CT392 - Industrial Demilitarized Zone Design Principles
Agenda

Fundamentals and Review

What is an IDMZ?

Methodology

Network Segmentation
Fundamentals and Review
Purdue Reference Model

- MES - Manufacturing Execution System measures and controls production facilities; it tracks and measures key operational criteria such as product, equipment, labor, inventory, defects, etc.; a key interface to the Enterprise-level applications; **Level 3 & 4**
- Historian - Collects historical data from the plant floor applications and reports or displays them in various report formats; **Level 3**
- SCADA - Supervisory Control and Data Acquisition; large scale distributed measurement and control systems, usually covers a geographical area; **Level 3**
- HMI - Human Machine Interfaces display operational status to operation personnel and may allow them to perform basic functions (e.g. start/stop a process); **Level 2**
- Programmable Automation Controller or Programmable Logic Controller; controls a subset (Cell/Area), e.g. a line or function, as well as the relevant devices in that Cell/Area; **Level 1**
- Sensor/Actuator device - a device that measures or controls key functions or aspects of the industrial automation process; **Level 0**
Campus Network Diagram to Ground 
Our Conversation

- Hierarchical, modular and scalable building blocks
- Creates small domains - clear demarcations and segmentation
  - Fault domain (e.g. Layer 2 loops), broadcast domain, domains of trust (security)
- Easier to grow, understand and troubleshoot
- Multi-tier switch model
  - Core
    - Aggregates distribution switches
    - Backbone of network
    - Industrial DMZ connectivity
  - Distribution
    - Aggregates access switches
    - Provides Layer 3 services
  - Access
    - Aggregates industrial automation and control system (IACS) devices
    - Provides Layer 2 services
Go Beyond Defense in Depth

- SearchSecurity.com defines “Defense in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier.”

For example, this fundamental need for layered protections is captured in the “Defense-in-Depth” strategy being used by DoD for protecting information systems. A source of information on implementing layered protections is the Information Assurance Technical Framework (IATF, http://www.iatf.net/). The IATF advocates the use of multiple information technology protection.


A fundamental principle that must be part of any network protection strategy is defense-in-depth. Defense-in-depth must be considered early in the design phase of the development process, and must be an integral consideration in all technical decision-making associated with the network. Utilize technical and administrative controls to mitigate threats from identified risks to as great a degree as possible at all levels of the network. Single
Industrial Network Convergence
Continuing Trend

Traditional – 3 Tier Industrial Network Model

EtherNet/IP - Enabling/Driving Convergence of Control and Information

Converged Plantwide EtherNet/IP Industrial Network Model
Industrial Network Convergence
Continued Trend – Industrial Demilitarized Zone (IDMZ)

Wide Area Network (WAN)
- Physical or Virtualized Servers
  - ERP, Email
  - Active Directory (AD), AAA – Radius
  - Call Manager

Office Applications, Internetworking, Data Servers, Storage

Enterprise Security Zone

Physical or Virtualized Servers
- Firewall for separation
- Unified Threat Management
- Authentication & Authorization
- Application & Data Sharing via replication or terminal services

Industrial DMZ

- Gbps Link for Failover Detection
- Firewalls (Active)
- Firewalls (Standby)

Physical or Virtualized Servers
- FactoryTalk Application Servers & Services Platform
- Network Services – e.g. DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

Plant-wide / Site-wide Network
Integrated Architecture
What is an Industrial DMZ?

- A IDMZ, or Industrial Demilitarized Zone, is a sub-network placed between a trusted network (industrial) and an untrusted network (enterprise). The IDMZ contains business facing assets that act as brokers between the trusted and untrusted networks.
- Traffic never travels directly across the IDMZ.
- A properly designed IDMZ can be unplugged if compromised and still allow the industrial network to operate without disruption.
Demilitarized Zone (DMZ)

- Sometimes referred to a perimeter network that exposes an organization's external services to an untrusted network. The purpose of the DMZ is to add an additional layer of security to the trusted network.
Industrial Demilitarized Zone (IDMZ)
Controlling Access to the Industrial Zone

- Sometimes referred to a perimeter network that exposes an organization's external services to an untrusted network. The purpose of the IDMZ is to add an additional layer of security to the trusted network.

Enterprise Security Zone

Industrial DMZ

Industrial Security Zone

TRUSTED?
UNTRUSTED?

BROKER
Industrial Demilitarized Zone (IDMZ)

Controlling Access to the Industrial Zone

- All network traffic from either side of the IDMZ terminates in the IDMZ; network traffic does not directly traverse the IDMZ
  - Only path between zones
  - No common protocols in each logical firewall
- No control traffic into the IDMZ, CIP stays home
- No primary services are permanently housed in the IDMZ
- IDMZ shall not permanently house data
- Application data mirror to move data into and out of the Industrial Zone
- Limit outbound connections from the IDMZ
- Be prepared to “turn-off” access via the firewall
Set-up functional sub-zones in the IDMZ to segment access to data and services (e.g. Partner zone, Operations, IT).
Controlling Access to the Industrial Zone

Logical Model – Industrial Automation and Control System (IACS)
Converged Multi-discipline Industrial Network
No Direct Traffic Flow between Enterprise and Industrial Zone
Agenda

- Fundamentals and Review
- What is an IDMZ?
- Methodology
- Network Segmentation
Methodology

A methodology is usually a guideline system for solving a problem, with specific components such as phases, tasks, methods, techniques and tools.\cite{1} It can be defined also as follows:

1. "the analysis of the principles of methods, rules, and postulates employed by a discipline";\cite{2}
2. "the systematic study of methods that are, can be, or have been applied within a discipline";\cite{2}
3. "the study or description of methods".\cite{3}

- Develop a scientific method to develop repeatable, measureable and maintainable solution(s)

- Look at the problem “holistically” and drill down to each system
IDMZ / Network Reconnaissance (Design Pre-work)

**Identify “types” of Assets in Industrial Zone and those that support Manufacturing**

**Identify “who” owns the hardware and software on the asset.**

**Recon Phase**
- Identify Assets Or Asset Classes
  - ACTION: Document Assets by documentation, interviews and network scanning
- Identify Asset Owners
  - ACTION: Document Asset Owners and Schedule Interviews

**Design Phase**
- Requirements Phase
- Architectural Phase
- Tech. Design Phase
- Implement
- Maintain
Classify Asset Types

Goal: Identify assets that support manufacturing process.
Goal: Identify if asset belongs in the Industrial or Enterprise Zone.
Diagram Data Sources Feeding Higher Level Assets

Industrial Security Zone

- Reporting Server
- MES Server
- Domain Controller
- Historian Server
- HMI Server
- Quality Control Server
- IACS Domain Controller
- IACS Server
- Engineering Workstations
- Historian Server

IACS Controls

IACS Databases
Identify System Owners / Users
Interview Process

- Interview process identifies how the owners and clients of the assets
  - Operate
  - Configure
  - Patch
  - Upgrade
- Identifies where the data is produced and consumed
- This process is used to gather requirements
## IDMZ / Network Design Methodology

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirements Phase</strong></td>
<td>Interview all system owners to gather requirements for operations, configuration and maintenance.</td>
</tr>
<tr>
<td><strong>Architectural Phase</strong></td>
<td>Produce high level documentation and drawings to meet every requirement.</td>
</tr>
<tr>
<td><strong>Technical Design Phase</strong></td>
<td>Produce detailed documentation such as drawings, switch configurations, VLAN, IP Address, Firewall ACL’s.</td>
</tr>
<tr>
<td><strong>Implementation</strong></td>
<td>Verify, “was the product built right” and Validate, “was the right product built” process.</td>
</tr>
<tr>
<td><strong>Maintain</strong></td>
<td>Modify configurations and assets to fix anomalies or required operational changes.</td>
</tr>
</tbody>
</table>

**Requirements**

Requirements are a statement identifying a capability, physical characteristic or quality factor that bounds a product or process problem for which a solution will be pursued. (Source: IEEE Standard 1220-1994)

**Architectural Phase**

High level architectural recommendations that are proposed to meet the customer requirements.

**Technical Design Phase**

Detailed information usually written by the coder or implementer that describes how the system or product will be programmed, configured to meet the customer requirements and the high level architecture.

**Implementation**

The system components are brought together and tested during this phase per the testing plan.

**Maintain**

System has been Verified and Validated and is maintained by Operations and Maintenance.
High Level Architecture

Enterprise Security Zone

Industrial DMZ

Industrial Security Zone

- Reporting Server
- Domain Controller
- Historian Server
- MES Server
- HMI Server
- Quality Control Server
- IACS Domain Controller
- IACS Server
- Engineering Workstations
- Historian Server
How to Derive High Level Architecture

No Control Protocols Through the Firewall(s)
Move the Assets Around To Minimize Cross Zone Traffic – Especially Control Protocols
High Level Architecture – Review All Use Cases and Meet All Requirements

Use Case – Configure Historian from Enterprise

Enterprise Security Zone

Industrial DMZ

Industrial Security Zone

- Reporting Server
- Domain Controller
- Historian Server
- Historian Owner
- Remote Desktop Gateway
- HMI Server
- Quality Control Server
- IACS Domain Controller
- IACS Server
- Engineering Workstations
- Historian Server
- MES Server
High Level Architecture – Review Use Cases

Use Case – Move Data From Industrial Historian to Enterprise Historian

Enterprise Security Zone

Industrial DMZ

Industrial Security Zone

Reporting Server

Domain Controller

Historian Server

Historian Owner

Use Case – Move Data From Industrial Historian to Enterprise Historian

MES Server

Historian Mirror

HMI Server

Quality Control Server

IACS Domain Controller

IACS Server

Engineering Workstations

Historian Server
Assets Typically Found in Industrial DMZs

Level 5
- Terminal Services
- Patch Management
- AV Server
- Web Services Operations
- File Transfer Server

Level 4
- Historian Mirror
- Enterprise Network

Level 3
- FactoryTalk Application Server
- FactoryTalk Directory
- Engineering Workstation
- Domain Controller
- Site Manufacturing Operations and Control

Level 2
- FactoryTalk Client
- Operator Interface
- Engineering Workstation
- Operator Interface

Level 1
- Batch Control
- Discrete Control
- Drive Control
- Continuous Process Control
- Safety Control

Level 0
- Sensors
- Drives
- Actuators
- Robots
- Process Control
- Basic Control
- Cell/Area Zone

Remote Access Technologies
- Remote Access Technologies

Enterprise Zone
- Enterprise Network
- Site Business Planning and Logistics Network

IDMZ
- Web E-Mail CIP
- IDMZ

Rockwell Automation
Assets Typically Found in Industrial DMZs

**Level 5**
- Router
- Enterprise Network

**Level 4**
- E-Mail, Intranet, etc.
- Site Business Planning and Logistics Network

**Windows Server Updating Service (WSUS)**
- Terminal Services
- Patch Management
- Historian Mirror
- Web Services Operations
- File Transfer Server

**Enterprise Zone**

**IDMZ**

**Level 3**
- FactoryTalk Application Server
- FactoryTalk Directory
- Engineering Workstation
- Domain Controller

**Level 2**
- FactoryTalk Client
- Operator Interface

**Level 1**
- Batch Control
- Discrete Control
- Drive Control
- Continuous Process Control
- Safety Control

**Level 0**
- Sensors
- Drives
- Actuators
- Robots

**Industrial Zone**

**Cell/Area Zone**

**Process**
## IDMZ / Network Design Methodology

### Requirements Phase

Requirements are a statement identifying a capability, physical characteristic or quality factor that bounds a product or process problem for which a solution will be pursued. (Source: IEEE Standard 1220-1994)

**ACTION**

Interview all system owners to gather requirements for operations, configuration and maintenance.

### Architectural Phase

High level architectural recommendations that are proposed to meet the customer requirements.

**ACTION**

Produce high level documentation and drawings to meet every requirement.

### Technical Design Phase

Detailed information usually written by the coder or implementer that describes how the system or product will be programmed, configured to meet the customer requirements and the high level architecture.

**ACTION**

Produce detailed documentation such as drawings, switch configurations, VLAN, IP Address, Firewall ACL's.

### Implementation

The system components are brought together and tested during this phase per the testing plan.

**ACTION**

Verify, “was the product built right” and Validate, “was the right product built” process.

### Maintain

System has been Verified and Validated and is maintained by Operations and Maintenance.

**ACTION**

Modify configurations and assets to fix anomalies or required operational changes.
Agenda

Fundamentals and Review

What is an IDMZ?

Methodology

Network Segmentation
Industrial Zone - Architecture to support IDMZ

- Division of plant-wide / site-wide architectures into functional areas for secured access
  - ISA-99 “Zones and Conduit” model
- OEM’s Participation
  - IP Address
  - VLAN ID’s
  - Access layer to Distribution layer cooperation
- System design requires full cooperation of all System Integrators, OEM’s, IT and Plant/Site Engineering

Zones and Conduits

Copyright © 2013 Rockwell Automation, Inc. All Rights Reserved.
Data Link / Network Layers

Control Systems are Designed with Availability Requirement First!

Layer 2 Access Link
Layer 2 Interswitch Link/802.1Q Trunk
Layer 3 Link

Enterprise Zone Levels 4 and 5
Industrial Demilitarized Zone (IDMZ)

Industrial Zone Site Operations and Control Level 3

Cell/Area Zones Levels 0–2

VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 41
VLAN 42
VLAN 43
VLAN 44
VLAN 45

Security
Integrity
Availability
Confidentiality

Layer 3 Link

VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 41
VLAN 42
VLAN 43
VLAN 44
VLAN 45
The Cell/Area zone is a Layer 2 network for a functional area (plant-wide or site-wide). Key network considerations include:

- Structure and hierarchy using smaller Layer 2 building blocks
- Logical segmentation for traffic management and policy enforcement (e.g. QoS, Security) to accommodate time-sensitive applications
Questions?