SECURING DISTRIBUTED ENERGY RESOURCES

The use of small-scale distributed energy resources (DERs), such as wind and solar photovoltaics, are growing rapidly and transforming the power grid. In fact, a distribution utility may need to remotely communicate with thousands of DERs and other grid edge devices—many of which are not owned by them. How can companies provide secure access to DERs and monitor and trust the ever-growing amount of data coming from them?

The NIST National Cybersecurity Center of Excellence demonstrates how to apply the cybersecurity capabilities shown here to protect the digital communication and control of cyber-physical grid edge devices.

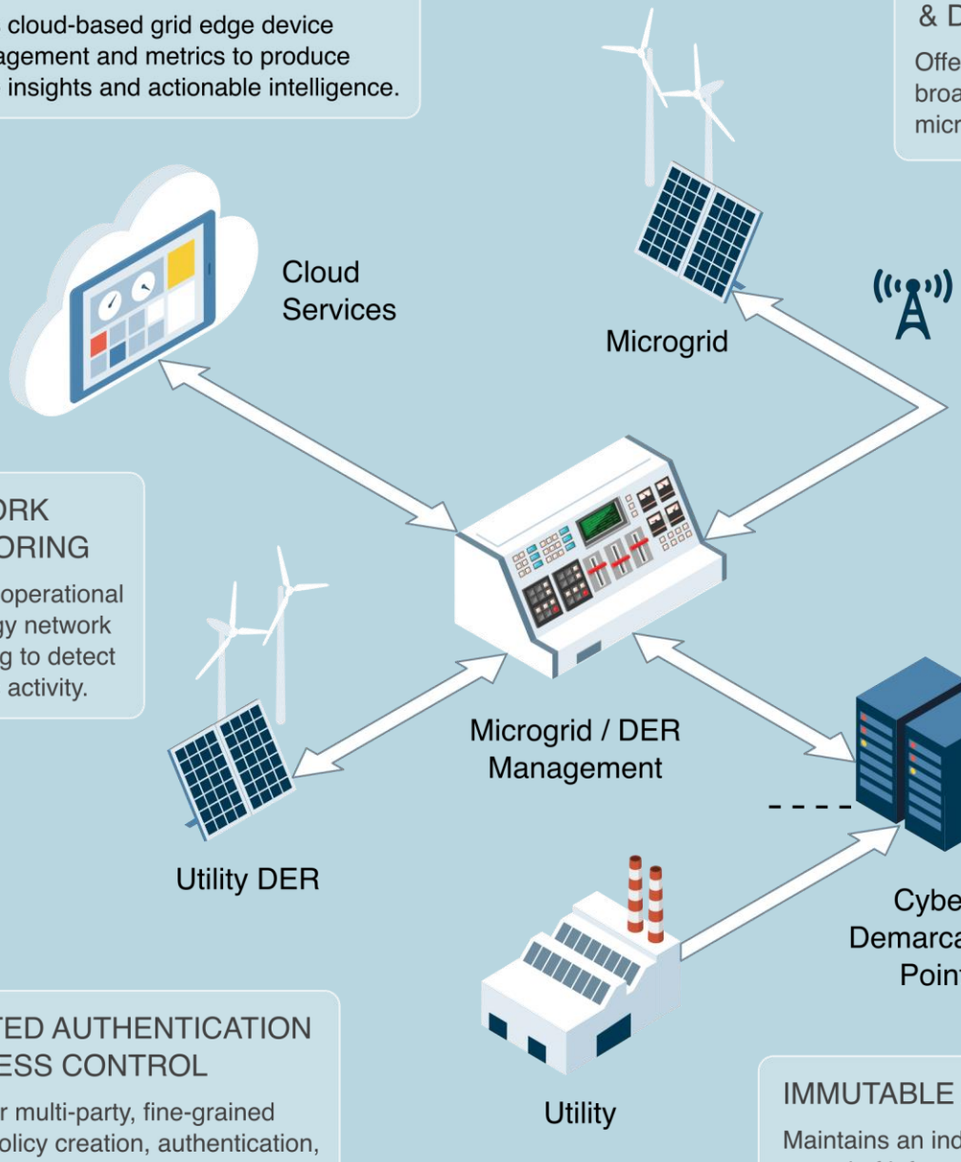
Learn more by visiting:
https://www.nccoe.nist.gov/iiot

ANALYSIS & VISUALIZATION

Provides cloud-based grid edge device log management and metrics to produce real-time insights and actionable intelligence.

COMMUNICATIONS & DATA INTEGRITY

Offers LTE on wireless broadband for campus microgrid communications.



NETWORK MONITORING

Provides operational technology network monitoring to detect malicious activity.

MALWARE DETECTION

Detects process anomalies or unwanted grid edge device modifications.

TRUSTED AUTHENTICATION & ACCESS CONTROL

Allows for multi-party, fine-grained access policy creation, authentication, and secure access control and data sharing for human, machine, and application interactions across utility and grid edge device operations.

IMMUTABLE AUDIT TRAIL

Maintains an independent, unchangeable record of information exchanges between a grid operator and the device owner(s).

Anterix · CISCO · DOTS BRIDGES · radiflow Secure your Assets · SA SPHERICAL ANALYTICS · sumo logic · tdi technologies · University of Maryland 1856 · xage SECURITY

NIST National Institute of Standards and Technology U.S. Department of Commerce | NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE