INL/MIS-22-66611-Revision-0

Distributed Renewables Cyber Resilience

April 2022

Changing the World's Energy Future

Craig G Rieger, Jake P Gentle, Andrew A Bochman, Jeremiah Miller

Idaho National Laboratory

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

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed 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. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-22-66611-Revision-0

Distributed Renewables Cyber Resilience

Craig G Rieger, Jake P Gentle, Andrew A Bochman, Jeremiah Miller

April 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Distributed Renewables Cyber Resilience

Craig Rieger, Jake Gentle and Andy Bochman
Idaho National Laboratory

Jeremiah Miller
Solar Energies Industry Association

The benefits of renewable energy continue to grow, with wind generation supplying 9.2% generation in the United States (US)[1] but 22.6% in other western countries like Germany[2]. Solar is at 2.8% in the US[3,4] and near 10% in Germany[5]. Through diversification and greater distribution system integration, the application of renewable energy promises greater power system resilience from threats that include damaging storms and cyber-attack[6,7]. The ability for communities to meet critical load demand, distribution can lift the resilience burden on transmission systems and large-scale generation suppliers to fulfill these needs. Diversification of generation assets can reduce the impact from individual threats, as disruptions from compromise are likely smaller in scale and less likely to affect all assets, specifically from cyber-attack. Looking to the future and potential impacts of climate change, distribution and diversification provide practical pathways for resilience and impact reduction.

However, the control systems necessary to integrate the distribution and diversification required to maintain power system stability expand the attack surface via more communications interfaces.[8] As a result, the resilience to cyber-attack must be elevated to levels proportional to increasing threat levels in order to give owners and operators the reliability their mission demands. Advancing a reference architecture[9] that enables secure design across all generation types, large and small scale, is critical to the future of distributed power system resilience.

A Reference Architecture for Orchestrated Response

The application of secure technologies and applications will underpin next generation resilient designs for energy applications, informed by R&D and applied by industry. To inform a reference architecture design and R&D gaps for the renewables industry, a survey was conducted to evaluate the current state of the industry. The survey was sent to:

- Cybersecurity vendors
- Original Equipment Manufacturers (OEMs) in solar energy, wind energy, electric vehicles (EVs)

A security architecture includes several elements:

- Detect: Monitoring of network traffic to recognize undesirable traffic
- Analyze: Methods, including machine learning, to baseline normal traffic and recognize abnormal

[1] https://www.eia.gov/tools/faqs/faq.php?id=427&t=3.
[2] https://www.windpowermonthly.com/article/1737041/wind-generated-electricity-germany-slumps-new-low-2021.
[3] Utility scale only
[4] https://www.eia.gov/tools/faqs/faq.php?id=427&t=3.
[5] https://www.solarfeeds.com/mag/solar-power-statistics-in-germany-2021/.
[6] https://thehill.com/opinion/energy-environment/591233-the-electrical-grid-of-the-future-must-be-built-around-community.
[7] https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6900108.
[8] https://standards.ieee.org/ieee/1547/5915/
[9] Others have been proposed. e.g. https://sunspec.org/wp-content/uploads/2020/01/EPRI-Security-Architecture-for-the-Distributed-Energy-Resources-Integration-Network.pdf

- Decide/Visualize: Presentation of information to cyber defenders for quick recognition and response
- Mitigate/Recover: Methods to stop a cyber-attack and reverse any negative affects
- Share: Providing of indicators of cyber-attack that can be securely shared and benefit the defenses of other organizations

These security architecture element's functions[10] are provided through the following security tools (Figure 1), noting that many of the tools provide multiple functions:

- Detect, Analyze: Host/Network Intrusion Detection Systems (HIDS/NIDS)
- Decide/Visualize: Security Information and Event Management (SIEM)
- Mitigate/Recover: Security Orchestration, Automation and Response (SOAR)
- Share: Structured Threat Information eXpression (STIX), Trusted Automated eXchange of Intelligence Information (TAXII)

Those surveyed were asked about their integration of said tools, and additionally, traditional access controls and encryption provided-perimeter defenses.

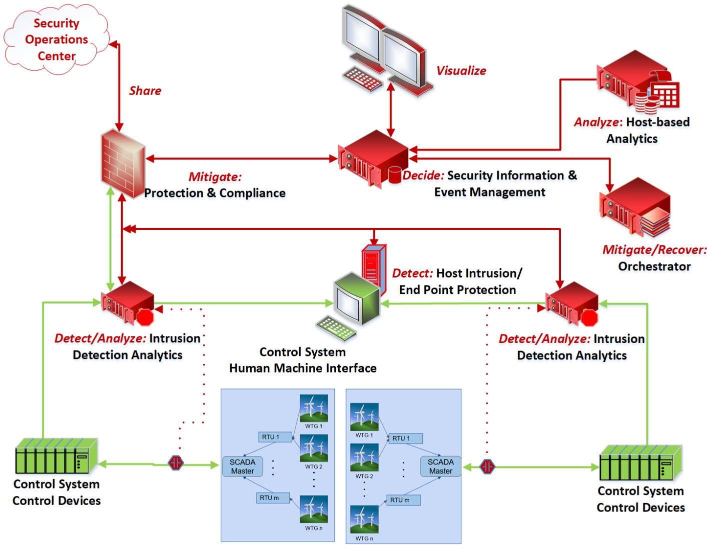

Security Operations Center
Share
Visualize
Analyze: Host-based Analytics
Mitigate: Protection & Compliance
Decide: Security Information & Event Management
Mitigate/Recover: Orchestrator
Detect: Host Intrusion/ End Point Protection
Detect/Analyze: Intrusion Detection Analytics
Control System Human Machine Interface
Detect/Analyze: Intrusion Detection Analytics
Control System Control Devices
RTU 1
SCADA Master
RTU m
WTG 1
WTG 2
WTG n
WTG 1
WTG 2
WTG n
RTU 1
SCADA Master
RTU m
Control System Control Devices

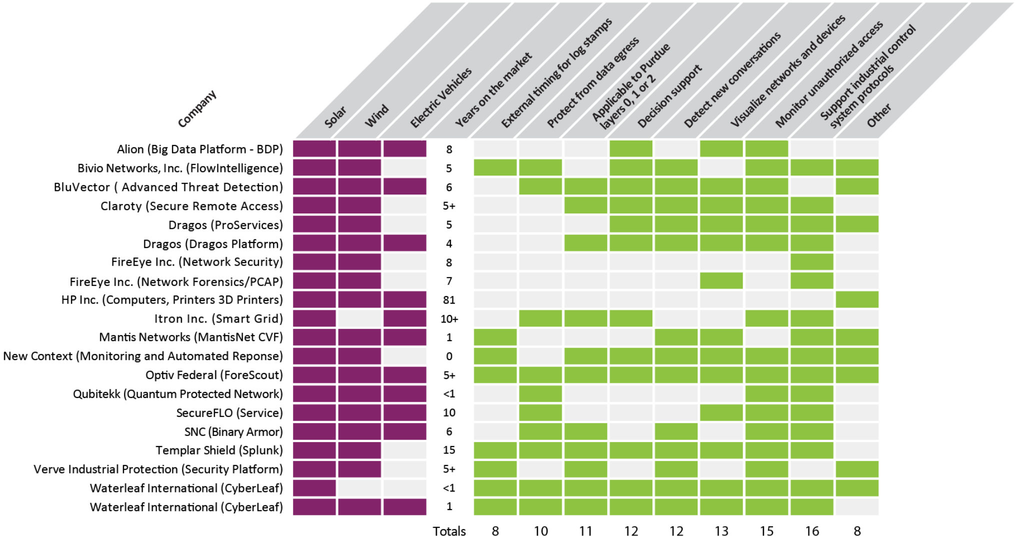
Figure 1. Reference Architecture

The survey garnered insightful perspectives from both cybersecurity vendors and OEMs on the technologies listed. The full results can be found here. As an example of the results analysis, Figure 2 provides a summary example for NIDS from cybersecurity vendors. Each table provides the company, product, renewables domains impacted, and common capabilities of each product. In addition, for each capability (using categories provided), it also shows how many respondents indicated the same capability support.

Many cybersecurity vendors responded to the survey, but only a limited number of OEM renewables vendors chose to (Figure 3). Evident from the cybersecurity vendors is the belief that their products may provide benefits in this domain. Less evident is a similar level of engagement on and enthusiasm for cybersecurity from the renewables industry OEMs. Clearly, more discussion on cybersecurity reference architectures is warranted, with more substantial industry

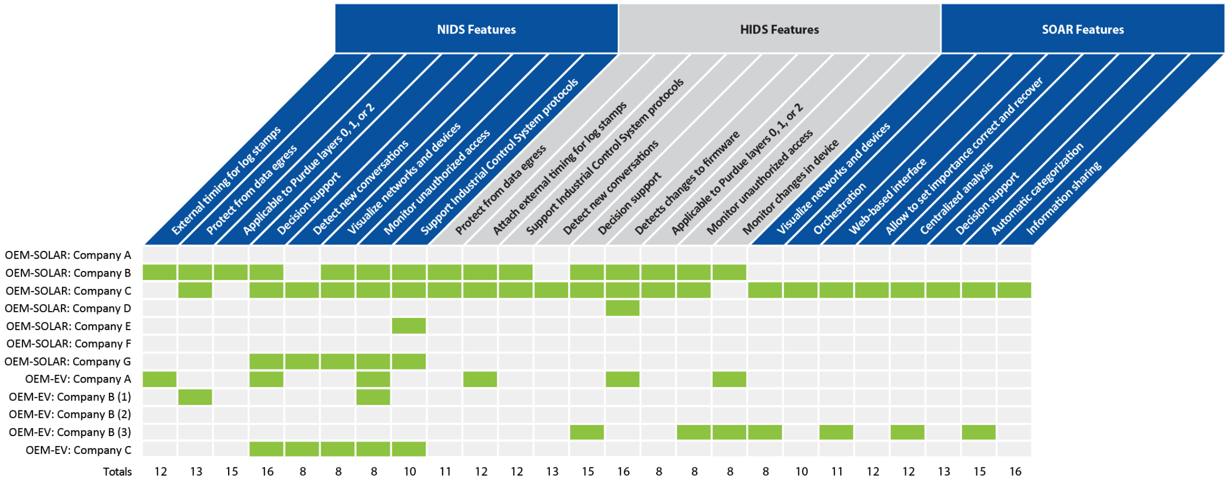
[10] Please note the proposed architecture is structurally agnostic and likely to be implemented in a hybrid manner. Energy resource data flow is no longer strictly hierarchical, thus functional security is essential regardless of alignment to traditional data hierarchies.

participation. Specifically, a greater understanding of the tools, benefits, and costs of investment would be helpful. While large asset owners have integrated security, further discussion/evaluation is needed on the security of distributed renewables to ensure high levels protection and resilience as designed in. The resulting discussion should illuminate the need for decision making tools that align benefits with investments. To achieve and maintain a common threat posture between large scale utilities and renewables, integration of security capabilities that aggregate seamlessly is necessary.



Company	Solar	Wind	Electric Vehicles	Years on the market	External timing for log stamps	Protect from data egress	Applicable to Purdue layers 0, 1 or 2	Decision support	Detect new conversations	Visualize networks and devices	Monitor unauthorized access	Support industrial control system protocols	Other
Alion (Big Data Platform - BDP)	🟪	🟪	🟪	8				🟩		🟩	🟩		
Bivio Networks, Inc. (FlowIntelligence)	🟪	🟪		5	🟩	🟩		🟩	🟩		🟩	🟩	🟩
BluVector (Advanced Threat Detection)	🟪	🟪	🟪	6		🟩	🟩	🟩	🟩	🟩	🟩		🟩
Claroty (Secure Remote Access)	🟪	🟪		5+			🟩	🟩	🟩	🟩	🟩	🟩	
Dragos (ProServices)	🟪	🟪		5				🟩	🟩	🟩	🟩	🟩	🟩
Dragos (Dragos Platform)	🟪	🟪	🟪	4			🟩	🟩	🟩	🟩	🟩	🟩	
FireEye Inc. (Network Security)	🟪	🟪		8								🟩	
FireEye Inc. (Network Forensics/PCAP)	🟪	🟪		7						🟩		🟩	
HP Inc. (Computers, Printers 3D Printers)	🟪	🟪	🟪	81									🟩
Itron Inc. (Smart Grid)	🟪		🟪	10+		🟩	🟩	🟩			🟩	🟩	
Mantis Networks (MantisNet CVF)	🟪	🟪	🟪	1	🟩				🟩	🟩		🟩	🟩
New Context (Monitoring and Automated Reponse)	🟪	🟪		0	🟩		🟩	🟩	🟩	🟩	🟩	🟩	🟩
Optiv Federal (ForeScout)	🟪	🟪	🟪	5+	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Qubitekk (Quantum Protected Network)	🟪	🟪	🟪	<1		🟩					🟩	🟩	
SecureFLO (Service)	🟪	🟪	🟪	10		🟩				🟩	🟩	🟩	
SNC (Binary Armor)	🟪	🟪	🟪	6		🟩	🟩		🟩		🟩	🟩	
Templar Shield (Splunk)	🟪	🟪		15	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Verve Industrial Protection (Security Platform)	🟪	🟪		5+	🟩		🟩		🟩		🟩		🟩
Waterleaf International (CyberLeaf)	🟪			<1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Waterleaf International (CyberLeaf)	🟪	🟪	🟪	1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
				Totals	8	10	11	12	12	13	15	16	8

Figure 2. Example Survey Results Summary for the SIEM Security Technology



	NIDS Features								HIDS Features									SOAR Features							
	External timing for log stamps	Protect from data egress	Applicable to Purdue layers 0, 1, or 2	Decision support	Detect new conversations	Visualize networks and devices	Monitor unauthorized access	Support Industrial Control System protocols	Protect from data egress	Attach external timing for log stamps	Support Industrial Control System protocols	Detect new conversations	Decision support	Detects changes to firmware	Applicable to Purdue layers 0, 1, or 2	Monitor unauthorized access	Monitor changes in device	Visualize networks and devices	Orchestration	Web-based interface	Allow to set importance correct and recover	Centralized analysis	Decision support	Automatic categorization	Information sharing
OEM-SOLAR: Company A																									
OEM-SOLAR: Company B	🟩	🟩	🟩	🟩		🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	🟩	🟩								
OEM-SOLAR: Company C		🟩		🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
OEM-SOLAR: Company D														🟩											
OEM-SOLAR: Company E								🟩																	
OEM-SOLAR: Company F																									
OEM-SOLAR: Company G				🟩	🟩	🟩	🟩	🟩																	
OEM-EV: Company A	🟩			🟩			🟩			🟩				🟩			🟩								
OEM-EV: Company B (1)		🟩					🟩																		
OEM-EV: Company B (2)																									
OEM-EV: Company B (3)													🟩			🟩	🟩	🟩		🟩		🟩		🟩	
OEM-EV: Company C				🟩	🟩	🟩	🟩	🟩																	
Totals	12	13	15	16	8	8	8	10	11	12	12	13	15	16	8	8	8	8	10	11	12	12	13	15	16

Figure 3. OEM Survey of Cybersecurity Application

Planning for a Cyber Resilient Power System

An integrated security reference architecture will establish a resilient foundation for countering threats through, among other things, comprehensive real-time awareness. Building upon this foundation will include automated and autonomous responses, firing off in real time, and distributed mitigations to maintain operations of the system in spite of damaging storms and cyberattacks. Achieving comprehensive resilience for the nation's power system requires not only a high confidence correlation of mis-operation versus malicious attack, but also recognition that the power system lives in continuously contested space[11]. In establishing distributed protection approaches, the ability to recognize/respond to threats localizes impact and prevents catastrophic loss. It also reduces the time to recognition and response, limiting the adversary's ability to comprise the power system.

As we look to advance if not accelerate the integration of distributed renewables, it is important to ensure that the appropriate, tailored cybersecurity approach is applied consistently across all interfaces to establish the secure reference architecture suggested. As we progress toward this goal, it is important to understand the positions and perspectives of industry. In so doing, a more precise understanding of where government investments are required can assist prioritization. The survey presented in this article provides some of this perspective, but we would like to hear from additional industry representatives to ensure an accurate correlation of the need. To that end, please take a moment to complete a short Qualtrics industry survey. The results of the updated survey results will be shared broadly with the renewables industry.

[11] https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies