Questions for Industrial Cybersecurity students to ask while on industrial tours

Asset inventory

- How many total PLCs do you have?
- How many total network addressable VFDs do you have?
- How many different PLC vendors do you have?
- Can you explain the procedures used to keep your PLCs up to date with the latest firmware?
- Do you use any smart or networked UPSes (in your control enclosures)?

Network issues

- Has a process ever shut down as the result of a network issue?
- How do you keep track of network services allowed on your plant network?
- How would you detect a new IP address on your plant network?

Change detection

- What procedure is used to make a set point change?
- How would you detect an unauthorized set point change?
- What procedure is used to make a control logic change (PLC programming)?

Connection to corporate or external networks

- What production data is used for business operations such as financial planning, automated accounting or automated reordering from your suppliers?
- How do you provide control system vendors or integrator firms with remote access?
- Can you technician lap top access your email? Can it access the internet?
- What is your strategy for connecting the plant floor to cloud services?

Recovery

- How do you keep backups of control logic programs?
- How do you keep backups of historian databases?

Clear security questions

- How do you monitor for vulnerability disclosures that might affect your plant?
- How frequently do you conduct cyber security assessments for the plant network?
- Have you ever practiced what to do in case of a cyber security incident on your plant network?
- Do you worry about supply chain integrity, including tampering?
- Do you regularly monitor for rogue WiFi access points?
- Would you participate in a local industrial cyber security working group if one existed?

IT-OT Gap

- In what circumstances does your IT or networking group interact with your operations group?
- Do you feel like you have a good relationship with the IT people? Why or why not?

Observations to make

- What physical security did you notice?
- Were there contact switches on control panels?
- Were wireless communications used?