AZZO
technology comes together®

ENERGY ORCHESTRATION IN A WORLD OF CYBERSECURITY, CLOUD AND IoT

JASON HEINDEL
AZZO USA LLC

azzo.com

INTRODUCTION

The intent of this white paper is not to provide a comprehensive design and implementation guide for cybersecurity and network infrastructure but rather provide the general reader who may be an end user interested in a microgrid or perhaps a design team member working actively on a microgrid project a set of general topics to consider regarding IT networking and cybersecurity relative to microgrids.

The basis for this document originates from AZZO's extensive work in renewable energy projects, specifically with microgrids and how we deliver these projects.

THE WHY

Deploying a microgrid provides challenges not only with the physical infrastructure and electrical distribution, but also from the controls perspective. A microgrid control system is at its core a type of industrial control system. Much like any type of industrial control system, microgrid controls are at risk from cyber-attack. Many readers will be familiar with the Stuxnet cyberattack against industrial facility SCADA systems or Target hack via the BMS system or the recent SolarWinds hack of an IT monitoring system platform.

The first instinct of many may be to reduce the chances of a cyberattack by isolating the microgrid control system from connection to the Internet or other building systems. This is called "air gapping" i.e. creating a physical gap between the control system and other systems, networks and the Internet. That could be a good strategy, but in today's Internet of Things (IoT) enabled and digitized world, there are many reasons why the control system will need to connect to the world at large.

In the case where a system is air gapped, the only way to do software updates, system programming etcetera is to physically connect another computer or memory devices to the control system. This is as much a vulnerable entry point into these systems as a network connection. In many cases, cyberattacks are carried out with social engineering, designed to thwart airgapped security, such as infected USB. In today's IoT-enabled world, there is great need connect microgrid control systems both to other control systems and the world at large via the Internet.

There are many microgrid use cases that can only be supported via connection to the Internet and cloud-based services. Cloud based microgrid optimization systems exist to provide forecasts and predictions as to what the control system should do in anticipation of changing conditions. Those changing conditions can include a reduction in photovoltaic output due to expected cloud cover, changing utility energy pricing, anticipated ancillary grid support requirements or storm preparedness.

USE CASE 1

Prediction of reduced next-day photovoltaic generation

In the case of prediction of reduced next-day photovoltaic generation because due to cloud cover, the microgrid may orchestrate the ramping up of storage of electricity or it may opt to ramp up production of other DERs (Distributed Energy Resources) or curtail loads to match predicted generating capability. These types of forward-looking capabilities are only possible with an Internet-connected Artificial Intelligence planning system.

USE CASE 2

Optimal operation of the generating and distribution assets

Another benefit of an Internet-connected microgrid is to ensure optimal operation of the generating and distribution assets. Similar to how the jet engine manufacturer Rolls-Royce remotely monitors the operation of their fleet of engines, many DER manufacturers remotely monitor the operation of their generating equipment and can dispatch maintenance crews to enact repairs. Like Rolls-Royce, cogeneration manufacturer Gruppo AB provides remote monitoring and support for their engine/ generator equipment. This provides a major opportunity for microgrid owner/ operators who many not have the interest or technical capabilities to support complex generating assets like combined heat and power biogas generators. The customer gets the advantage of experienced technical support from the equipment manufacturer, but only if data from the equipment can reach the central monitoring station.

USE CASE 3

Vendor agnostic cloud-based orchestration platforms

Connecting DER equipment to the Internet enables centralized monitoring and management of disparate DER equipment manufacturers. PV inverters are often connected to a manufacture-specific monitoring portal.

But what happens if a property owner with PV systems on several malls, all of which were procured through different contracts and contain inverters made by several different manufactures. each with their own monitoring portal? How can the fleet of inverters be orchestrated from one central location when each inverter is connected to a different system? Utilization of vendor agnostic cloud-based orchestration platforms allow centralized monitoring without the need to log in to multiple different web portals. Enterprise management is only possible with IoT connected equipment and access to the Internet.

USE CASE 4

Healthcare microgrid control systems

In the age of the COVID pandemic, remote access and monitoring of any type of building systems is important but is particularly vital in electrical distribution systems. Having the ability to log in to a microgrid control system remotely and perform operations or investigate alarms and faults should be a mandatory requirement in the design of microgrid.

Interestingly, the 2021 edition of the NFPA 99 Healthcare Code received updates in the electrical section regarding the utilization of microgrids in healthcare that in section 6.10.6.1.2 states “Intelligence and Memory of health care microgrid control systems shall not be dependent on off-site resources.” This runs counter to the use cases previously discussed to use cloud services to optimize the operation of a microgrid. It seems like a shortsighted code requirement that doesn’t truly understand how modern microgrids operate. The code may also create a false sense of security by air gapping a microgrid. Recall the story of Stuxnet, air gapping is not a guarantee of a secure system. The latest standard appears to have omitted utilization of many of the tools and services that make microgrids truly useful. Hopefully, this section will be modified in coming editions of NFPA 99.

THE HOW

As we have described, there is no escaping the need to connect microgrid control systems to both the Internet and other systems. As a result, a proactive and educated approach to cybersecurity must be taken to ensure the security of the control system. Vendors, designers and contractors who are involved in the development of microgrid control systems should use control systems integrators who are cybersecurity experts in several key areas:

- Securing devices & hardware
- Utilizing secure software
- Securing user access to the control system
- Securing network traffic to and from cloud source

Securing Devices and Hardware

Microgrid control systems begin with a basic IT network architecture design. Much of today's microgrid equipment are Ethernet enabled, and thus require network cabling to connect to the control system. The control system will require some quantity of network switches which are managed by a network management solution. Firewalls will need to be provided at each access point to the control system from the Internet or other networks and systems. All these devices need to be included in an overall management solution. The switch management solution should allow for the ability to control and regulate the operation of any network port. Unused ports on any switches and devices need to be secured to remove a point of intrusion into the control network. The network management solution must also be able to whitelist ports and sites and grant access to only systems and sites that are approved by the system designers and operators.

The connected devices, electrical equipment and hardware the edge control layer and those systems and software that provide the onsite orchestration of the microgrid must be designed to conform to common standards such as IEC 61850. Electrical equipment and systems that use open protocols like IEC 61850 ensure a interoperability among microgrid components and systems. However, IEC 61850 alone will not ensure a cybersecure microgrid. IEC 61850 paired with a standard such as IEC 62443, discussed in the next section, provides a framework for electrical network cybersecurity.

Utilizing Secure Software Solutions

Microgrid control software solutions should be developed within a Secure Development Lifecycle (SLD) that is certified to a cybersecurity standard. A common standard used to certify SLD for electrical distribution system equipment and solutions is IEC 62443. For a purchaser of microgrids, IEC 62443 is a good benchmark for evaluating potential solutions and suppliers. There are many microgrid control software solutions in the market today. Careful evaluation must be made as to the cybersecurity processes & controls during the development of a software platform, and how that cybersecurity is maintained over the product lifecycle. As an iPhone updates its operating system regularly, control software needs to be evaluated for potential security risks and updated as required.

Equally important is to work with a partner who has expertise in cybersecure implementations/integrations. It is one thing to purchase certified hardware and software, however the proper deployment and configuration is essential to deliver on the protection the standard was meant to ensure. Improperly commissioned software and systems can easily create security risks. Proper certification of the systems integrators is as important as the certification of the components.

Securing User Access

As with any computer network, user access must be controlled. Systems need to have role-based access levels and authorizations with each user having a unique login and password. To manage the users, the control system should deploy a user management system such as Active Directory. It is possible to integrate a corporate network IT single sign on (SSO) system. However, the integration of a corporate wide SSO, presents challenges, the least of which is that the SSO managers likely have no familiarly with the control and operation of a microgrid. Establishing a standalone microgrid user management system is ideal. Once a user management system is established, Multi-Factor Authentication (MFA) should be incorporated.

Staff operating and managing the microgrid system AND the vendors and contractors that maintain and modify the control system must follow proper cybersecurity protocols. Laptops that connect to the network need to be secure and scanned for malware infection. During start up and commissioning phase of a project, vendors should only have access to the switch/ network segment that contains the equipment they are working on. Once the project is accepted, access the system should only allowed via direct coordination with the microgrid operator. Access must be revoked after then work is performed.

Securing Network Traffic

Finally, one of the most overlooked cybersecurity requirements is securing network traffic to and from the microgrid. It is common practice to provide unregulated Internet access to many types of DER equipment such as PV inverters. Through the connection to the Internet, the inverter manufacture will provide analytics on the operation of the asset. However, they often will use the same connection to push firmware updates to the equipment. As with any software or firmware update, sometimes things go wrong – AZZO has had experience with DERs suddenly not operating the way they were originally commissioned. The root cause was later determined to be a poor firmware update, which system operators were unaware was pushed by the equipment manufacturer . Securing traffic into the microgrid network is essential to prevent such unapproved firmware updates. With a regulated traffic flow, access to the equipment is only provided by exception, with careful coordination with the microgrid operator.

Regulating the traffic flow can be accomplished with a properly designed cloud hosting environment paired with a Software Defined Wide Area Network or SD-WAN. Providing a SD-WAN link between the cloud and the onsite systems and equipment allows the ability to segment and control traffic . In the example of unplanned firmware updates affecting microgrid performance, the SD-WAN regulates the flow of network traffic down to the site. The firmware is blocked until such time as it is given authorization to proceed via human intervention. Once the firmware is updated, the SD-WAN is again restricted, and no traffic can flow back down to the equipment.

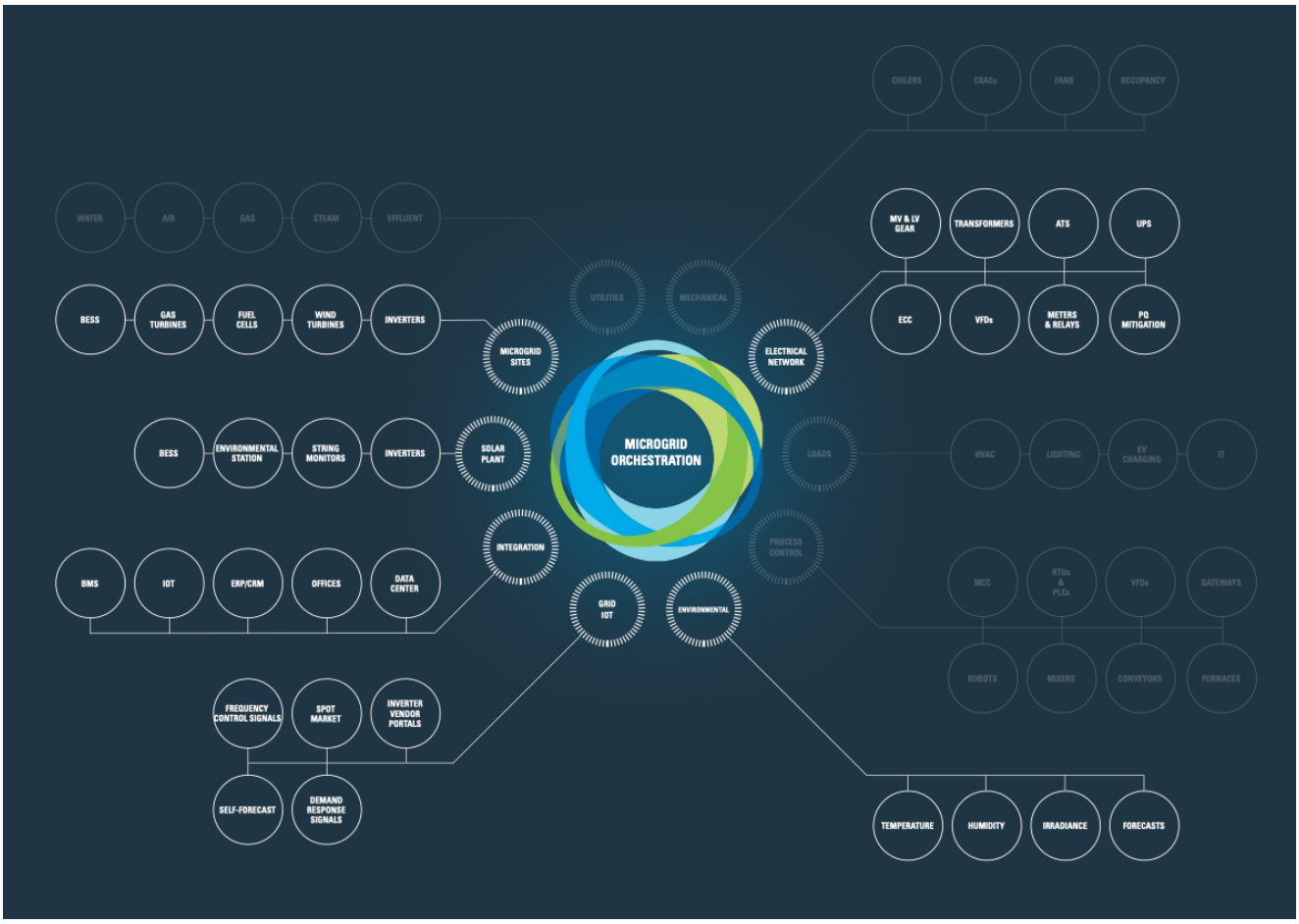

Figure 1 – Cloud, IOT & On-Premises Endpoints in a Secure Microgrid Architecture

SUMMARY

Microgrid control systems will need to be connected to the world at large via the Internet. Optimization, remote monitoring, control, and performance analytics can only be achieved with this connection. Owners, operators, designers, and implementers of microgrids need to be aware of the ramifications of cybersecurity. A microgrid project needs to have a well-defined and implemented cybersecurity strategy. This work should be performed by people and firms with the necessary experience and expertise.

ABOUT AZZO

AZZO is a global engineering and technology company that provides control & monitoring systems, fleet management and systems integration for the renewable energy and microgrid markets. We design, deploy and support these solutions bringing technology together with our core competencies in Energy Management, Electrical Engineering, Power Automation and Software Development.

Our customers are adding microgrids into an existing energy systems and strategies. AZZO is uniquely capable of integrating existing systems with new DER/microgrids with our Energy X platform.

AZZO has proven remote service capabilities which us to pre-commission these systems for plug-n-play cloud connectivity and remote monitoring and control architectures.

ABOUT THE AUTHOR

Jason Heindel is a 25-year veteran of the electrical industry holding progressive positions with some the largest electrical contractors in the country. He has transferred his design and construction experience to AZZO's USA operations where he develops and deploys control and monitoring solutions for the microgrid industry. Jason is a registered Electrical Designer in the State of Wisconsin.

WE CAN HELP YOU WITH YOUR ENERGY ORCHESTRATION SOLUTIONS.
CONTACT US TODAY TO LEARN MORE.

(USA) +1 973 575 5032 / (AUS) +61 1300 00 2996
solutions@azzo.com / solutions@azzo.com.au

AZZO
technology comes together®