SECURITYWEEK

ICS CYBER SECURITY CONFERENCE

Cybersecurity of Distributed Industrial Control Systems

19th October 2020 | Virtual Event

By Hal Aldridge, Ph.D.

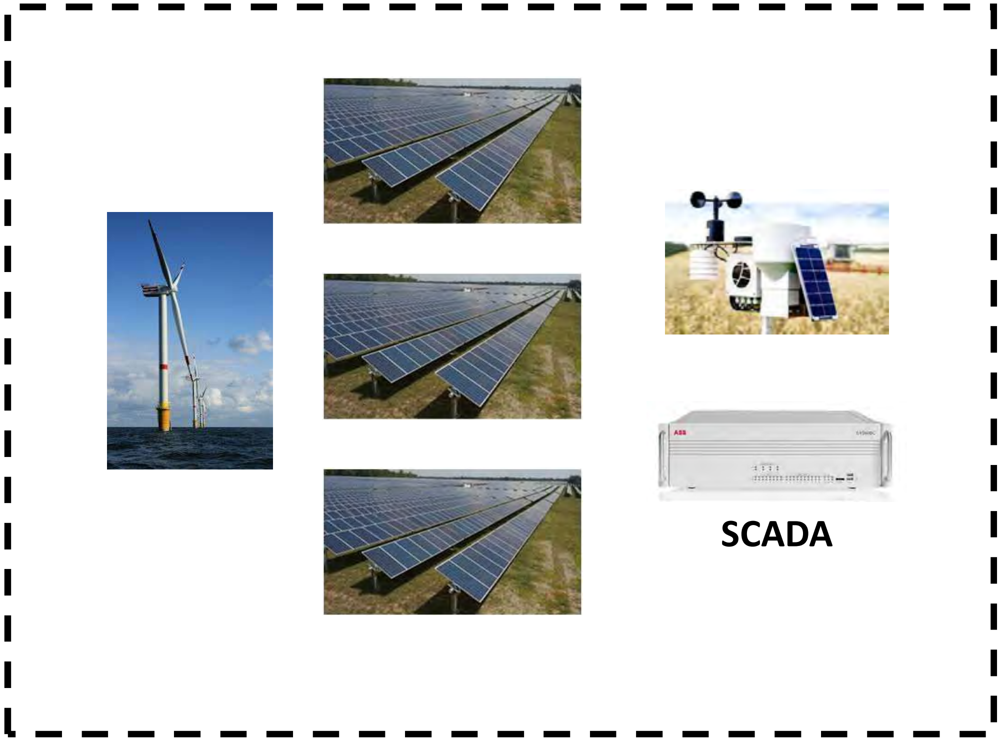
www.icscybersecurityconference.com

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

About Hal

- Ph.D. in Electrical and Computer Engineering from Carnegie Mellon University specializing in fault tolerant control systems
- 17 years experience development control systems for automation in space and defense applications at NASA and Northrop Grumman
- 13 years experience as CTO/CEO at companies developing high assurance cybersecurity for defense and industrial applications
- Currently CEO at ***SECMATION***

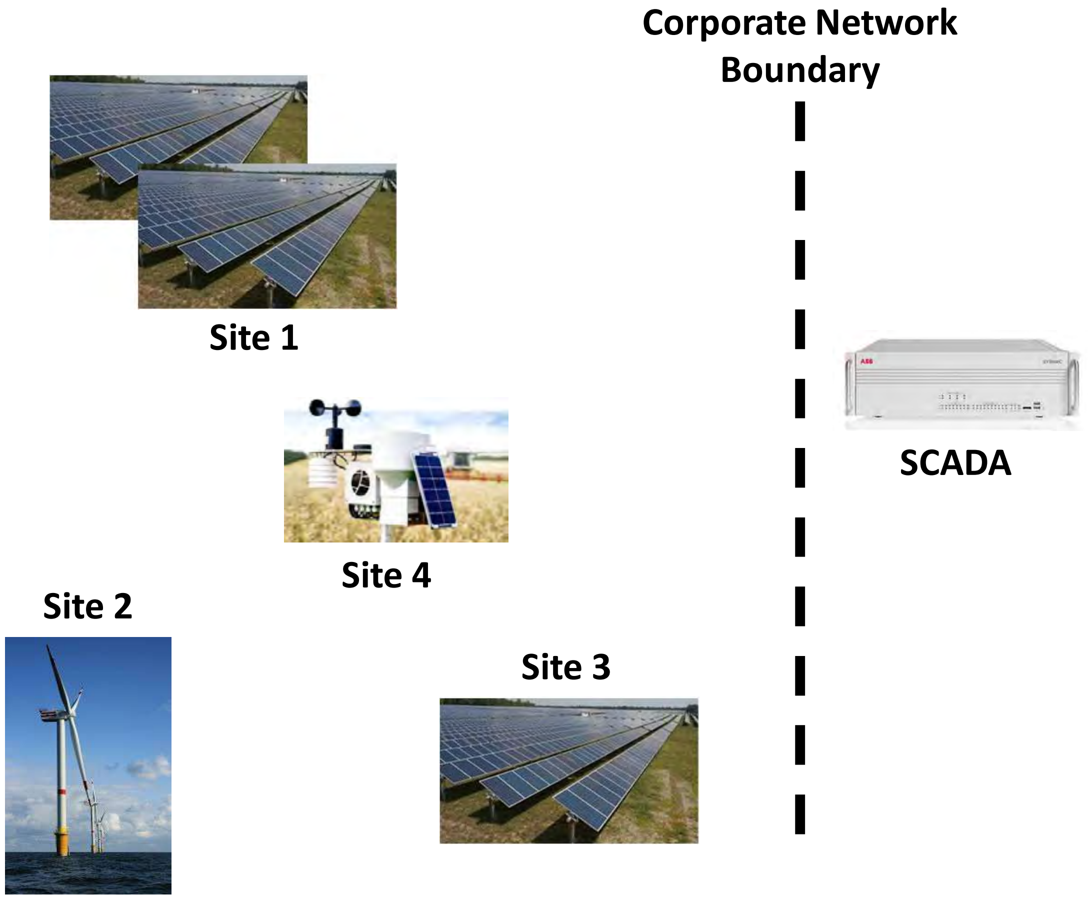
Traditional ICS Network



Example Renewable Energy Generation Application

- Air-Gapped or Tightly Controlled Private Network
- Wired or short-range wireless communications
- Challenges
    - Network topology vs. geography
    - Cost to deploy and maintain network infrastructure
    - Is it really secure?

Distributed ICS Network



Corporate Network Boundary

Site 1

Site 4

Site 2

Site 3

SCADA

- Equipment at **multiple sites** must coordinate with each other and corporate resources
- Sites are geographically challenged
- Not cost effective to implement private wired/wireless network
- Challenges
  - Availability
  - Latency
  - Security
  - $

Designing a Secure Distributed ICS

What does the Distributed ICS network need to function currently/safely?	Network Topology	Comm/Data Requirements
How will the communication be distributed?	Transport Provider	Wire/Wireless
What are the security/privacy related issues?	Trust	Data Security

Wireless for Distributed ICS

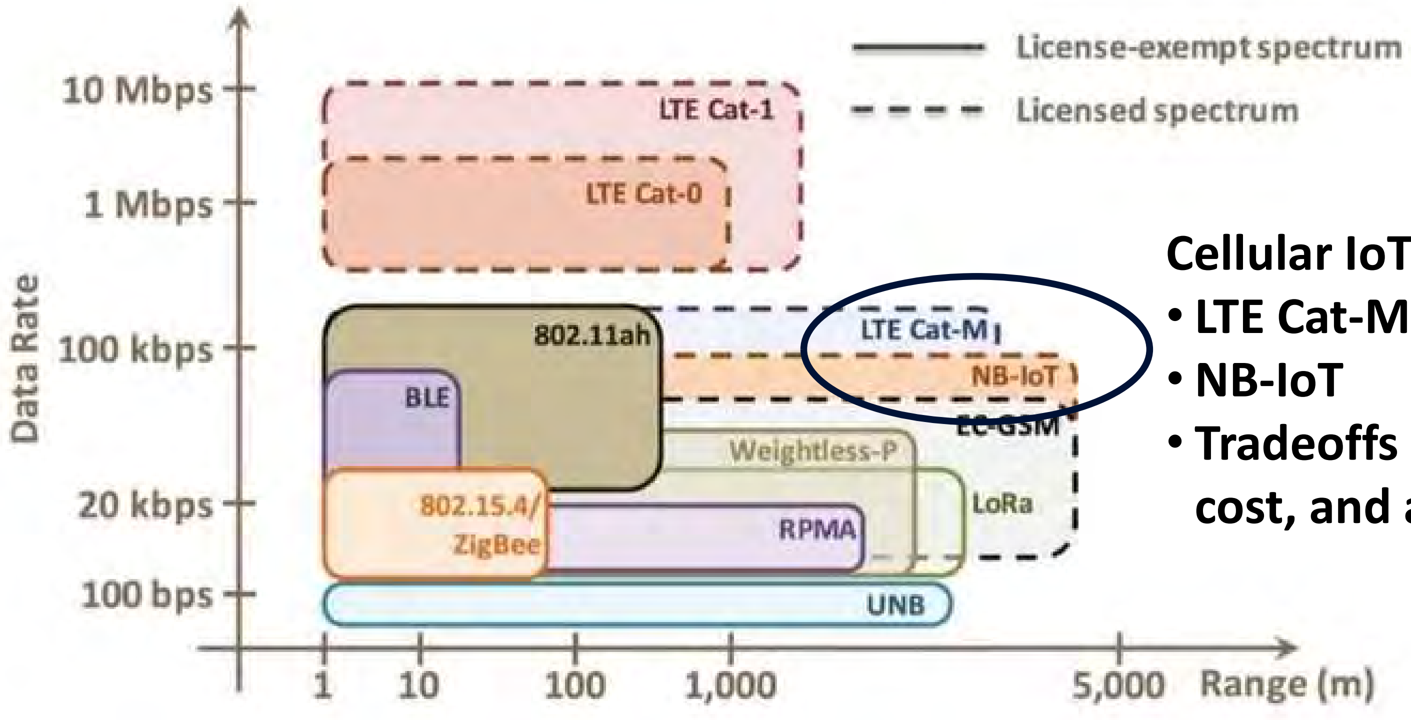
Wireless Technology Considerations

- Licensed vs. Unlicensed Frequency
- Spectrum Competition
- Network Topology – Mesh vs. Star
- **Cost**
- Standards – Openness
- Standards – Adoption
- Private vs. Public Network
- Proprietary Network
- IPv6
- SW/FW updates
- US-Only vs. Global Spectrum

Security Considerations

- Private vs. Public Network
- Data Sensitivity
- Trust in provider
- **Cost**
- Security/Safety policy
- Network vulnerabilities
- Security overhead
- Security maintenance
- Security pedigree / certifications
- Regulatory requirements
- Compatibility with legacy systems

Wireless Technology Trade-offs



Cellular IoT Services

- **LTE Cat-M**
- **NB-IoT**
- **Tradeoffs in speed, cost, and availability**

From: http://iot-fpms.wikia.com/wiki/LPWAN_networks

Cellular Challenges in ICS

- Availability – Service available in deployment area?
- Quality of Service – Reliable connection?
- Data Rates/Limits – Adequate for worst case needs?
- Connection Direction/Types – Connectivity in/through corporate network?
- Public/Private IP – Which meets security, flexibility, and data needs?

Cellular Connectivity/Solutions

- Standard Cellular Service
  - Lowest infrastructure complexity
  - Relies fully on security of end devices
- Multiprotocol Label Switching (MPLS)
  - Keeps cell traffic “off the internet” by routing internally at carrier
  - Lowers attack surface but must still trust the carrier
- Private Small Cell
  - Privately owned/operated cell network
  - Becoming more common/lower cost
  - Will proliferate in 5G

Transition to 5G

- Does anyone really know what 5G is/will be?
- What it likely will mean
  - Lower latency/higher data rates
  - Upgraded 3GPP 5G Security Standards
  - More flexible authentication and authorization
  - **More applications, telecom industry sees factory automation (and similar ICS applications) as target/growth area**

5G?

Who do you Trust? – Nobody…

- Distributed ICS lends itself to a **Zero Trust Networking (ZTN)** Model
  - Authenticate all data – Know origin before processing
  - Verify all data (e.g. packet inspection) – Check before processing. Sender may be authentic but could be compromised
  - Don’t trust the network/transport provider – Encrypt sensitive data

ZTN Challenges in ICS

- Overhead – How much does adding the required security mechanisms add to bandwidth/latency?
- “Invisibility” – How much can be done “behind the scenes” so ICS network can use ZTN with minimal/no modifications (especially an issue for legacy systems)?
- Security Pedigree – If you rely on security, do know how good it is?
- Failure Modes – What is the tradeoff for availability, safety, and security? Sometimes not an easy answer… Need to plan ahead.

What did we learn?

- Here is the secret… We just discussed some of the best practices for designing a ***Modern*** **Wide Area Network (WAN)**
- The usual ICS networking concerns are still there (protocols, reliability, availability, determinism, etc.) along with the normal challenges of using “IT” concepts in “OT” application
- We just switched the focus from **LAN to WAN**
- **Leveraging newly available technologies/standards makes the ICS WAN more secure and reliable**

SECMATION

Hal Aldridge, CEO
hal@secmation.com
www.secmation.com