Process Control Networks
Secure Architecture Design
Robert Alston
Principle Lead Network and Security Consultant

Over 25 years network experience including design, implementation, troubleshooting and integration of firewalls, routers, switches and infrastructure. Robert has several certifications in the field of networks and security. (CISSP, Cisco CCNA, Cisco CCDA, Certified Unix Engineer (CUE), Control System Security –US Department of Homeland Security) and Robert also has a Six Sigma Green Belt. Robert is based in Duluth, Georgia USA.
Agenda

Secure Process Control Architecture

• Defining Secure Network Architecture
  – What is a secure network architecture
  – Why a secure network architecture
  – Who needs a secure network architecture

• Designing Secure Network Architecture
  – Defense in depth
  – Layers of security
  – Security levels
  – Zone and Conduit Models
  – Building Blocks

• Questions & Answers
Defining Secure Network Architecture
What Is a secure Network Architecture?

• Controlled Access

• Defined security zones

• Layered levels of security

• Highly available (Redundancy)
Why a secure network architecture?

- Compliance and Regulation
- Targeted Attacks
- Open Systems
- Risks associated with breach
Who needs a secure network architecture?

• Critical Infrastructure
• Regulated Industries
• Manufacturing
• Businesses that depend on Process Systems
Designing Secure Network Architecture
Defense in depth

Defense in depth approach provides layers of security to protect critical assets

- Multiple protection mechanisms
- Layers of protection
- Resilient to attack
Layers of security

• Physical
  – Gates, locks, doors, etc.

• Electronic
  – Biometric, proximity, etc.

• Cyber
  – Firewalls, IDS/IPS, Access-lists, etc.

• Process control
  – Application access, role-based access, etc.
• SAL 1 – PROTECTION AGAINST CASUAL OR COINCIDENTAL VIOLATION (I.e. changing a setpoint to a value outside engineering defined conditions, interception of a password send over the network in clear text.)

• SAL 2 – PROTECTION AGAINST INTENTIONAL VIOLATION USING SIMPLE MEANS (I.e. virus infection, exploiting commonly known vulnerabilities of DMZ hosts)

• SAL 3 – PROTECTION AGAINST INTENTIONAL VIOLATION USING SOPHISTICATED MEANS (I.e. exploits in operating systems, protocols. Attacker requires advanced security knowledge, advanced domain knowledge, advanced knowledge of the target system. I.e. password cracking.)

• SAL 4 – PROTECTION AGAINST INTENTIONAL VIOLATION USING SOPHISTICATED MEANS WITH EXTENDED RESOURCES (Similar to SAL 3 but attacker now has extended resources to their disposal. I.e. StuxNet attack)
Manufacturing automation architecture

- **ISA95 functional hierarchical model**

  **Level 4**
  - **Business Planning & Logistics**
    - Plant Production Scheduling, Operational Management, etc.
  
  - **Time Frame**
    - Months, weeks, days

  - **Level 3**
    - **Manufacturing Operations Management**
      - Dispatching Production, Detailed Production Scheduling, Reliability Assurance, etc.
  
  - **Level 2**
    - **Batch Control**
    - **Continuous Control**
    - **Discrete Control**
  
  - **Level 1**
    - **Level 0**
      - **Time Frame**
        - Days, Shifts, hours, minutes, seconds

  - **Level 0**
    - The actual production process

  - **Time Frame**
    - Hours, minutes, seconds, subseconds

  - **Level 4**
    - Establishing the basic plant schedule - production, material use, delivery, and shipping. Determining inventory levels.

  - **Level 3**
    - Work flow / recipe control to produce the desired end products. Maintaining records and optimizing the production process.

  - **Level 2**
    - Monitoring, supervisory control and automated control of the production process.

  - **Level 1**
    - Sensing the production process, manipulating the production process.
Typical PCS Network Topology

Level 4
- Enterprise Switch
- Firewall
- Terminal Server
- Patch Mgmt Server
- Anti Virus Server
- eServer
- PHD Shadow Server
- L4 to L4
- Limited L3.5 to L3.5
- Very Limited L3 to L3
- Limited L2 to L2
- No Direct communications between L1 & L3 or L4

Level 3.5 DMZ
- Domain Controller
- ESF
- PHD Server
- Experion Server
- EAS
- 3RD Party App
- Subsystem Interface
- L3 to L3 Limited
- Very Limited L2 to L2
- Limited L2 to L2
- No communication between L1 & L3 or L4

Level 3
- Router
- Optional HSRP Router
- ESC
- ESF
- ACE
- Experion Server
- EST
- ESET
- Safety Manager
- Terminal Server
- Domain Controller

Level 2
- Qualified Cisco Switches

Level 1
- L1 to L1
Security levels

- **Level 1** - Controllers and real time control
- Level 2 – Servers, Operator Stations and supervisory control.
- Level 3 - Historians and Advanced Control and other Level 2 areas or units.
- Level 3.5 - DMZ accessed from the Business Network and the PCN.
- Level 4 - Is the business network with clients for Historians or Advanced Control applications.
- Level 3 and 3.5 utilizes standard open systems Ethernet technology and Level 4 utilizes standard open systems LAN technology.
Level 4

- Is the business network with clients for Historians or Advanced Control applications.
- Untrusted Network
- Separated by a firewall
- No direct connection to Level 3 or below
- Managed by Business IT department
- Level 4 utilizes standard open systems LAN technology.
Level 3.5

- Level 3.5

  - Is commonly called the DMZ

  - Typical nodes WSUS, Anti-Virus Server, Terminal Server, etc.

  - Provides connectivity for devices that are to be accessed from the Business Network and the PCN.

  - Security zone between the PCN and outside networks

  - Can be redundant, but not FTE capable
Level 3.5

Comm flow
- L4 to L4
- Limited L3.5 to L3.5
- Very Limited L3 to L3
- Limited L2 to L2
- Very Limited L1 to L1
- No Direct communications between L1 & L3 or L2
- No communications between L1 & L4 or L3
Level 3

- Level 3
  - Connections for Historians and Advanced Control
  - Routing
  - Access List control
  - connect other Level 2 areas or units
  - Can be redundant, but not FTE capable
  - HSRP
Level 2

- Level 2
  - Connections for Servers and Operator Stations
  - Supervisory control
  - Connection to Level 1
  - Protection for Level 1 with access lists
  - FTE capable
Level 1

- Controllers and real time control
- Controllers and Console Stations.
- FTE Bridge (FTEB) or C300
- Protected by all other levels
Example – Zones and conduits
The IACS shall employ malicious code protection mechanisms.

1. Malicious code protection mechanisms shall be employed at workstations, servers, or mobile computing devices on the network.

2. Malicious code protection mechanisms shall be employed at critical entry and exit points (e.g., firewalls, web servers, proxy servers, remote-access servers).

- Central virus protection management server providing updated virus signatures for Honeywell approved engines at the servers and stations
- McAfee – sPolicy Orchestrator Symantec/Norton

Network access control managing inside devices for their security posture and enforcing updates if required.

Cisco NAC (Clean Access Appliances) (Cisco Security Agent)

Threat protection by anti-virus / content filtering at the firewall

ASA 5500 series firewall (Cisco CSC)

Protection Shield

- Threat protection by providing a Shield around the equipment that filters on vulnerabilities (virtual patching) and malware.
- Tipping Point IPS (Virtual patching)

White listing

- Inspection for abnormal behavior, change control, and data integrity

FUTURE (Being investigated)

Testing of DAT files before multi-stage deployment of the DAT file in the process control system

Honeywell Life Cycle Services (Service Node)
Additional security boundaries

L4 – Enterprise network

L3.5 – Demilitarized zone

Local Access to business applications L3.5.1
Remote access and system management L3.5.2

Site wide MES L3.2

PE1
Site specific MES L3.1
CCR L2.1
Sub-station A L2.2
LCN1 L2.3

PE2
Site specific MES L3.1
CCR L2.1
Sub-station A L2.2
LCN1 L2.3

L3 – Process Information Network

Process Control Domain

External security boundary

Internal security boundary
Security planning and Functional design
Thank you

www.honeywell.com/ps