrupt the performance of the solar PV, but there are multiple protections upstream that can protect the local electricity system from instability.

Solar Panels

Owner: Project Developer in Non-vertically Integrated Market, Utility Provider in Vertically Integrated Market

Background: All solar projects include solar panels that produce direct current (DC) electricity from sunlight. Each individual panel needs to be combined with several other panels to provide enough power to meet the local load in the area or to supply energy to the electric grid. Typical projects are comprised of hundreds of panels and a failure on one or more panels only reduces the electrical output of the project by the panels rating. For example, having ten 250 watt solar panels fail would decrease the solar PV output by 2.5 kilowatts. This functionality allows for the vast majority of a project to produce electricity, even whether there is damage or issues with some of the panels.

Vulnerability: Solar panels are not a target for hackers since they do not have any remote control capabilities and only produce power at the point of use.

Risk to Grid Stability - Class I - Negligible: A physical attack on the solar panels would only impact the performance of the damaged solar panels and the rest of the solar PV would remain functional.

String Combiners

Owner: Project Developer in Non-vertically Integrated Market, Utility Provider in Vertically Integrated Market

Background: Grid-scale solar PV are made up of many rows of individual solar panels. Solar PV requires visibility over each of those individual panels and a level of control over their output to the larger system. String combiners control individual rows or "strings" of the panels and measure the electrical current, voltage and temperature of that string of panels and provide protections against electrical surges and overcurrents from that string that could damage the rest of the solar PV. String combiners also have a disconnect ability that allows remotely disconnecting a particular string from the rest of the system if that string is malfunctioning.

Vulnerability: Since these combiners are networked back to the DAS system, they are potentially vulnerable to a cyberattack.

Risk to Grid Stability - Class II - Marginal: A cyber attack on the string combiners through the DAS would most likely only impact the performance of the solar PV so the risk level will be defined by the size of the asset (the loss of a large array on a day it is expected to produce a large output is impactful).

Smart Inverters

Owner: Project Developer in Non-vertically Integrated Market, Utility Provider in Vertically Integrated Market

Background: The job of the inverter is to “invert” direct current (DC) electricity to alternating current (AC) electricity so that it can be used by homes and businesses. Electricity in homes and businesses is all AC electricity provided by the local distribution electric lines. Solar panels generate DC electricity from the sun, and batteries store DC electricity. Before electricity can be delivered from a DG system to the local electric distribution lines for delivery and use in homes and businesses, the DC electricity must be inverted to AC electricity. In addition to inverting the electricity from DC to AC, smart inverters monitor the local distribution electric system for voltage or frequency instability or faults and can open a circuit (e.g., shut off the flow of electricity,) if it senses those issues. Smart inverters also contain the same programmed abnormal voltage and frequency values as the switchgear and should be the first circuits to open in the instance of those abnormal values.

Vulnerability: Smart inverters are connected to the DAS system and are therefore potentially vulnerable to a cyberattack through the DAS. These inverters can be attacked directly through their wireless communication protocols, providing two distinct cyberattack vectors. It is also possible to physically attack the inverters.

Risk to Grid Stability - Class III - Critical: A cyber attack on the inverters through the DAS would most likely only impact the performance of the solar PV and potentially damage the inverters before the switchgear disables the system to protect other equipment.

Manual Disconnect Switches

Owner: Project Developer in Non-vertically Integrated Market, Utility Provider in Vertically Integrated Market

Background: Most solar PV include a manual disconnect switch for disconnecting the system from the grid for maintenance or emergency scenarios. This switch can act as a fail safe system in case the automated, programmable, and remotely connected equipment malfunctions. The disconnect switch can be activated manually with limited knowledge of power system operations to remove the DG asset from the grid. These switches are typically located next to the DG systems, but they can be in remote locations with limited physical security.

Vulnerability: Manual disconnect switches are not a target for hackers since it requires manual operation at the point of use.

Risk to Grid Stability - Class II - Marginal: A physical attack on the manual disconnect switch would most likely only impact the performance of the solar PV.

Smart Meters

Owner: Project Developer or Utility Provider in Non-vertically Integrated Market, Utility Provider in Vertically Integrated Market

Background: An electrical meter records the amount of power (kilowatts) and energy (kilowatt-hours) produced by the solar PV and provides the information necessary for utilities, project developers, and customers to buy and sell the energy. Standard meters need to be manually read at regular intervals in close proximity to the meter in order to conduct those financial transactions. Smart meters record additional types of electrical information in near real-time and uses cellular or wireless networks to communicate information from the meter to a central hub and send control signals from a central hub to the meter. This increased functionality changes the operation of the meter from a "read-only" device to a device more akin to a programmable recloser.

Vulnerability: Smart meters, like other equipment installed by the project developer, are connected to the DAS system and are therefore potentially vulnerable to a cyberattack. These meters can also be attacked directly through their wireless communication protocols, providing two distinct attack vectors. It is also possible to physically attack the smart meters.

Risk to Grid Stability - Class III - Critical: A cyber attack on smart meters either directly or through the DAS would most likely only impact the performance of the solar PV before the switchgear disables the system to protect other equipment.

Programmable Reclosers

Owner: Project Developer or Utility Provider in Non-vertically Integrated Market, Utility Provider in Vertically Integrated Market

Background: A circuit, like a light switch, that is both automated and remotely controlled by the utility using a wireless or wired data signal. If the recloser senses a "fault" on the local electric lines (e.g., a branch falling on the wires, a utility pole knocked down by weather or a vehicular accident) the recloser opens the circuit, cutting the flow of power equivalent to turning a light switch off.

Vulnerability: The network connected computer that controls the recloser can be vulnerable to a cyberattack since hackers can connect to it from anywhere in the world if they bypass network security measures.

Risk to Grid Stability - Class IV - Catastrophic: These systems are the main connection point for the DG system to the grid and there are only a few manufacturers and models available for use at distribution voltages. Programmable reclosers are at high risk to cyberattacks.

Switchgear

Owner: Project Developer in Non-vertically Integrated Market, Utility Provider in Vertically Integrated Market

Background: Two critical components of electricity are its voltage and frequency. Voltage is the pressure of the electricity being pushed through the wires. Frequency is specific to alternating current (AC) electricity, which travels like waves and the frequency is the distance between those waves. In the United States, the standard frequency of AC electricity is 60 Hertz. The switchgear monitors and controls the voltage and frequency of the electricity being sent to the local distribution system. Devices in the switchgear called "relays" are circuits that are programmed to open (shut off power) in a certain time frame when the voltage or frequency stray from their normal range (abnormal voltage or frequency ranges). The further the voltage or frequency strays from normal, the faster these relay circuits open, down to 0.16 seconds. The switchgear ensures that the DG system gets shut off before the abnormal voltage or frequency can cause instability on the local distribution system.

Vulnerability: Because the switchgear is connected to the DAS system, it can potentially be vulnerable to a cyberattack.

Risk to Grid Stability - Level II - Marginal: A cyber attack on the switchgear through the DAS would most likely only impact the performance of the solar PV and inhibit its safety mechanisms, but it could create an instability in the local distribution system.

Transformers

Owner: Project Developer and Utility Provider in Non-vertically Integrated Market, Utility Provider in Vertically Integrated Market

Background: A transformer is the first piece of equipment between the local electric distribution system and the DG system. The transformer transforms the voltage of the electricity from the DG system's lower voltage (usually ~500 - 1000 volts) up to the voltage of the local distribution system (usually ~15,000 volts or 15 "kilovolts").

Vulnerability: While the transformer itself is not typically directly connected to a network or accessible, it can be controlled through the connection to the DAS, if a vulnerability on the DAS is successfully exploited.

Risk to Grid Stability - Class IV - Catastrophic: A cyber attack on a transformer through the DAS would create dangerous instability on the local distribution system.

Distribution and Transmission Systems

Owner: Utility Provider in Non-vertically Integrated Market or Vertically Integrated Market

Background: The distribution and transmission system connects the solar PV transformer to the bulk electric system and allows for the energy produced to be used by customers and loads in the region. The voltage on the systems will range from tens of kilovolts on the distribution system to hundreds of kilovolts on the transmission system. Each of these systems are built using national standards and while the configuration may differ across the country, the components and operating principles are the same. The distribution and transmission systems are controlled remotely in many parts of the nation due to the immense distance covered by each system.

Vulnerability: Distribution and transmissions systems are very complex with multiple points of control with many different entities responsibility for its operation, making it a large target for cyber attackers and difficult to defend.

Risk to Grid Stability - Class IV - Catastrophic: A cyber attack on the distribution or transmission system has the potential of creating dangerous instability on the bulk electric system that could result in blackouts.