While the results of this survey reveal alarming statistics, organizations should use these findings as an opportunity to implement meaningful change to make a quantum leap in national and economic security.
Key survey findings include the following:

- 66% of respondents indicate their organizations are adding more connected IIoT devices to industrial control systems in the OT environment.
- 78% of respondents indicate they are not highly involved in industrial control system cybersecurity.

“Thousands of networked devices installed in critical infrastructure facilities are improving operating efficiency but increasing cyber risk,” said Carey Smith, president of Parsons Federal. “The perfect storm has already formed, with more connected devices in the industrial controls environment creating numerous points of access for increasingly sophisticated attacks. This survey puts a spotlight on the fact that converged OT and IT solutions are lagging behind the converged threat. The bolt-on, software-based, IT-centric model is not a plug-and-play solution to the OT cyber threat.”
End Point Protection in IT

Workstations and Servers
IT Place of Work
End Point Protection in ICS

Controllers

Valves and Meters
ICS Place of Work
Connection between IT and ICS

Computer Room AC and Power Distribution, Control, and Backup
Agenda

- What is ICS?
- Other, Related Terms
- Components
- Brief History
- Stakeholders
- Major Security Challenges
- Other Challenges
- What Do You Do Now?
- References
What is ICS? – A Definition

• One of many, many terms that seem the same to some folks, but very different to others

• Combination of control components – the system
  - E.g., electrical, mechanical, hydraulic, pneumatic

• Act together to achieve an industrial objective – the process
  - E.g., manufacturing, transportation of matter or energy, environmental conditioning

• Based on specified output or performance – the control

• May be fully or partially automated, the latter with a human in the loop
  - Open, closed, or manual

• Crucial to the operation of critical infrastructure
  - But, found in most operations in some form or another, such as building automation, security, and power management
What is ICS? – The Purdue Enterprise Reference Model*

Level 4
Business Planning & Logistics
Plant Production Scheduling, Operational Management, etc

Level 3
Manufacturing Operations & Control
Dispatching Production, Detailed Production Scheduling, Reliability Assurance, ...

Levels 2,1,0
Batch Control, Continuous Control, Discrete Control

* ISA-95
What is ICS? – The Purdue Model In Operation

* Also called Tiers

Level* 5: Corporate management and external connection

Level 4: Control system front end and IT network

Level 3: Field point of connection

Level 2: Field control system connected via Internet Protocol (IP)

Level 1: Field control system connected via non-Internet Protocol (IP)

Level 0: Sensors and actuators

“De-Militarized Zone” (DMZ)

Enterprise Zone

DMZ

Business Zone

DMZ

Operations Zone

Control Device Zone

Instrumentation Zone

Customer Web Services

Web facing e-mail

DNS

File/Print/Apps

Directory

Business DB

E-Mail

SIEM Correlator

Patch

Historian Mirror

Historian

SIEM Aggregator

Patch Deployment

Historian

Directory

Alarm Server

Historian

HMI

HMI

HMI

Engineering

Engineering

HMI Engineering

Patch Deployment

SIEM Aggregator

SIEM Correlator

Historian Mirror

Historian

Alarm Server

Directory

Web facing e-mail

DNS

Customer Web Services

Parsons

Safety Instrumented Systems
Other, Related Terms

- SCADA – supervisory control and data acquisition, various
- EMCS – energy management (or monitoring) control system, could be power or HVAC
- BMS – building management (control) system, HVAC, lighting
- DCS – distributed control system, usually electricity production and distribution
- IT and OT – information and operational technology
- IoT – Internet of Things, also IIoT, industrial IoT, could be a light bulb, or a wireless component of a much more complicated control system
- PIT – platform IT, mostly defense force projection platforms, control over weapons systems, for example

There may be more of which you are aware
Components

• IT (with a mix of OT)
  ▪ Routers and switches (OSI layer 2 and 3), some industrial grade
  ▪ Firewalls and one-way taps (data diodes)
  ▪ Servers for Active Directory, DNS, historian, log data
  ▪ Human Machine Interface (HMI) Workstations for operator, and Engineering Workstations for process engineer, programmer, and field technician (usually laptops)
  ▪ Operating systems – Windows and Unix
  ▪ Programming Language – many high-order languages, as well as database languages
  ▪ Protocols – TCP, IP, UDP, and others

• OT (at this level, little or no IT)
  ▪ Controllers - batch, discrete, drive, continuous, safety
    ▪ PLC – programmable logic controller
    ▪ RTU – remote terminal unit
  ▪ IED – (no bang, just control) intelligent electronic device
  ▪ Communication gateways
  ▪ Sensors and actuators
  ▪ Operating systems – QNX, VxWorks, Windows Embedded Compact, Embedded Linux
  ▪ Programming Language – ladder logic, function block, structured text, and others
  ▪ Protocols – ModBus, DNP3, ProfiBus, Ethernet/IP (industrial Protocol), and others
Brief History

- Physical Systems – you are in a maze of twisty pipes
- Local Controllers – electronic systems that receive information from sensors, display status, and permit an on-site technician to change settings that change activity using actuators
- Remote Analog Controllers – extended the local controllers via dedicated communications to centralized stations
- Digital Networks – addition of proprietary and industry protocols over standard circuits, such as RS 232, 422, and 485, yes, they’re still used
- The Internet – and intranets – replacement of the digital networks with Ethernet and application of TCP and IP
- A Plethora of IT/OT Systems – just too many to name
Stakeholders

• Those who care, or should
• Producers of power, treated water, HVAC
• Users of the services, especially major users, i.e., data centers
  • CIO
  • CISO
  • COO
Major Security Challenges

- End points are different, workstations versus controllers
- Internet
- Insider Threat
- Single Points of Failure
- Lack of Backup
- Failure to Look at Root Cause
- Attackers have the edge, don’t they always?
Other Challenges

- Executive Buy-in
- Funding
- Training and Awareness
- Lack of Understanding of the Network
- Lack of Concern for Functional Side
- Mixed Bag of Components, HW, SW, Old and New Tech
- Inability to Patch in Many Cases
- Lack of effective security tools - IT Tools Can Be Dangerous in OT
  - Some cause ICS failure, such as NMAP, Vulnerability Scans
  - Some are ineffective, such as traffic analysis from an IT point of view
- Lack of Security in Protocols
  - ModBus,
What Do You Do Now?

- Get Informed – *educate* yourself
- Know your Network – *educate* yourself
- How OT Fits in IT – *educate* your engineers and cyber folks
- How IT Fits in OT – *educate* your cyber folks and engineers

- There will be plenty more to do later, but for you now, ... well, you get the idea
References

• National Institute for Standards and Technology (NIST) Special Publication (SP) 800-82 Revision 2

• Committee for National Security Systems Instruction (CNSSI) 1253, Security Control Overlays for Industrial Control Systems

• ANSI/ISA-95 Enterprise-Control System Integration
Questions?

Thank you!