Cybersecurity for Critical Infrastructure (ICS, SCADA & IIoT)
Agenda

• ICS Introduction
• SANS ICS Security Survey Sharing
• Challenges
• Best Practice Deploying ICS Security
• Case Study and Summary
Process Control Network Evolution

20+ Years Ago

https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

Purdue Enterprise Reference Architecture (PERA)

Enterprise | Business | Level 4
---|---|---
DMZ | DMZ or 3.5
Manufacturing | Manufacturing Operations | Level 3
Plant HMI | Control Systems | Level 2
Intelligent Devices | Level 1
Process | Level 0

20+ Years Ago

Manufacturer Operations | Level 3
Control Systems | Level 2
Intelligent Devices | Level 1
Process | Level 0
### Process Control Network Transition to Industrial 4.0

- **What’s exciting to see is**

<table>
<thead>
<tr>
<th>Purdue Reference Architecture</th>
<th>IoT/IoT Reference Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enterprise</strong></td>
<td><strong>The Cloud</strong></td>
</tr>
<tr>
<td>Business</td>
<td>Business</td>
</tr>
<tr>
<td>Level 4</td>
<td>Level 4</td>
</tr>
<tr>
<td><strong>DMZ</strong></td>
<td><strong>DMZ or 3.5</strong></td>
</tr>
<tr>
<td>DMZ or 3.5</td>
<td></td>
</tr>
<tr>
<td><strong>Manufacturing</strong></td>
<td><strong>Manufacturing Operations</strong></td>
</tr>
<tr>
<td>Manufacturing Operations</td>
<td>Level 3</td>
</tr>
<tr>
<td><strong>Plant HMI</strong></td>
<td><strong>Control Systems</strong></td>
</tr>
<tr>
<td>Control Systems</td>
<td>Level 2</td>
</tr>
<tr>
<td>Intelligent Devices</td>
<td><strong>Intelligent Devices</strong></td>
</tr>
<tr>
<td>Level 1</td>
<td>Level 2</td>
</tr>
<tr>
<td>Process</td>
<td><strong>Process</strong></td>
</tr>
<tr>
<td>Level 0</td>
<td>Level 0</td>
</tr>
</tbody>
</table>

“IoT reference architectures must reflect these expanded operational borders, while also accounting for a secure and trustworthy integrated data network and ensuring that endpoints are both trusted and protected”
## SANS Survey 2018: Characterizing IIoT Device Connection

### Table 1. The Purdue Model and IIoT Connection Facts

<table>
<thead>
<tr>
<th>Purdue Model Hierarchy</th>
<th>% of IIoT Devices Connecting to Network Infrastructure</th>
<th>Protocols Used</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>32.4%</td>
<td>1. IP Suite (27.3%) 2. Web (21.2%) 3. IP Domain-specific (19.2%)</td>
<td>1. Wired (25.8%) 2. Wi-Fi (22.7%) 3. Cellular (17.5%)</td>
</tr>
<tr>
<td>Internet DMZ (Gateway)</td>
<td>32.4%</td>
<td>1. IP Suite (28.3%) 2T. Web &amp; IP Domain-specific (18.2%)</td>
<td>1. Wired (27.8%) 2. Wi-Fi (18.6%) 3. Cellular (18.6%)</td>
</tr>
<tr>
<td><strong>Business Zone</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 5: Enterprise Business Network</td>
<td>37.3%</td>
<td>1. IP Suite (33.3%) 2T. Web &amp; IP Domain-specific (22.2%)</td>
<td>1. Wired (30.9%) 2. Wi-Fi (27.8%) 3. Cellular (21.6%)</td>
</tr>
<tr>
<td>Level 4: Business Unit or Plant Network</td>
<td>44.1%</td>
<td>1. IP Suite (36.4%) 2. IP Domain-specific (31.3%) 3. Web (21.2%)</td>
<td>1. Wired (41.2%) 2. Wi-Fi (28.9%) 3. Cellular (19.6%)</td>
</tr>
<tr>
<td>Control Demilitarized Zone</td>
<td>32.4%</td>
<td>1. IP Suite (24.7%) 2. IP Domain-specific (22.2%) 3. Web (20.2%)</td>
<td>1. Wired (30.9%) 2. Wi-Fi (19.6%) 3. Cellular (17.5%)</td>
</tr>
<tr>
<td><strong>Process Control SCADA Zone</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 3: Operations Support</td>
<td>43.3%</td>
<td>1. IP Suite (35.4%) 2. IP Domain-specific (31.3%) 3. Web (22.2%)</td>
<td>1. Wired (42.3%) 2. Wi-Fi (26.8%) 3. Serial (20.6%)</td>
</tr>
<tr>
<td>Level 2: Supervisory Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 1: Control Devices</td>
<td>50.4%</td>
<td>1. IP Suite (25.3%) 2. IP Domain-specific (25.3%) 3. Non-IP based (21.2%)</td>
<td>1. Wired (27.8%) 2. Wi-Fi (16.5%) 3. Serial (15.5%)</td>
</tr>
<tr>
<td>Level 0: Process (Instrumentation)</td>
<td>30.4%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety Zone</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SANS Survey Securing Industrial Control System (2017, 2018)

Source: https://www.sans.org/reading-room/whitepapers/ICS/paper/38505

https://ics.sans.org/ics-library/survey/2017
ICS Standards Survey

Which cyber security standards do you map your control systems to?
*Select all that apply.*

![Bar chart showing the top 5 ICS security standards](chart.jpg)

Figure 18. Mapping to the Top 5 ICS Security Standards
Top Threat Vectors

What are the top three threat vectors you are most concerned with?

Rank the top three, with “First” being the threat of highest concern.

- Devices and “things” (that cannot protect themselves) added to network
- Internal threat (accidental)
- External threats (hacktivism, nation states)
- Extortion, ransomware or other financially motivated crimes
- Phishing scams
- Malware families spreading indiscriminately
- Integration of IT into control system networks
- External threats (supply chain or partnerships)
- Internal threat (intentional)
- Industrial espionage
- Other

Figure 5. Top Threat Vectors
Security Technology Used/Planned

What security technologies or solutions do you currently have in use? What new technologies or solutions would you most want to add for control system security in the next 18 months? Select only those that apply.

<table>
<thead>
<tr>
<th>Technology</th>
<th>In Use (%)</th>
<th>Planned (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial intrusion detection systems (IDS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Industrial intrusion prevention systems (IPS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control system network security monitoring software and solutions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset identification and management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security awareness training for staff, contractors and vendors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability scanning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring and log analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User and application access controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment and audit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-malware/Antivirus</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security Assessments

Regular security assessments/audits by trained and experienced security practitioners are fundamental to identifying areas of greatest risk and optimally targeting resources. Effective assessments provide:

- **Breach detection**. Analysts often find long-dwelling advanced persistent threats (APTs) only during detailed analyses of security controls, logs and configurations.
- **Network traffic analysis**. The highly deterministic nature of ICS networks enables assessment and identification of normal OT events and activities, allowing detection of anomalous and potentially disruptive or damaging communications.
- **Asset and network inventory**. Audits should validate the accuracy of asset and network documentation, including configuration data, while also identifying potential risks with rogue devices that should not be connected to the ICS.
- **Vulnerability identification and evaluation**. Assessments confirm the presence of vulnerabilities discovered by internal and external parties, evaluate the accompanying risks and recommend responsive actions, such as patching, reconfiguration, and replacement or addition of compensating controls.
- **Risk remediation action plans**. Assessments include recommended actions to address identified risks and evaluate whether the recommendations of earlier assessments have been completed.

*Figure 6. Top 11 Security Technologies in Use/Planned*
Challenges in Securing ICS/SCADA Networks

- Typical challenges faced in SCADA/ICS Network Security
  - Stopping advanced threats
  - Exploits
  - Malware & APTs
  - Protecting unpatched/unpatchable Legacy Systems
  - Managing Network Integration & Remote Access

Increasing Visibility and Segmentation

- Safely migrating to Industrial IoT architectures
  - Public Cloud & SaaS
  - Mobility
- CIP Standards
  - CFATS
  - Reducing cost and effort of compliance

…while addressing uptime and safety requirements

**High Profile Malware Targeting Critical Infrastructure**

- **Stuxnet**
  - The first case noted of a sophisticated digital weapon launched against control systems in Iran.

- **Flame**
  - Defined as a sophisticated malware and very complex. Capable of spreading to other systems over LAN connections or USB. Can record audio, screenshots, keyboard activity, and network traffic.

- **Energetic Bear**
  - A power malware which allowed its operators to monitor energy consumption in real time, or cripple physical systems.

- **Duqu**
  - Collection of computer malware thought to be related to Stuxnet. Used for looking for information that could be useful in attacking ICS.

- **Shamoon**
  - Like Stuxnet, Duqu and Flame, Shamoon targets energy companies. It did not disrupt services like Stuxnet, or steal business information like Flame and Duqu. Instead it removed and overwrote hard drive information.

- **German Steel Mill Attack**
  - Second confirmed case in which a wholly digital attack caused physical destruction of equipment.

- **Dragonfly**
  - Evidence points to pharmaceutical companies as the primary target. Malware does contain an Industrial Protocol Scanner used to find devices typically installed in packaging consumer goods.

- **Ukraine Attack**
  - BlackEnergy3
    - The primary objective appears to be cyber-espionage, discovery trojan-droppers capable of infecting SCADA Industrial Control systems could mean something more nefarious.
Recent Cyber Attack on Critical Infrastructure

DHS Says SamSam Ransomware is Targeting Critical Infrastructure Entities

The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have issued a joint alert this week indicating that the SamSam ransomware is targeting critical infrastructure entities. This type of attack is particularly concerning as it can have severe consequences on the safety and security of the country. SamSam is a ransomware that encrypts files on the victim’s computer and demands a ransom to decrypt them.

Russia's Power Grid Is an Easy Target for U.S. Hacking

The real message U.S. officials are sending to Moscow is that Russia can be hacked without White House authorization. Last week, the Federal Bureau of Investigation and the Department of Homeland Security issued a joint warning to U.S. power grids, stating that they are vulnerable to cyber-attacks.

Hacking Group Adds Electric Utilities to Its Energy Sector Targets

The most dangerous threat to ICS has new targets in its sights. Dragos identified the XENOTIME activity group expanded its targeting beyond oil and gas to the electric utility sector. This expansion to a new vertical illustrates a trend that will likely continue for other ICS-targeting adversaries.
Example: Attack to the Ukraine Electric Grid

1. **Breach Perimeter**
   - Spearphishing (Black Energy 0-day)
   - Steal User Credentials

2. **Deliver Malware**
   - Domain Controller
   - Host

3. **Endpoint Operations**
   - Corrupt HMI (known malware)

4. **Reach the Target**
   - Corrupt Firmware (ICS control plane protocols)
   - Open Electric Relays (ICS data plane protocols)

**Attack Chain**:
- Spearphishing
- Steal User Credentials
- Pivot to SCADA (using stolen credentials)
- Deliver Malware
- Endpoint Operations
- Reach the Target

Networks:
- Utility Corporate/Business Network
- Control Center
- Substation

**Layers**:
- IT
- OT

Palo Alto Networks Recommendation for ICS Security Best Practice
1: Aligning with Security Standard, Control or Framework (eg. NIST, CIS CSC.)
2. Applying with Zero-Trust Architecture Concept

- **Secure Access**: All resources are accessed in a secure manner regardless of location.

- **Access Restriction**: Access control is on a “need-to-know” basis and is strictly enforced.

- **Inspect & Log**: Inspect and log all traffic.

---

Appendix B: Relevant Team Biographies

**John Kindervag**

Principal Analyst Serving Security & Risk Professionals

John serves Security & Risk Professionals. He is a leading expert on wireless security, network security, security information management, and PCI data security. John leads research efforts for Forrester’s Data Security and Privacy and Security Architecture and Operations playbooks.
Zero-Trust Segmentation Gateway between Levels

- Access control
- Firewall
- Threat Prevention System
- Content Filtering
- Encrypt/Decrypt
- Packet forwarding
- Activity Monitoring
Breaking All Attack Kill-Chain As much As Possible

1. RECONNAISSANCE
   Harvesting email addresses, conference information, etc.

2. WEAPONIZATION
   Coupling exploit with backdoor into deliverable payload

3. DELIVERY
   Delivering weaponized bundle to the victim via email, web, USB, etc.

4. EXPLOITATION
   Exploiting a vulnerability to execute code on victim’s system

5. INSTALLATION
   Installing malware on the asset

6. COMMAND & CONTROL (C2)
   Command channel for remote manipulation of victim

7. ACTIONS ON OBJECTIVES
   With "Hands on Keyboard" access, intruders accomplish their original goals

Protect

Challenges in Segmenting ICS/SCADA Networks

- Production/System runtime requirements
- Protecting Legacy systems
- Controlling access to production networks from enterprise
- Necessary skill set resides in different department
- Complying with regulations
- Cost to implement
ISA 95/Purdue Model Levels

LEVEL 4
Business Logistics/Enterprise Services

LEVEL 3.5
DMZ or 3.5

LEVEL 3
Manufacturing Operations Systems
Control Systems
Intelligent Devices

LEVEL 2
Process

LEVEL 1

LEVEL 0
Zero Trust Segmentation based on Purdue Enterprise Reference Architecture
3. Applying Global Threat Intelligence for Automated Prevention

Network Sensors feed any new File, URL, C2, DNS insights – Exploits immediately blocked at endpoints

File & threat intel analysis & correlation yields instant PREVENTION – and artifacts for future threat analysis

Automated protection delivered in as little as minutes
4: Leveraging Machine Learning and AI to detect advanced threats automatically

Cyber Attack Kill Chain

Time Profile
- History, per Detector
- Network -> Application

Peer Profile
- Peer profile, per Detector

Entity Profile
- Entity Type
- User, admin, workstation, server, server type

Pre-Compute Learning

ML Technique

Less False Positive
SO, WHAT’S THE PROBLEM?
Siloed ‘point products’

Not integrated & automated

Manual Correlation!
Key Challenges

Security Skills Shortage

So Many Manual Integration

Increasing Complexity
Traditional Threat Detection Architecture cause massive time for Detection and Remediation

1. Need high security skill
   • Use case development and life cycle
   • SIEM Expert for manual correlation rules

2. Time to Triage and eliminate false positive
   • Manually integrate, validate and confirm alert with several log source and threat intelligence
   • Understand the chain of incident, root cause and impact
   • Lack of Trusted Threat intelligence source

Traditional Threat Detection Architecture cause massive time for Detection and Remediation

Skill Shortage
Too Many Tools
Long Time to Remediate
High CAPEX OPEX
Applying Machine Learning and AI Threat Detection Platform

Improve

1. Reduce OPEX cost (use case management, log normalization and rule correlation)
2. Reduce the alert and false positive
3. Reduce time to triage and root cause analysis with impact
4. Prioritize alerts for most critical incident
5. Proactively advanced threat detection & hunting
6. Reduce time to remediate impact

Response Challenges
1. Non-standard incident response workflow and playbook
2. Manual incident response operation with multiple teams
3. Slow time to contain threat and remediate impact
4. Lack of measurement
5. Lack of central knowledge based and lesson learn
5: Leveraging Security Orchestration and Automation Response Tools for Incident Response

Figure 3-1. Incident Response Life Cycle

Incident Response Challenges

What does a security team do?

- Study security data
- Manually follow security processes
- Collaborate with peers
- Manually investigate
- Manually take response and enforcement actions
- Measure performance
Applying Machine Learning and AI Threat Detection Platform

**Protect**
- Network
- Endpoint
- Cloud

**Detect**
- Threat intelligence
- Data Lake
- AI&ML

**Response**
- NW
- EndPoint
- IDM
- Server
- App
- Database

**Platform Sensors**
- 3rd Party Log

**SIEM**
- SOC Team

**Threat Alert!**
- Investigate & Response

**SOAR Platform**
- Collaboration
- Measurement
- Automated Workflow & Playbook
- Security Incident Ticketing

**Improvement**
1. Reduce OPEX cost (use case management, log normalization and rule correlation)
2. Reduce the alert and false positive
3. Reduce time to triage and root cause analysis with impact
4. Prioritize alerts for most critical incident
5. Proactively advanced threat detection & hunting
6. Reduce time to remediate impact

1. Reduce time to response, containment and eradicate the threats
2. Standardize security process and workflow with automation.
3. Orchestrate several security devices with automation (analyze & response).
4. Continuous measurement and improvement
**SUMMARY**

**Prevent**
Deploying Zero-Trust Architecture to reduce attack surface and prevent known and unknown threats.

**Automatically Detect**
Leveraging the Machine Learning and AI and Threat Intelligence for advanced threat detection analytic.

**Rapidly Investigate**
Lower operating costs by accelerating investigations and root cause analysis.

**Respond**
Leveraging SOAR technology for automated incident response process.

Align with Security Framework or Standard
Palo Alto Networks: Case Study
Protecting Utilities IT and OT infrastructure around the World
Case Study: Electric Transmission Data Network (NERC CIP)

Customer Profile
• Major N. American Utility (Regulated)

Challenges
• Meeting and exceeding NERC CIP regulatory requirements
• Improving visibility and segmentation within OT environments
• Rapidly detecting and stopping advanced threats
• Rising OPEX related to security administration across 2 control centers and 17 high-voltage transmission substations

Security
• Facilitate NERC CIP Compliance
• Layer-7 Visibility and Zero-trust segmentation
• Advanced Threat Prevention
• Advanced Threat Detection and Response
Case Study: Power Generation (Regulated)

Customer Profile
• Major N. American Electricity Generator operating multiple generation (Nuclear, Fossil, Renewable)

Challenges
• Minimal segmentation of IT & OT
• Endpoint security within Distributed Control System (DCS) ineffective at stopping advanced threats; required frequent, disruptive patching

Security
• Better visibility, control and threat prevention on the network with Zero-Trust architecture
• Advanced threat prevention (zero-day) capabilities
• Safer VPN access for remote users
Case Study: Australian Electricity Distribution

Customer Profile
- Electricity distributor, 200,000 kms of poles and wires with 1M customers (residential +commercial)

Challenges
- Poor visibility within OT
- Dumb firewalls, decentralized management
- No capabilities to detect and top advanced threats

Security
- Better visibility and control over traffic between business and OT and intra-OT with Zero-Trust segmentation
- More real time protections by leveraging global threat intelligence via AutoFocus
- Automated ingestion of 3rd party threat intelligence and translation to threat response/enforcement
- Advanced Threat Detection and Response
THANK YOU