

# Seeing the Unseen: An Evaluation of Active Scanning in ICS Environments

Jennifer Guerra  
DEFCON ICS Village  
August 10, 2024

## Our Purpose

Advance cyber innovation to defend modern, renewable energy technologies against high-priority cybersecurity risks to the energy sector.

### Track 1

Address utilities' most urgent security interests by assessing market-ready cybersecurity solutions in a representative testing architecture.

### Track 2

Help developers improve pre-market cybersecurity technologies and bridge the “valley of death” between innovation and commercialization.

# Track 1 Cohorts

## Cohort 1

### **Strong Authentication and Authorization**

*Status: Complete*

Tested three solution providers to address risks related to authentication and authorization within distributed energy resource (DER) environments.

Evaluated capabilities such as user management of field devices, interconnection of DER systems, and authentication and authorization of commands.

## Cohort 2

### **Hidden risks due to incomplete system visibility, device security, and configuration**

*Status: In Progress*

Evaluating two solution providers that actively identify all industrial control system (ICS) assets connected to a utility's infrastructure—physically and virtually—to understand the totality of assets that need to be monitored and protected within the environment.

Selected solutions support the identification of unauthorized, unmanaged, or compromised assets to be removed or remediated.

# Key Takeaways from Cohort 1

## Move Beyond Perimeter Security



Heavy focus on perimeter: insufficient security approach for modern hyper-connected systems.

Internal defensive devices: provide higher visibility, improve understanding of network topology, and effective placement of security assets.



## Enable Multifactor Authentication

This best practice can defend against an attacker's lateral movements through a compromised network.



## Invest in Defense-in-Depth Security

Signature-based detections alone will fail to defend networks. No single solution can protect against all threat scenarios.



## Living-off-the-Land Techniques Difficult to Defend

Attackers abusing native protocols and legitimate device relationships are difficult to detect and stop.



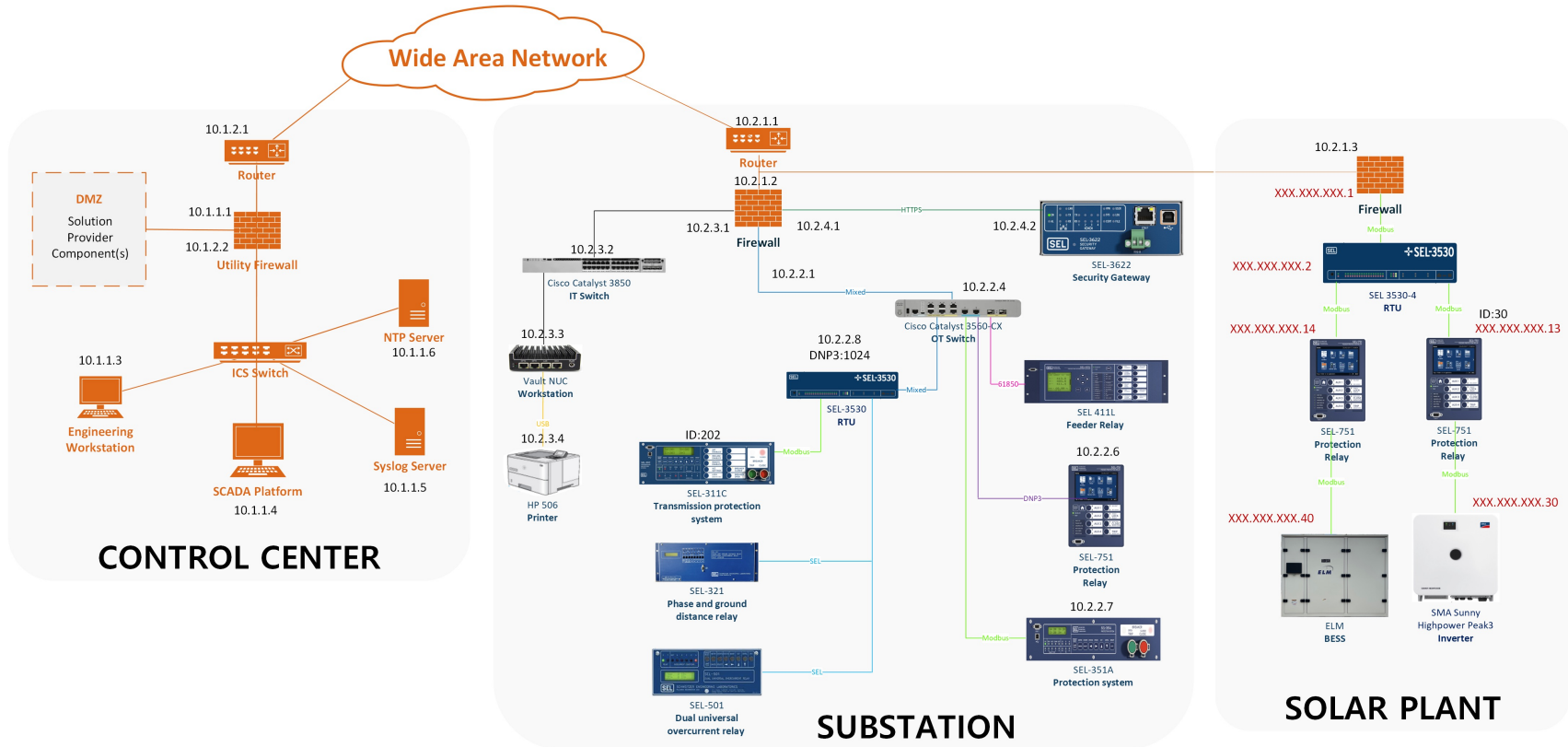


# Cohort 2 Theme





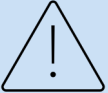


Hidden risks due to incomplete system visibility, device security, and configuration.

# Cohort 2 Baseline Operation Environment



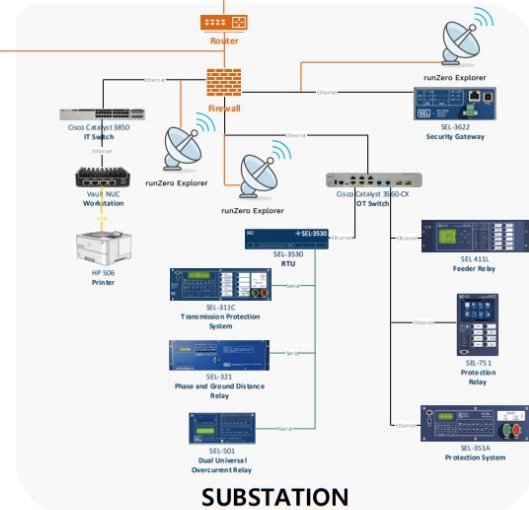
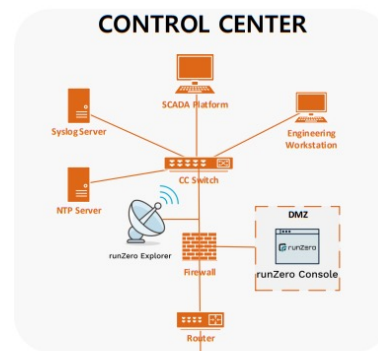
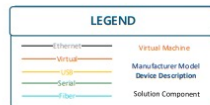
# Cohort 2 Evaluation Topics

Evaluation Topic			Description
1	<b>Initial Discovery</b>		How does the solution perform during initial scan of environment?
2	<b>Change Discovery</b>		How does the solution identify changes to the environment?
3	<b>Passive Discovery</b>		What can the solution identify passively?
4	<b>Scale Discovery</b>		How does the solution perform at scale?
-	<b>Interruption to Operations</b>		Does the solution affect the normal operation of devices?

## Scenario 1: Initial Discovery

- Deployed as self-hosted, on-premise, and air-gapped
- runZero Console on DMZ in control center
- Explorers on virtual machines hosted behind the firewall in each subnet of interest

**CECA** CLEAN ENERGY  
CYBERSECURITY  
ACCELERATOR  
OPERATING ENVIRONMENT  
COHORT 2



runZero version: 20240301



## Scenario 1:

### Results

- Identified any services available, and ports open for probes enabled in the scan
- Identified Transmission Control Protocol port 20,000 as open on the operational technology (OT) devices communicating via a Distributed Network Protocol 3 (DNP3) but did not identify a DNP3 service.

Device	Hostname	IP Address	MAC Address	MAC Vendor	OS	OS Version
Substation OT (11 devices)						
Sub firewall	✓	✓	✓	✓	✓	✓
OT switch	✓	✓	✓	✓	✓	✓
Sub-ot admin vm	✓	✓	✓	✓	✓	✓
Sub-ot runZero vm	✓	✓	✓	✓	✓	✓
SEL 3530 RTAC	✓	✓	✓	✓	✓	
SEL 411L		✓	✓	✓		
SEL 751		✓	✓	✓		
SEL 351A		✓	✓	✓		
*SEL 311C						
*SEL 321						
*SEL 501						
Substation OT gateway (3 devices)						
Sub-ot-gateway admin vm	✓	✓	✓	✓	✓	✓
Sub-ot-gateway runZero vm	✓	✓	✓	✓	✓	✓
SEL 3622	✓	✓	✓	✓	✓	
PV plant (8 devices)						
PV firewall	✓	✓	✓	✓	✓	✓
PV admin vm	✓	✓	✓	✓	✓	✓
PV runZero vm	✓	✓	✓	✓	✓	✓
SEL 3530 RTAC	✓	✓	✓	✓	✓	
SEL 751		✓	✓	✓		
SEL 751		✓	✓	✓		
SMA Sunny Highpower	✓	✓	✓	✓	✓	
ELM BESS	✓	✓	✓	✓	✓	✓

# Scenario 1: Results

- Port 502
- Modbus protocol
- Vendor

Services	
XXX.XXX.XXX.40 —	
- 0/arp	
- 135/tcp	
- 445/tcp	
- 502/tcp	
- 3389/tcp	
- 5040/tcp	
- 8080/tcp	
Back to top ⓘ	
XXX.XXX.XXX.40 7 services	
XXX.XXX.XXX.40 - 502/tcp	
hw.certainty	0.25
hw.product	MicroGrid Site Controller
hw.vendor	ELMFieldSight LLC
hw.version	1.0.8.40
ip.flags	DF
ip.id	21268
ip.mtu	1500
ip.tos	0
ip.ttl	128
modbus.productCode	MicroGrid
modbus.productName	MicroGrid Site Controller
modbus.revision	1.0.8.40
modbus.vendor	ELMFieldSight LLC
modbus.vendorURL	http://www.fieldsight.com/
protocol	modbus
source	syn
tcp.flags	syn,ack
tcp.mss	1460
tcp.options	MSS:05b4 · WindowScale:08
tcp.optionsLen	1
tcp.urg	0
tcp.win	65535
tcp.winScale	8
ts	Mar 21 2024 1:59PM [UTC -6] (Thu)

## Scenario 1:

### Results

- Port 20,000 – identified as open on OT devices communicating via DNP3
- Did not identify a DNP3 service.

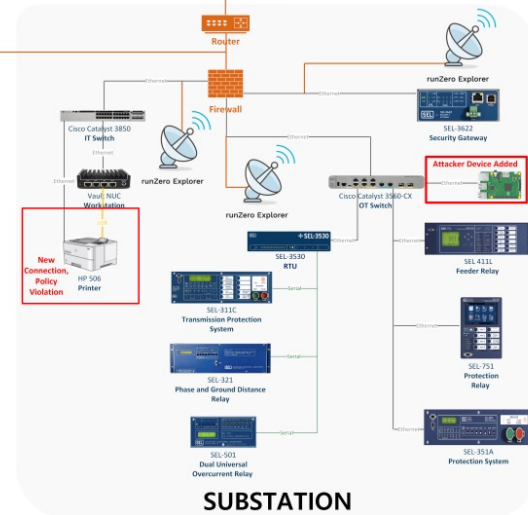
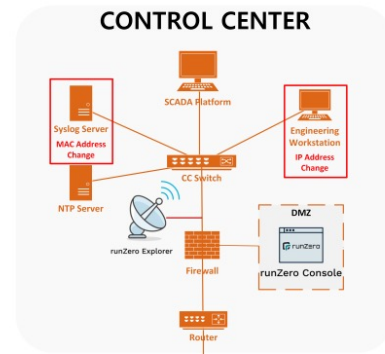
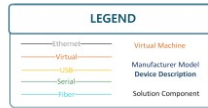
Services	
10.2.2.6 5 —	
0/arp	
21/tcp	
23/tcp	
80/tcp	
20000/tcp	
Back to top ↑	
10.2.2.6 – 5 services	
🔗 10.2.2.6 – 20000/tcp	
🔍 ip.flags	📄 🔍 DF
🔍 ip.id	📄 🔍 37890
🔍 ip.mtu	📄 🔍 1500
🔍 ip.tos	📄 🔍 0
🔍 ip.ttl	📄 🔍 64
🔍 source	📄 🔍 syn
🔍 syn.rtt	📄 🔍 2386987
🔍 tcp.flags	📄 🔍 syn,ack
🔍 tcp.mss	📄 🔍 1460
🔍 tcp.mssMultiplier	📄 🔍 6
🔍 tcp.options	📄 🔍 MSS:05b4 · WindowScale:00
🔍 tcp.optionsLen	📄 🔍 12
🔍 tcp.ts	📄 🔍 1285599780
🔍 tcp.urg	📄 🔍 0
🔍 tcp.win	📄 🔍 8688
🔍 tcp.winScale	📄 🔍 0
🔍 ts	📄 🔍 Mar 21 2024 1:59PM [UTC-6] (Thu)

## Scenario 2: Change Discovery

- Connected a Raspberry Pi running Kali Linux OS in the substation OT subnet
- Plugged the printer into the switch via ethernet
- Changed IP address of the engineering workstation in the control center
- Changed MAC address of the syslog server in the control center



OPERATING ENVIRONMENT  
COHORT 2 - SCENARIO 2



## Scenario 2: Results

- Identified each of the four changes introduced into the environment. Profiled just as in-depth as other devices.
- Changed IP address tracked; updated device entry for the engineering workstation with the new IP
- With the changed MAC address for the syslog server, runZero platform created new device entry in the inventory database, and marked the "old" syslog server as "offline"

Console > Alerts

Alerts					Acknowledge All	Clear
Date	Type	Organization	Message	Acknowledged		
Mar 22 2024 6:10PM [UTC+0] (Fri)	Alert	Headquarters	New Asset - An asset not previously identified has been found.	<button>Acknowledge</button>		
Mar 22 2024 6:10PM [UTC+0] (Fri)	Alert	Headquarters	New Asset - An asset not previously identified has been found.	<button>Acknowledge</button>		
Mar 22 2024 6:10PM [UTC+0] (Fri)	Alert	Headquarters	New Asset - An asset not previously identified has been found.	<button>Acknowledge</button>		

Console > Inventory > Assets

Asset inventory

Scan

Import

Integrate

Export

address:10.1.1.5

Search

Query builder

...

Select

Scan

Modify

Delete

Cols

Prefs

0 selected

Viewing 2 results

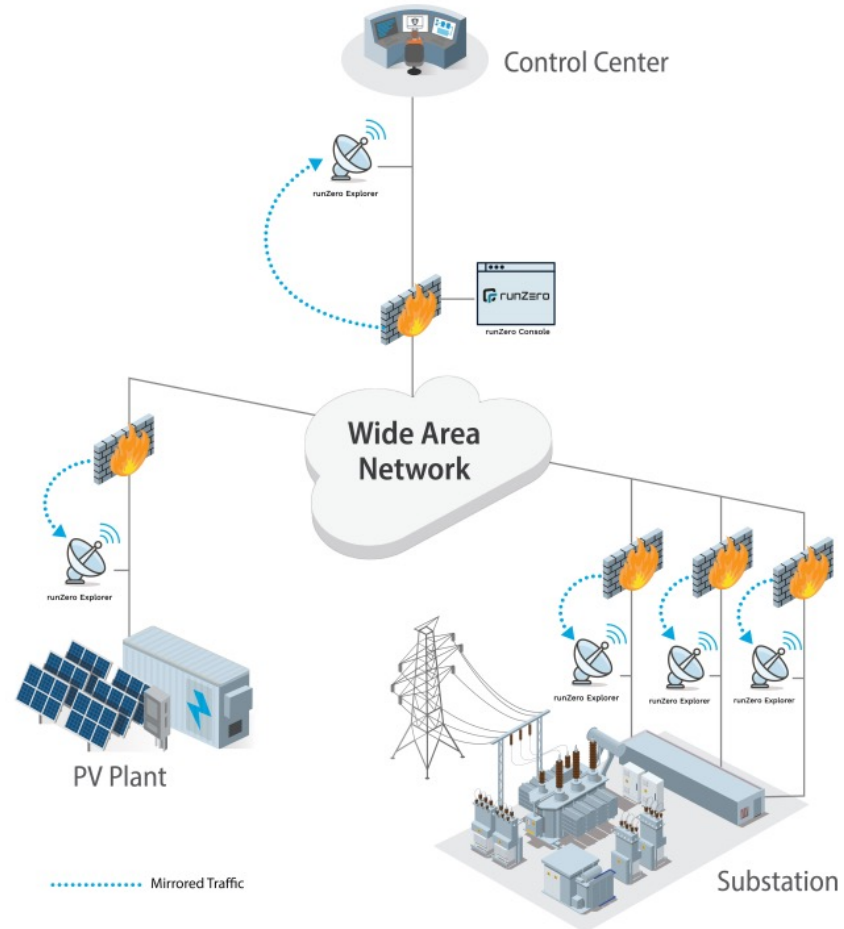
20 results

ID	Up	Addresses	Hostname	Type	MAC	MAC vendor	OS
<input type="checkbox"/> 5e95af0a-1b9c-495...	<div></div>	10.1.1.5+1		<div>Server</div>	10:CS:95:01:04:01	Lenovo	<div>Ubuntu Linux 20.04</div>
<input type="checkbox"/> 6aa1f9b4-4837-487...	<div></div>	10.1.1.5+1		<div>Server</div>	10:CS:95:FF:04:FF	Lenovo	<div>Ubuntu Linux 20.04</div>



## Scenario 3: Passive Discovery

- Traffic collection point sampling via a mirror port on firewall interface
- Each Explorer configured to listen to any broadcast traffic on its subnet



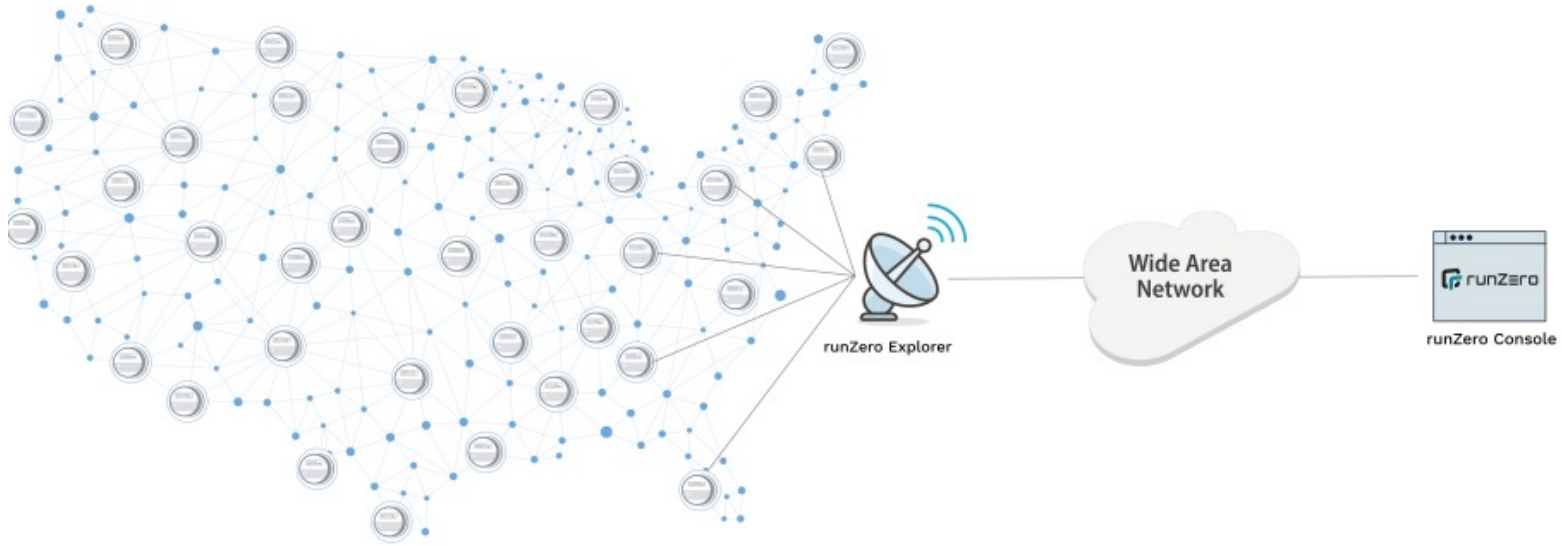
## Scenario 3:

### Results

- Unable to identify quiet assets as expected with passive detection
- Unable to identify network infrastructure
- Only able to identify signatures that traverse the sampling point

Device	Hostname	IP Address	MAC Address	MAC Vendor	OS	OS Version
Substation OT (11 devices)						
Sub firewall		✓	✓	✓		
*OT switch						
Sub-ot admin vm	✓	✓	✓	✓		
Sub-ot runZero vm	✓	✓	✓	✓		
SEL 3530 RTAC		✓	✓	✓		
*†SEL 411L						
SEL 751		✓	✓	✓		
SEL 351A		✓	✓	✓		
*SEL 311C						
*SEL 321						
*SEL 501						
Substation OT gateway (3 devices)						
Sub-ot-gateway admin vm	✓	✓	✓	✓		
Sub-ot-gateway runZero vm	✓	✓	✓	✓		
†SEL 3622						
PV plant (8 devices)						
PV firewall		✓	✓	✓		
†PV admin vm	✓	✓	✓	✓		
PV runZero vm	✓	✓	✓	✓		
SEL 3530 RTAC		✓	✓	✓		
SEL 751						
SEL 751		✓	✓	✓		
SMA Sunny Highpower	✓	✓	✓	✓		
ELM BESS		✓	✓	✓		

# Scenario 4: Scale Discovery



The scale environment size represents the number of customers that could be served by a larger substation featuring 3,948 Advanced Metering Infrastructure (AMI) devices on a single flat network within the subnet (10.200.0.0/20).

# Scenario 4: Results

- Average time for scans approximately 2 hours, 15 minutes
  - Increasing scan rate settings could have led to faster scan times
- Average network traffic amounted to approximately 170 kB for each device
  - Traffic would change based on probes enabled in the scan profile
- Platform accurately generated an alert when it identified an added device
  - Alerts are highly configurable

## Alerts

Acknowledge All

Clear

Date	Type	Organization	Message	Acknowledged
Mar 11 2024 4:19AM [UTC+0] (Mon)	Alert	Headquarters	New Asset: A new asset not previously identified has been found on the network.	<p>Acknowledge</p>

# Interruption to Operations

- Monitoring throughout testing
  - Verified the Supervisory Control and Data Acquisition (SCADA) Platform for ability to poll downstream devices
  - Internet Control Message Protocol (ICMP) polling apparatus to detect any unresponsive hosts
  - Network captures to track communications and solution traffic
- runZero results
  - Active scanning methods did not measurably affect the deployed ICS assets nor ongoing SCADA process and communications

*Note: CECA conclusions cannot be assumed to be generalizable, as the sample of devices and protocols was limited by the time and availability to perform tests*



# Key Takeaways from Cohort 2 (ongoing)

## RunZero

- Tested for its ability to discover detailed information about all **IP-addressable** devices in the environment
- Solution collected **detailed** information about devices, including **all open ports** and some OT protocols like Modbus
- Active scanning methods showed **no impact** on ICS assets' performance nor ongoing SCADA processes and communications

## Asimily

- Currently undergoing testing
- Public report due out later in 2024



A satellite view of Earth at night, showing the curvature of the planet and the glowing lights of cities and continents. The sun is visible on the left horizon, creating a bright glow and lens flare effect.

# Thank You

[www.nrel.gov](http://www.nrel.gov)

NREL/PR-5T00-90761

This work was authored by the National Renewable Energy Laboratory (NREL), operated by Alliance for Sustainable Energy LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. The views expressed in the article do not necessarily represent the views of DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

*Photo from iStock-627281636*

