Impacts of Ransomware on Operational Technology

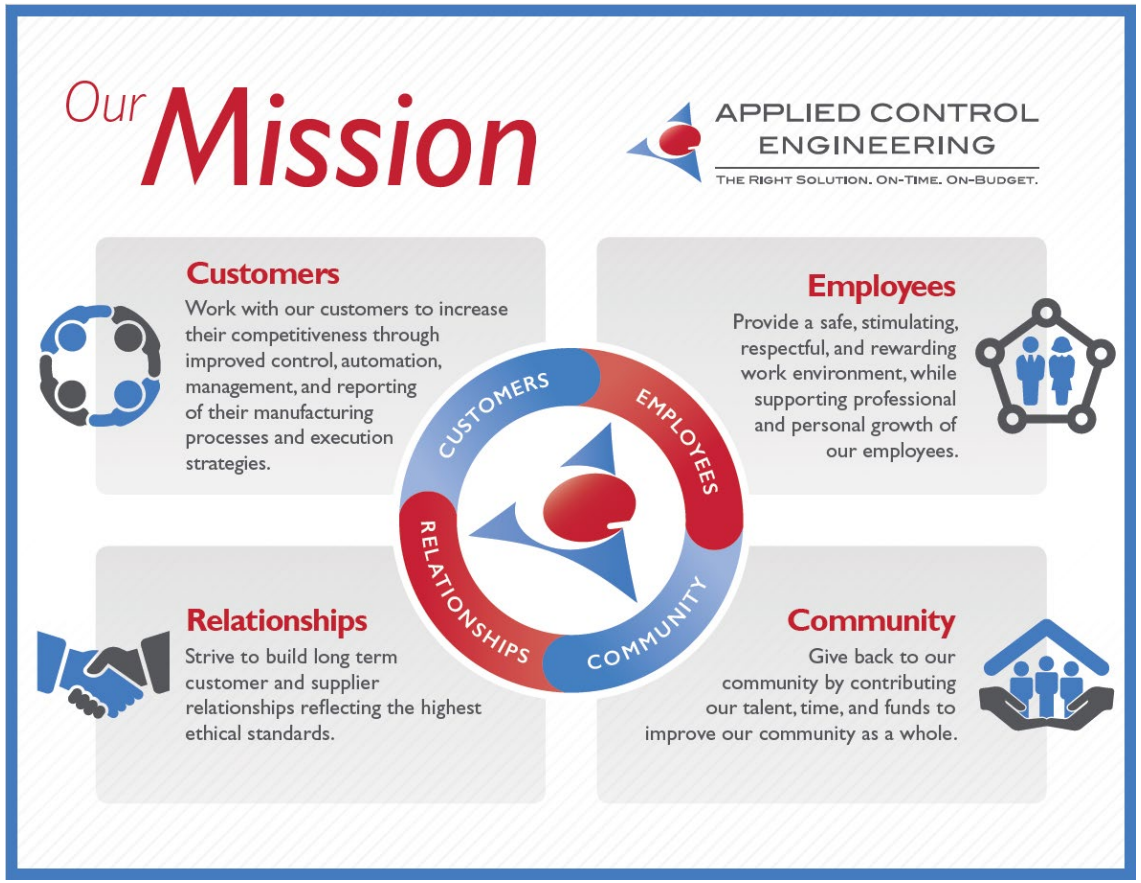
October 4, 2022

Timothy Mullen, GICSP

- Cybersecurity Team Leader (mullent@ace-net.com)

…with Applied Control Engineering

- Independent control systems integrator established in 1991
- 2021 Control Engineering System Integrator of the Year
- Offering services including *Advanced Process Control*, *OT Cybersecurity Assessment and Remediation*, and *Legacy System Migration*



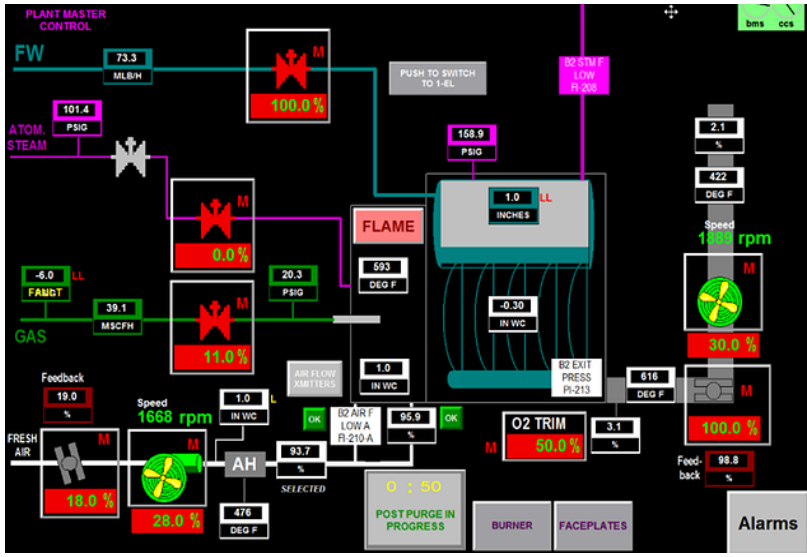
Offices in:

- Delaware Valley
- Chesapeake Region
- Greater Boston
- Greater Pittsburgh
- Gulf Coast
- Lehigh Valley
- New England

Agenda

- Review the differences and similarities between IT and OT
- Review the unique risks that malware (including ransomware) pose to OT systems
- Identify ways to limit the impact

The machines are in control



Some definitions

- OT: Operational Technology
  - The purpose of OT systems is to monitor and control physical processes such as machines, reactors, and factory lines
  - Includes traditional digital Industrial Control Systems (ICS) technologies alongside newer Industrial Internet of Things (IIOT) systems
  - Utilizes a large number of dedicated-purpose, embedded-system-style devices
    - Incumbent vulnerability visibility and management challenges

IT vs OT

- Traditional song is that IT is more data focused and OT is more function focused
  - In terms of the C-I-A triad, IT cares about C-I-A while OT cares about A-I-C

IT

- Technology served by technology
  - Need for upgrade cycles is understood
- In larger organizations often supported by dedicated network, infrastructure, security teams
- “Data” is typically an essential component of the system performing its critical functions

OT

- Technology serves the machines
  - The “machine” is expected to run for decades after purchase
- Needs to be supported by technicians, controls engineers, and integrators
- The “data” component is often low-confidentiality and low-volume
- System downtime = no product produced

The Convergence

- OT uses COTS IT networking technology and Windows computers
  - We're all on Ethernet now…
- Both IT and OT systems are required for the critical production functions to be completed
  - See Colonial Pipeline, etc.
- Emerging IIoT typically depends on cloud for AI/ML based applications
- Response time and uptime requirements for the systems in their respective areas
- Networking design and infrastructure design challenges
- Patch and antivirus management of server and client operating systems
- Identification and management of cybersecurity risks

Typical Network Architecture

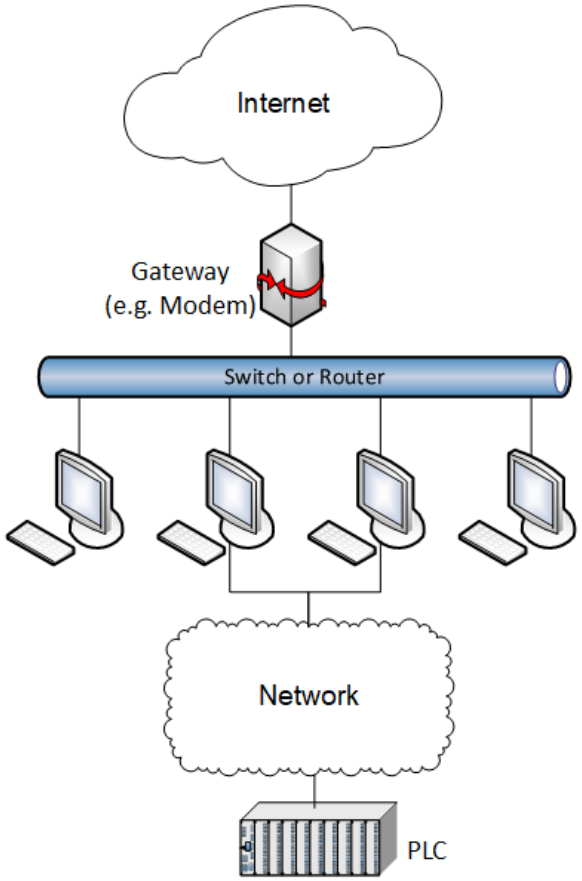


Figure 1. A diagram of a low-security configuration that poses a large risk to ICS assets.

What the control systems do for us

- Human Safety
  - Enforce safeguards that protect people from hazards
  - Safety logic increasingly being integrated into networked processors
- Physical Integrity
  - Enforce limits that protect equipment and product from damage
- Production
  - Perform the actions that produce the product

The Big Bad

Oldsmar, Florida Water Treatment Plant

- 02/2021, unidentified actor(s) used TeamViewer to connect to a SCADA HMI PC at a water treatment plant and commanded a 100-fold increase to the sodium hydroxide dosing setpoint
  - SCADA: supervisory control and data acquisition
  - HMI: human machine interface

Stuxnet

- 2009, advanced attack that jumped the air-gap, took advantage of zero-days in systems including Siemens PLCs to physically damage equipment by running it out of specification while reporting to operators that equipment was operating correctly

Consequences

- Hazards to human safety
- Hazards to process
- **Hazards to production**

The Common Con: Ransomware

- Per IBM Security X-Force, 33% of attacks against OT in 2020 were ransomware, the largest single attack type. In 2021, manufacturing was the most targeted industry

Colonial Pipeline

- 2021, business network infected with ransomware by DarkSide, pipeline shutdown while extent of attack unknown and while billing systems non-functional

Norsk Hydro, Hexion, and Momentive by LockerGoga

- 2019, LockerGoga ransomware infects and shuts down Norsk Hydro production plants

Also see **History of Industrial Control System Cyber Incidents, INL,** Kevin E. Hemsley, Dr. Ronald E. Fisher

The Soft Spot

- While the most important parts of the system are always the controllers, many control systems are effectively down if the **HMI** doesn't work
- Industry is extremely wedded to Windows operating systems for HMI
  - Typically managed differently than IT machines. For example, more often not domain joined
- Isolation between development and production systems often lacking
- Business needs have or will eventually pierce the "air-gap"
  - Upstream reporting, Need to send production orders downstream, etc.

Hazard to Production: What is the Recovery Time

- Do you know *what* all the system components are that need to be restored?
- Do you know *how* they need to be brought up to work?
- Do you know *where* to find your backups?
- Do you know how to *reapply* recent changes?
  - Licensing and software?

Actions

- Come up with an OT cybersecurity policy
  - Start small and act in proportion to your needs
  - Create requirements for new systems instead of waiting to evaluate and fix after delivery.
    - Cheaper to build-in at the start than retrofit.
- Design better systems that
- Retrofit or replace existing systems to transition away from legacy technologies
  - Contact a system integrator who is experienced in controls retrofits to transition away from legacy technologies
- Take advantage of established technologies to limit impacts
  - Virtualize legacy machines that cannot be upgraded yet
  - Deploy image-based backup systems and follow the 3-2-1 rule
- Harden systems and keep them up-to-date
  - Recognize and meet the risk

Actions (cont.)

- Create disaster recovery plans
  - Forces you to answer the questions around a down system
  - Not just a cybersecurity benefit: fork lifts hit panels, sprinklers start to leak, etc.
  - Often, a third party can facilitate capturing the critical information my providing a fresh set of eyes

Impacts of Ransomware on Operational Technology

APPLIED CONTROL ENGINEERING

THE RIGHT SOLUTION. ON-TIME. ON-BUDGET.