Lessons Learned Performing Cyber Asset Discovery at Generating Facilities

Matthew E. Luallen
mluallen@encari.com

Introduction of Presenter

- **Matthew E. Luallen**
- **Co-Founder, Encari**

- **Mr. Luallen has written, consulted and trained extensively on process control and SCADA security issues. He worked with electric utilities with first the NERC UA1200 cybersecurity guidelines and in recent years with the NERC CIP mandatory standards. He has presented on ICS cybersecurity within CI to the FBI Infragard, USSS ECTF, ISA, NERC RROs, DOE National Labs, US Army Central Command, FAA, European Union, RCMP, and asset owners. Prior to incorporating Encari, Mr. Luallen provided strategic guidance for Argonne National Laboratory, U.S. Department of Energy, within the Information Architecture and Cyber Security Program Office.**

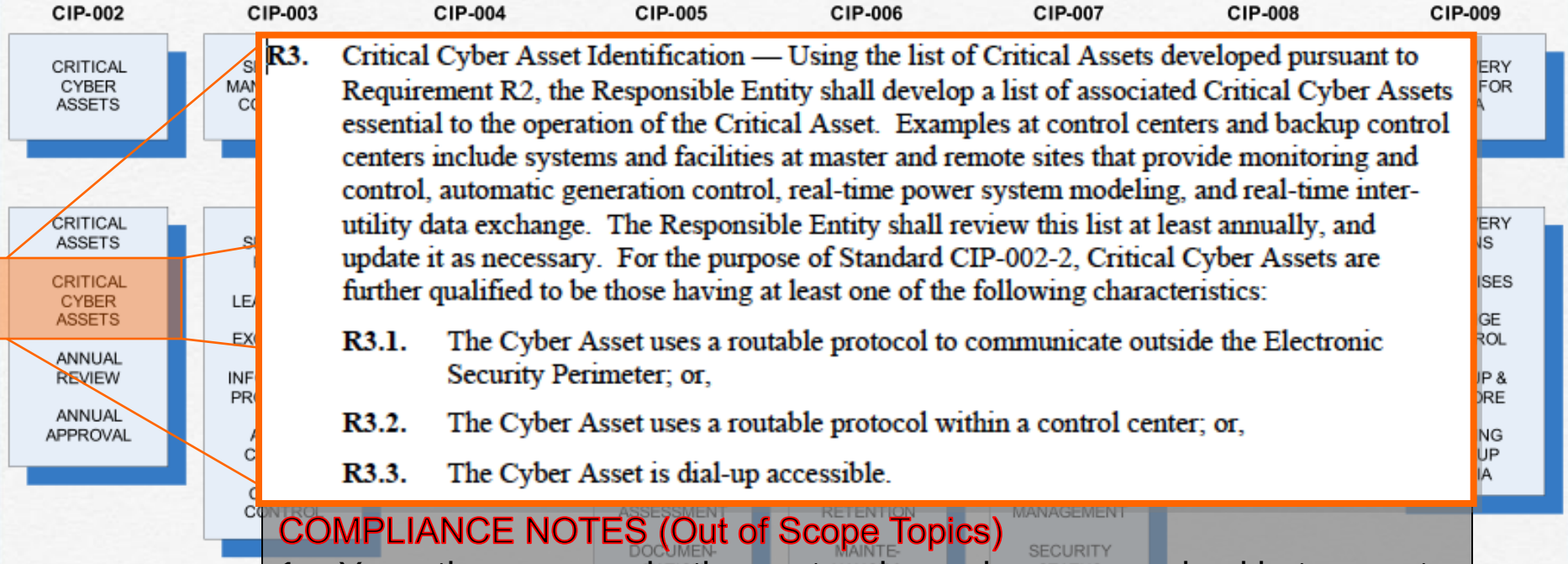
- **Mr. Luallen is also a CISSP, a 10 year CCIE, a certified instructor for Cisco Systems, a certified instructor and faculty for the SANS Institute, and adjunct faculty for DePaul University.**

ENCARI

Agenda

- **NERC CIP Standards Brief Introduction**
- **Performing a site survey to discover the physical location of Cyber Assets associated with the facility**
- **Interviewing Engineering staff to learn the critical functionality of each Cyber Asset**
- **Identifying engineered Cyber Asset dependencies**

NERC CIP Regulations
(This presentation is not about, it is due to)



R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

COMPLIANCE NOTES (Out of Scope Topics)

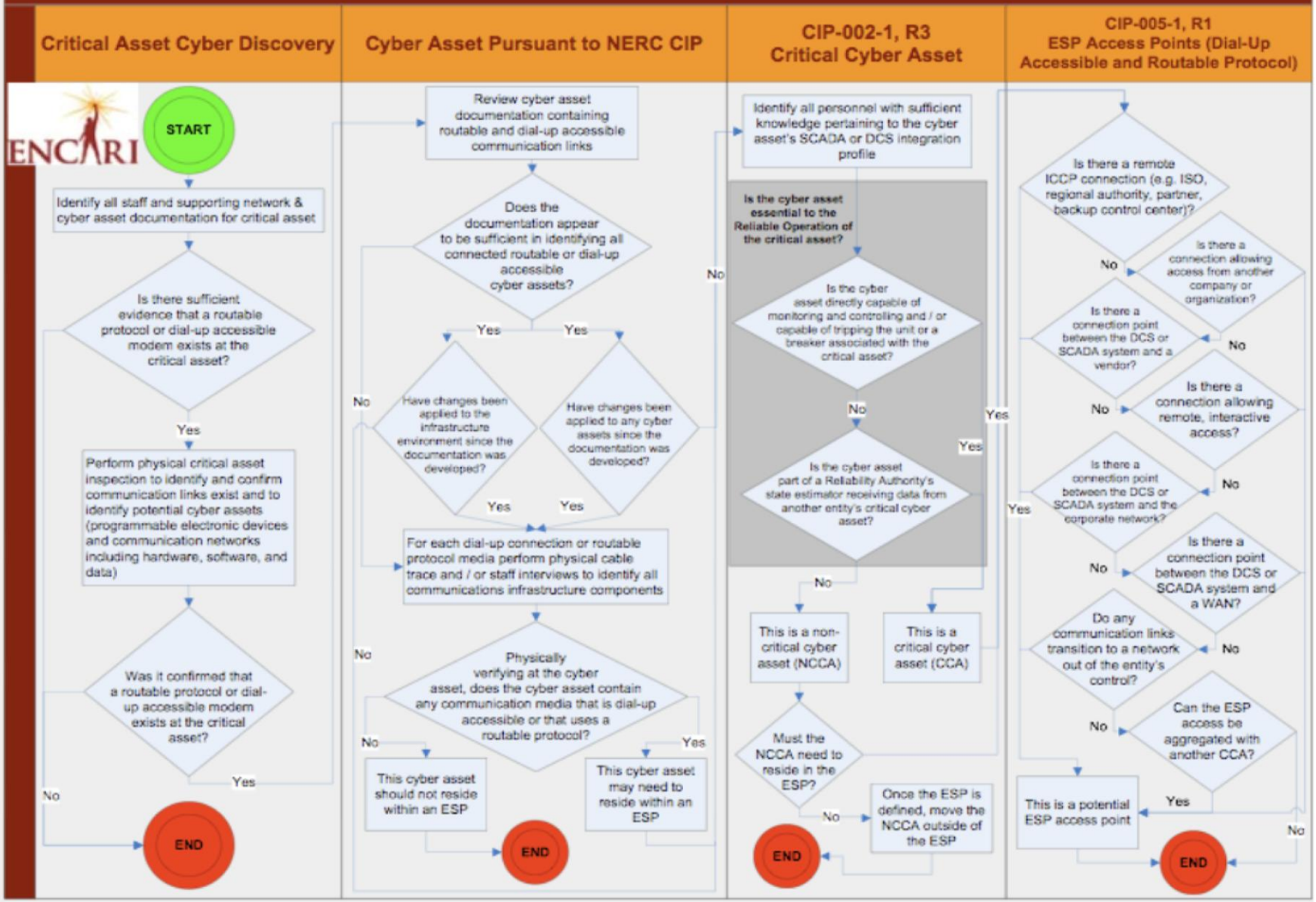
1. Yes, other communication protocols can be compromised but are not bound by the regulation; and,
2. Yes, routable has been derived to mean outer communication protocol headers (tunnels allowed), not inner (eg. MPLS); and,
3. Yes, there is no definition of “control center” versus generating facility “control room” in the NERC Glossary

ENCARI

Reference Sources and Presentation Goal

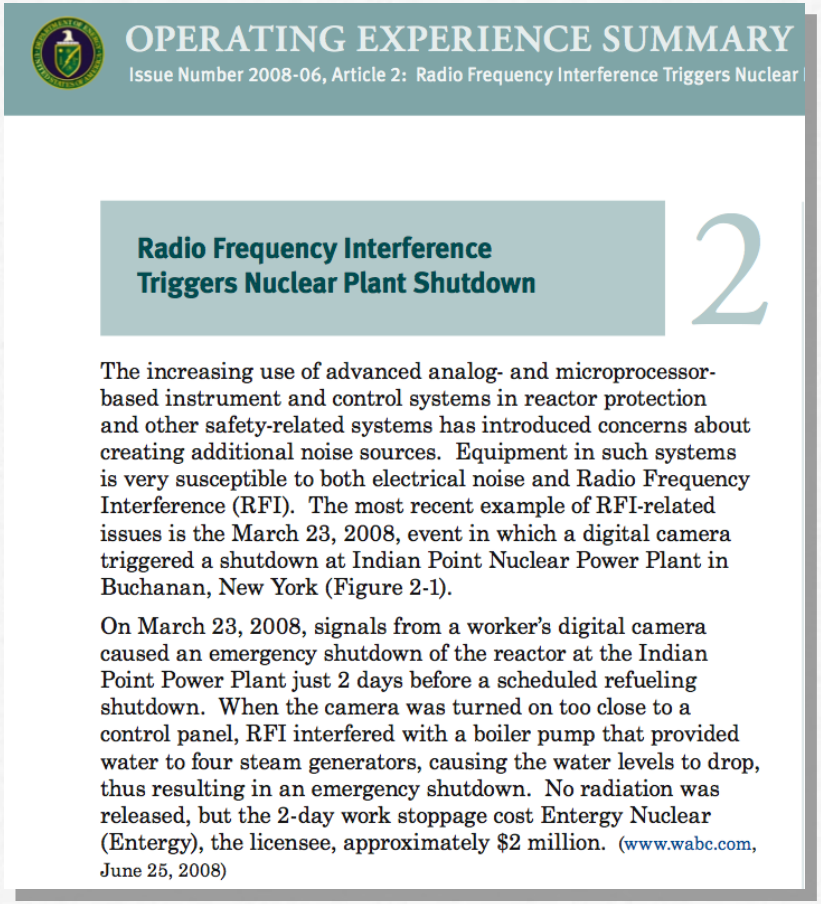
- **Fossil fuel and Hydro units deemed Critical Assets or in preparation of possibility of becoming a Critical Asset under NERC CIP Compliance**
- **Aided by lessons learned performing Cyber Asset discovery at control centers and substations**
- **Further aided by years of experience performing Cyber Asset discovery at universities and government facilities (a worthy set of adversaries)**
- **GOAL: How do you find your Cyber Assets.**

Cyber Asset, Critical Cyber Asset, Electronic Security Perimeter (ESP) and ESP Access Point Selection Methodology



Operating Experiences

- Digital camera RF interfered with boiler pump
- Breaker opened by physical security contractor
- Vibration monitor wire decoupled
- Board light bulb changed using pliers
- Inappropriate settings established by AI system
- <insert own personal war story>



OPERATING EXPERIENCE SUMMARY

Issue Number 2008-06, Article 2: Radio Frequency Interference Triggers Nuclear

Radio Frequency Interference Triggers Nuclear Plant Shutdown 2

The increasing use of advanced analog- and microprocessor-based instrument and control systems in reactor protection and other safety-related systems has introduced concerns about creating additional noise sources. Equipment in such systems is very susceptible to both electrical noise and Radio Frequency Interference (RFI). The most recent example of RFI-related issues is the March 23, 2008, event in which a digital camera triggered a shutdown at Indian Point Nuclear Power Plant in Buchanan, New York (Figure 2-1).

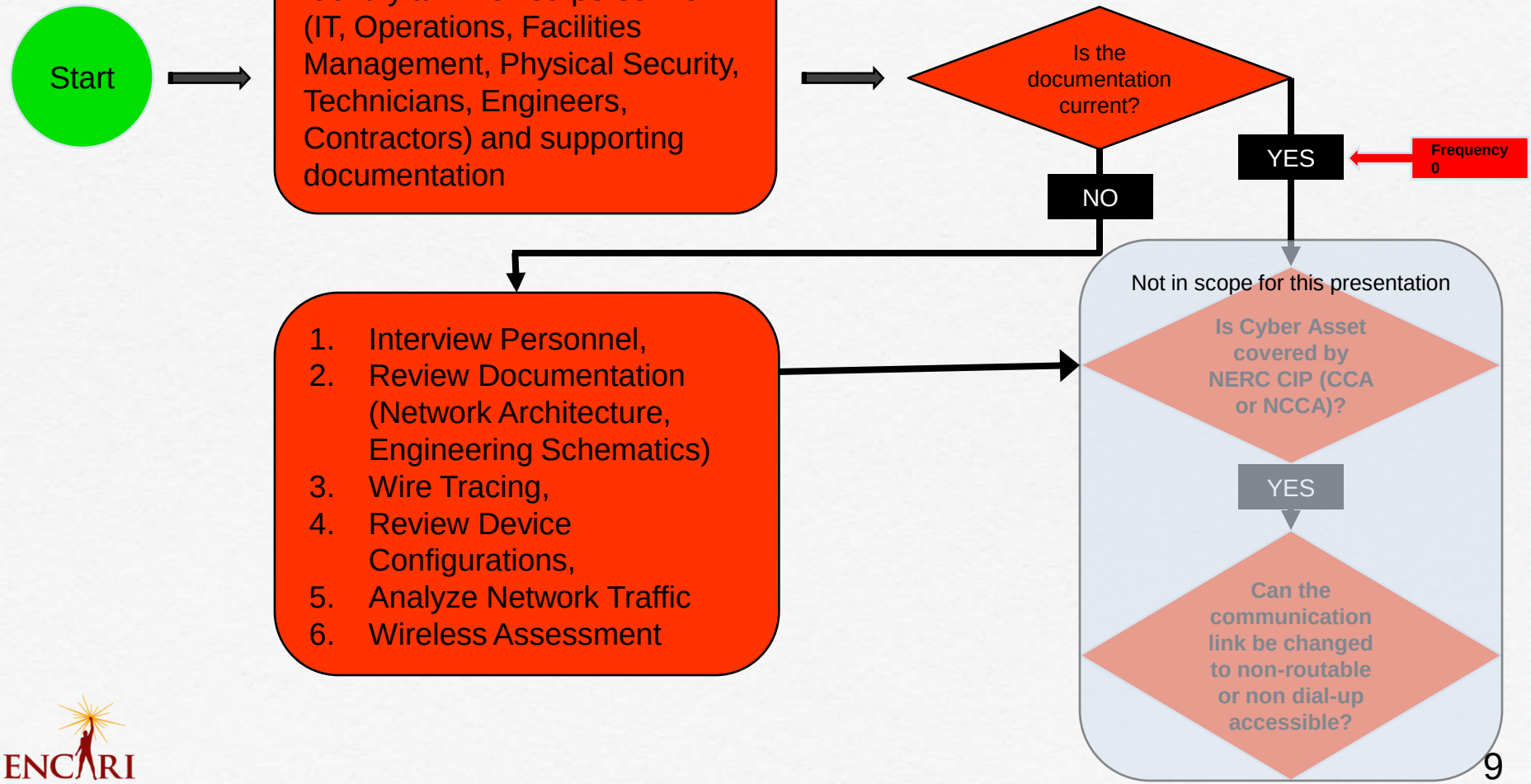
On March 23, 2008, signals from a worker's digital camera caused an emergency shutdown of the reactor at the Indian Point Power Plant just 2 days before a scheduled refueling shutdown. When the camera was turned on too close to a control panel, RFI interfered with a boiler pump that provided water to four steam generators, causing the water levels to drop, thus resulting in an emergency shutdown. No radiation was released, but the 2-day work stoppage cost Entergy Nuclear (Entergy), the licensee, approximately $2 million. (www.wabc.com, June 25, 2008)

ENCARI

Famous "Last" Words

- That fiber cable goes where?
- This is the janitor's closet and the main patch panel?
- The Internet is accessible through this WAP, connected on this port over here, and people are using it right now
- Yep, the unit just tripped.
- The CEM system is not critical. - Sidebar Discussion – We make operational decisions based upon NOx emissions.
- When did that get connected?!
- Yes, we do control the vibration monitors from corporate. They can not trip the unit. - Sidebar Discussion - Oh, we just enabled that?
- I did not touch it.
- Who plugged that in?!

Critical Asset Cyber Discovery



Labeling Cyber Assets as Critical (although out of scope)

- **Interview appropriate personnel to identify if the Cyber Asset**
  - **Can control a critical asset**
  - **Can be removed while the critical asset is operational**
  - **Is necessary for the reliable operation of the critical asset**
- **Essentially, can the Cyber Asset trip the unit or directly affect control of the unit?**
  - **Indirect control is inclusive for practical security, but be cautious about what is in your organization's absolute authority**

Interview Personnel

1. Interview Personnel,
2. Review Network Documentation,
3. Review Engineering Schematics
4. Wire Tracing,
5. Review Device Configurations,
6. Analyze Network Traffic
7. Wireless Assessment

- **Interview IT, Facilities Management, Operations, Physical Security, Vendors and Contractors to understand Cyber**
- **Operational procedures may make cyber asset indirectly critical; however not bound by NERC CIP standard (eg. NOx Emissions reach X ppm the operator shuts down the unit)**
- **What cyber assets or tools do you have manual procedures for?**
- **What data flows can you still calculate manually?**

Review Documentation

1. Interview Personnel,
2. Review Network Documentation,
3. Review Engineering Schematics
4. Wire Tracing,
5. Review Device Configurations,
6. Analyze Network Traffic
7. Wireless Assessment

- **Municipalities have shared infrastructure (eg. sewer, water, transmissions, gen) may use same control system**

- **Attempt to ensure documentation accuracy by taking sample sets of information (eg. This network device has 10 network cables entering it and only 9 in the documentation)**

Review Engineering Schematics

1. Interview Personnel,
2. Review Network Documentation,
3. Review Engineering Schematics
4. Wire Tracing,
5. Review Device Configurations,
6. Analyze Network Traffic
7. Wireless Assessment

- **Cyber, Physical events can alter operations**
- **Can cyber / physical security personnel influence operational decisions? Who granted the authority?**
- **Ask if the organization has integrated cyber and physical security in to operations (eg. NERC PER, PRC Standards); further directly in to CPA, PE, …**
- **Engineered capabilities may make cyber asset indirectly critical; however, not bound by NERC CIP standard (eg. HPWI system extinguishing unit flame)**

Wire Tracing

- **Cyber assets may be multi-homed with multiple dial-up or layer 3 connected communication interfaces (e.g. printers connected to servers; management interfaces connected to corporate; printers with 802.11 connectivity)**
- **Devices communicating across internal phone wires, Review WAN Bill Details**
- **Expansive Network (Engineering House, Coal Handling, Coal Dumping, HPWI System, Water Analysis, Pump House, Sump Pumps, Shared Systems among Units, Multiple Units, Railcar Wireless Control, Crane Wireless Control, Cellular Control)**
- **Actual critical assets may be coupled together (tightly) at OSI layer 2**

1. Interview Personnel,
2. Review Network Documentation,
3. Review Engineering Schematics
4. Wire Tracing,
5. Review Device Configurations,
6. Analyze Network Traffic
7. Wireless Assessment

Review Device Configurations

- **Router / Host ARP Tables**
- **Switch and Host MAC address tables**
- **DNS host tables**
- **Host, Firewall, Switch configuration settings**
- **PLCs, Relays, Control System software**

1. Interview Personnel,
2. Review Network Documentation,
3. Review Engineering Schematics
4. Wire Tracing,
5. Review Device Configurations,
6. Analyze Network Traffic
7. Wireless Assessment

Analyze Network Traffic

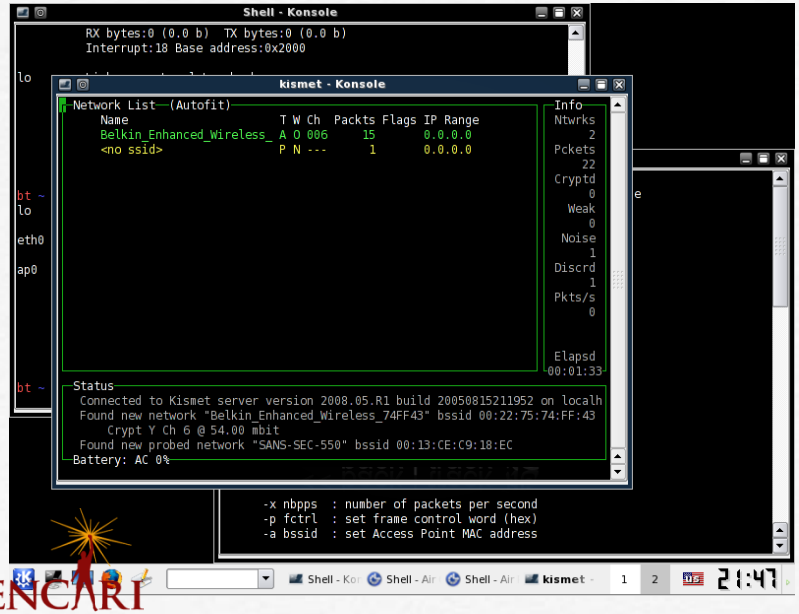
- **Enable port spanning / mirroring to replicate data streams to a sniffer; even better is to use a “Tap”**
- **Ensure vendor allows port spanning on their hardware**

1. Interview Personnel,
2. Review Network Documentation,
3. Review Engineering Schematics
4. Wire Tracing,
5. Review Device Configurations,
6. Analyze Network Traffic
7. Wireless Assessment

Wireless Assessment

- **Break / fix scenarios lead to wireless**
- **Deployment cost considerations (TBD with Security)**
- **RF Walkthrough (802.11) and 900 Mhz**

1. Interview Personnel,
2. Review Network Documentation,
3. Review Engineering Schematics
4. Wire Tracing,
5. Review Device Configurations,
6. Analyze Network Traffic
7. Wireless Assessment



Wi-Spy Comparison

	Wi-Spy 900x	Wi-Spy 2.4i	Wi-Spy 2.4x*	Wi-Spy DBx*
Antenna	RP-SMA	Internal Trace	RP-SMA	RP-SMA
Frequency Range	862 to 928 MHz	2.400 to 2.495 GHz	2.400 to 2.495 GHz	**2.4GHz:** 2.400 to 2.495 **5GHz:** 5.150 to 5.850
Frequency Resolution	24 to 375 KHz	373 KHz	27 to 421 KHz	**2.4GHz:** 26 KHz to 3 MHz **5GHz:** 24 KHz to 3 MHz
Filter Bandwidth	54 to 750 KHz	429 KHz	60 to 675 KHz	**2.4GHz:** 58 to 650 KHz **5GHz:** 54 to 600 KHz
Amplitude Range	-105 to -6.5 dBm	-100 to -6.5 dBm	-110 dBm to -6.5 dBm	-100 dBm to -6.5 dBm
Amplitude Resolution	0.5 dBm	0.5 dBm	0.5 dBm	0.5 dBm
Compatible Software	Chanalyzer Lite Chanalyer 3	Chanalyzer Lite	Chanalyzer Lite Chanalyzer 3 WirelessMon VisiWave	Chanalyzer Lite Chanalyzer 3 WirelessMon VisiWave

General Notes

- **Systems may have lots of additional applications installed as necessary by the Engineers**
- **Standardized deployment model – vendors, systems, applications, IP addresses, MAC addresses**
- **Personnel know some vulnerabilities – discuss them routinely**

NERC CIP Compliance Statement

- **If your organization has identified a Critical Asset and no Critical Cyber Assets due to the communication protocol requirement**

YOU MUST IMPLEMENT STRICT CHANGE MANAGEMENT CONTROLS INCLUSIVE OF ENSURING CYBER SECURITY REVIEW IN THE PROCUREMENT PROCESS AND ALL SYSTEM CHANGES

Q&A

- **This work is "To Be Continued", we are actively authoring a whitepaper with asset owners on this topic. If you are interested in being involved, please contact me.**
- **Contact Information**
  - **Matthew Luallen – Co-Founder, Encari**
    - (866) 943-9901
    - mluallen@encari.com