Plant Safety and Industrial Control System Cyber Security
Andreas Agostin, Eaton Singapore
Industrial Network Specialist Asia Pacific, MTL Products
Introduction

- Deficits in refineries, petrochemical/chemical plants, power plants, and water treatment plants can **threaten** the **environment** and the **health** of employees and local residents, and may cause significant **financial damages**. In the event of an incident, downtime and loss of production can incur substantial added costs.

- Plant Safety is addressed in various ways
  - Physical security
  - Accident avoidance through mechanical safety protection
  - Accident avoidance through policies
  - Safety Systems
  - IT security
  - **OT (ICS) security**
Triton: hackers take out safety systems in 'watershed' attack on energy plant

Sophisticated malware halts operations at power station in
diolated attack that threatens to
turn back Iran's energy program.
## Well-known ICS Incidents caused by Malware

<table>
<thead>
<tr>
<th>Year</th>
<th>Malware name</th>
<th>Activity; Malware design</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>Night Dragon Operation</td>
<td>Espionage; Remote Access Trojan</td>
</tr>
<tr>
<td>2010</td>
<td>Stuxnet</td>
<td>Sabotage of Siemens PLC in Iran</td>
</tr>
<tr>
<td>2011</td>
<td>Duqu</td>
<td>Espionage; related to Stuxnet</td>
</tr>
<tr>
<td>2012</td>
<td>Flame</td>
<td>Espionage; related to Stuxnet</td>
</tr>
<tr>
<td>2012</td>
<td>Shamoon</td>
<td>Sabotage; wiped HDDs at Saudi Aramco</td>
</tr>
<tr>
<td>2014</td>
<td>Havex</td>
<td>Espionage; Remote Access Trojan targeting energy, aviation, pharmaceutical, defense, and petrochemical</td>
</tr>
<tr>
<td>2016</td>
<td>Industroyer</td>
<td>Sabotage; targeted Ukraine electr. substations</td>
</tr>
<tr>
<td>2018</td>
<td>TRITON</td>
<td>Sabotage; targeted SIS (Triconex) at petrochemical plant in Saudi Arabia</td>
</tr>
</tbody>
</table>
So what is the perimeter, the boundary?

Perimeter = Internet / Office network

(?)

Pan Pacific Hotel Singapore
7 December 2018
Typical infrastructure and its perimeters

- Firewall from Office Network to Internet
- Firewall between Plant Network and Office Network
- Plant Network with Data Servers
  - accessible from office network
  - two network cards (one for plant network, one for control network)
- Redundant control network
Equipment malfunction

"Data storm" blamed for nuclear-plant shutdown
Robert Lemos, SecurityFocus 2007-05-18

The U.S. House of Representative's Committee on Homeland Security called this week for the Nuclear Regulatory Commission (NRC) to further investigate the cause of excessive network traffic that shut down an Alabama nuclear plant.

During the incident, which happened last August at Unit 3 of the Browns Ferry nuclear power plant, operators manually shut down the reactor after two water recirculation pumps failed. The recirculation pumps control the flow of water through the reactor, and thus the power output of boiling-water reactors (BWRs) like Browns Ferry Unit 3. An investigation into the failure found that the controllers for the pumps locked up following a spike in data traffic -- referred to as a "data storm" in the NRC notice -- on the power plant's internal control system network. The deluge of data was apparently caused by a separate malfunctioning control device, known as a programmable logic controller (PLC).

"If you were to test any control systems that have any more than three or four (different) network-connected devices, they could be knocked over very easily."

Dale Peterson, CEO, DigitalBond

Vulnerabilities in equipment

Currently 275 vendors listed with over 1000 vulnerabilities

Source: https://ics-cert.us-cert.gov/advisories-by-vendor

Cisco issues critical warning after CIA WikiLeaks dump bares IOS security weakness

Cisco says vulnerability in 300 models of Catalyst switches

Possible causes for ICS incidents

- Malfunctioning equipment
- Sabotage
- Denial of service
- Unauthorised access
- Unauthorised actions by vendors
- Unintended employee actions
- Theft
- Natural or manmade disaster
- Application of security patches
- Misconfigured firewalls
- Viruses, Worms, Malware
Cyber Security Incident Types

- Human error
- Software or device flaw
- Malware infection
- Disgruntled Employee
- External Hacker

Source: Industrial Security Incident Database ISID (now: RISI)
Infrastructure Vulnerabilities

- Manifold attack patterns paired with various control system vulnerabilities result in a vulnerable infrastructure environment

- Hacker, Malware, Virus
- Misconfigured firewalls
- Control system vulnerabilities (e.g. bugs)
- Unauthorized connections, sabotage
- Infected remote support
- Malfunctioning equipment
- Accidental incidents
The Bastion Model is not enough
So what can be done?

Common practice to protect industrial control systems in critical infrastructure:

- Air Gaps / Sneakernet
- ‘Bastion’ model
- Defense-in-depth
1. Air Gap

Air Gaps:
- No physical connection between plant network and office network/internet
- Often, firewall mistaken as ‘isolation’
Air Gap Problems

Air Gaps:

"In our experience, in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the Enterprise network. On average, we see 11 direct connections between those networks and in some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise environment."

Air Gap
Problem: Sneakernet

Higher risk than network link, as no control about transported data
2. Bastion Model

Bastion Model:
- Rely on a central line of defense (typically a firewall)

Note:
- Typical infrastructure uses the ‘Bastion’ model
Bastion Model
Problem: Firewalls

Problems:
- 80% of firewalls misconfigured\(^1\)
- Common firewall flaws\(^2\):
  - passing Microsoft Windows networking packets
  - passing rservices (rlogin, rsh, and reexec)
  - having trusted hosts on the business LAN
  - Most common: not providing outbound data rules. This may allow an attacker who can sneak a payload onto any control system machine to call back out of the control system LAN to the business LAN or the Internet


Bastion Model
Problem: Perimeter

- Mis-configured firewalls
- Infected Laptops
- Unauthorized connections
- External / 3rd party Networks
- Remote Support
- Print Copy Fax
- Vulnerabilities
The solution

Common practice to protect industrial control systems in critical infrastructure:

- Air Gaps / Sneakernet
- ‘Bastion’ model
- Defense-in-depth
Defense-in-depth
IEC 62443: Zones (and Conduits)

- A core concept in the ANSI/ISA/IEC 62443 security standard is “Zones and Conduits”
- Defines segmentation inside the control system
  - Physical (if plant is not limited to local)
  - Logical / functional
- ICS networks divided into layers or zones based on control function
- Multiple separated zones manage that “defense in depth” strategy
3. Defense-in-depth

Defense-in-depth
ISA-62443 (former ISA-99) Structure

Foundational information such as concepts, models and terminology

Creating and maintaining an effective IACS security program

System design guidance, Defense-in-depth model

Assessment of cyber security tools, mitigation countermeasures technologies

https://www.isa.org/isa99/

= published
## Defense-in-depth
### IEC 62443 (TC65 WG10) Publications

<table>
<thead>
<tr>
<th>IEC TS 62443-1-1:2009</th>
<th>Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 62443-2-1:2010</td>
<td>Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program</td>
</tr>
<tr>
<td>IEC TR 62443-3-1:2009</td>
<td>Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems</td>
</tr>
<tr>
<td>IEC 62443-3-3:2013</td>
<td>Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels</td>
</tr>
<tr>
<td>IEC 62443-4-1:2018</td>
<td>Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements</td>
</tr>
</tbody>
</table>

Equivalent to ISA-62443 (formerly ISA 99) publications

[https://webstore.iec.ch/searchform&q=62443&FUZZY=0](https://webstore.iec.ch/searchform&q=62443&FUZZY=0)
Defense-in-depth
IEC 62443: Zones (and Conduits)

Security Zone Definition

- “Grouping of logical or physical assets that share common security requirements”
  (Source: ANSI/ISA-62443:2015)

- A zone has a clearly defined border (either logical or physical), which is the boundary between included and excluded elements

Example of physical Zones

- DCS
- 3rd party package
Defense-in-depth
IEC 62443: (Zones and) Conduits

Connecting the Zones

- Connections between the zones are called ‘conduits’, and these must have security controls to:
  - Control access to zones
  - Resist Denial of Service (DoS) attacks or the transfer of malware
  - Shield other network systems
  - Protect the integrity and confidentiality of network traffic

- Understand and manage all your conduits between zones, not just the obvious ones
Defense-in-depth
IEC 62443: (Zones and) Conduits

Conduits

- A path for the flow of data between two zones
  - can provide the security functions that allow different ones to communicate securely
  - Any communication between zones must have a conduit.

![Diagram showing DCS, 3rd party package, and conduit]
Typical Control Network Architecture
Typical Control Network Architecture
Applying Defense-in-depth to fully protect critical infrastructure
Zones & Conduits Provide Defense in Depth (IEC 62443)
Zones & Conduits Provide Defense in Depth (IEC 62443)
Zones & Conduits Provide Defense in Depth (IEC 62443)
Securing the plant

- Implements Defense-in-Depth concept with Zones and Conduits
- Deep Packet Inspection for vulnerable and critical protocols

We are not just another IT firewall:
- Designed to employ within process area
- Protects with firewall module that understands industrial protocols
- Enforcer modules offer deep packet inspection for most common industrial protocols
- Allows super-fine granularity to limit data access and data exchange
- Rule generation is fast and less likely to be prone to human error
Industrial solution, industrial protocols

- Knows all common industrial protocols, besides all common IT protocols
- Unknown or proprietary protocols can be added by user

We meet industrial requirements:
- No downtime as no configuration is required at deployment
- Avoids network changes by being IP free
- Designed for plant engineers who want to protect the process, rather than IT people who do not understand process requirements
- Rule generation from inside the event logger window
Low cost solution

We reduce costs by:

- Minimizing impact on the network structure, whether new or existing network
- Minimizing installation costs due to Zero Configuration
- Minimize startup time through TEST mode and simple rule generation
- New: fibre connection makes converters unnecessary

- Small unit matching the design principles of Zones and Conduits of IEC 62443
- Designed for use with process control equipment with demand for few protocols per unit
Current White Papers from DCS are based on Defense in Depth

“Yokogawa recommends a comprehensive approach based on the defense in depth strategy.”

“TAKE A DEFENSE-IN-DEPTH APPROACH”

Zones and conduits are built on the defense in depth concept. Defense in depth is the coordinated use of security countermeasures to protect the integrity of information assets in a network. Proper implementation of a defense in depth strategy involves the implementation of three steps. A summary is each step is provided below.
Conclusion

- Risks are constantly changing. Models that were appropriate in the past are no longer sufficient.
- IEC 62443 defines the cybersecurity lifecycle - a powerful framework used to secure IACS.
  - The cybersecurity lifecycle is a process consisting of assessment, establishing countermeasures, monitoring them, and maintaining (adjusting/improving) them.
  - One part of Defense-in-depth is technology, the others are policies and procedures.
→ Implement Defense-in-depth based on logical/functional Zones (segregation) and conduits (communication paths)
Thank you, Sponsors
Copyright

Copyright © 2017 FieldComm Group™
This document contains copyrighted material and may not be reproduced in any fashion without the written permission of the FieldComm Group™.

Trademark Information
FieldComm Group™, FOUNDATION™ Fieldbus, HART-IP™ and FDI™ are trademarks, and HART®, WirelessHART®, ROM® and SIF® are registered trademarks of FieldComm Group, Austin, Texas, USA.

Any use of these terms hereafter in this document, or in any document referenced by this document, implies the trademark/registered trademark. All other trademarks used in this or referenced documents are trademarks of their respective companies. For more information, contact FieldComm Group at the address below.

Attention: FieldComm Group President
FieldComm Group
9430 Research Blvd., Ste. 1-120
Austin, TX 78759, USA
Voice: (512) 792-2300
Fax: (512) 792-2310
http://www.fieldcommgroup.org

Intellectual Property Rights
The FieldComm Group (the Group) does not knowingly use or incorporate any information or data into the HART, FOUNDATION Fieldbus and FDI protocol standards, which the Group does not own or have lawful rights to use. Should the Group receive any notification regarding the existence of any conflicting private IPR, the Group will review the disclosure and either (A) determine there is no conflict; (B) resolve the conflict with the IPR owner; or (C) modify the standard to remove the conflicting requirement. In no case does the Group encourage implementers to infringe on any individual's or organization's IPR.