Industrial Control Systems

Chris Hankin
Generic ICS Architecture

- Human Machine Interface (HMI)
- Remote Diagnostics and Maintenance
- Controller
- Actuators
- Sensors
- Controlled Process
- Process inputs
- Process outputs
- Disturbances
- Set points, Control algorithms, Parameter constraints, Process data
- Manipulated variable
- Controlled variables
Glossary

• DCS: Distributed Control System – intelligence gathering throughout controlled process
• IED: Intelligent Electronic Device
• PLC: Programmable Logic Controller
• RTU: Remote Terminal Unit – a computer with radio interfacing
• SIS: Safety Instrumented System
• SCADA: Supervisory Control and Data Acquisition
CNI Sectors (UK)

- 13 sectors:
  - Chemicals
  - Civil Nuclear
  - Communications
  - Defence
  - Emergency Services
  - Energy
  - Finance
  - Food
  - Government
  - Health
  - Space
  - Transport
  - Water
Control Components

- SCADA, DCS and PLCs
- Electrical – for example, sensors
- Mechanical – for example, valves
- Hydraulic – for example, hydraulic presses
- Pneumatic – for example in HVAC control systems
ICS Industrial Sectors

• Manufacturing
  • Process-based:
    • Continuous Processes – for example, petroleum in a refinery or distillation in a chemical plant.
    • Batch Manufacturing – distinct start and end point, for example in food production.
  • Discrete: parts assembly and machining

• Distribution industries – typical in critical infrastructure (for example power or water distribution).

• Difference in geographic spread: manufacturing normally localized.
Water Distribution
Interdependencies

- Links between SCADA and DCS – for example power generation (DCS) liked with power distribution (SCADA).

- Interdependencies between critical infrastructure sectors – for example water treatment systems reliant on Grid.

- Possibilities of cascading failures.
Interdependencies, contd

Interdependencies, contd

From: Anytown: Final Report
A DEFRA funded project - Community Resilience Funding for Local Resilience Forums in England
Matthew Hogan, London Resilience Team
Interdependencies, contd
Interdependencies, contd
Interdependencies, contd
UK Power Outage, August 2019

• Lightning strike on transmission circuit at 4.52pm on Friday 9 August – return to normal operation after 20 seconds
• Off-shore windfarm and gas powered station both reduced supply – loss of 5% (1GW) capacity
• 1.1M customers without power for 15-50 minutes
• Trains stopped on SE rail – a number of cases, engineers were required to restart
• Other critical facilities affected – for example Ipswich hospital and Newcastle airport.
ICS Design Considerations

- Control Timing Requirements
- Geographic Distribution
- Hierarchy
- Control Complexity
- Availability
- Impact of Failures
- Safety
SCADA

From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security
Basic SCADA Comms Topologies

From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security
Large SCADA Comms Topology

From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security
Example of Implementation

From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security
DCS Implementation

From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security
PLC Control System Example
Modbus TCP/IP

• Protocol Data Unit (PDU) and Application Data Unit (ADU)
• The ADU consists of an Address, PDU and Error Check
• PDU format: Transaction ID, Protocol ID, Length, Unit ID, Function Code, Data
• Read, Write, Diagnostic codes
• Vulnerabilities: Identification, MITM, undocumented Function codes
Ethernet/IP

• Built on Common Industrial Protocol (CIP)
• CIP packet structure: Command, Length, Session handle, Status, Sender context, Options, Command specific data
• Vulnerabilities: Identification, MITM, undocumented commands
DNP3

- Distributed Network Protocol
- Data Link Layer – source and destination
- Transport Control Layer – fragmented packets sequence
- Application Layer – Function codes
- Read, Write, Delete, Restart
- Vulnerabilities: Identification, Fuzzing
Siemens S7comms

- Proprietary protocol
- S7 STP CPU
- S7 Identification
- S7 Password Brute Force
Countermeasures

• Keep firmware up to date
• Strong Network Segmentation and Network Security
• Password Brute-Force Countermeasures to prevent attacker from being able to gain access to password files
ICS-CERT Advice (based on 2013/2014)

Seven Strategies to Defend ICSs

- Implement Application Whitelisting – 38%
- Implement Secure Remote Access – 1%
- Ensure Proper Configuration/Patch Management – 29%
- Monitor and Respond – 2%
- Reduce your Attack Surface Area – 17%
- Manage Authentication – 4%
- Build a Defendable Environment – 9%