Engineering Standard

SAES-T-566 9 April 2018

Plants Demilitarized Zone (DMZ) Architecture

Document Responsibility: Plants Networks Standards Committee

Contents

Contact: Ghamdi, Khalid Sulaiman (ghamks0b) @ phone +966-13-8801354

1 Scope

This standard defines the minimum mandatory requirements governing the design, installation, configuration, and commissioning of Saudi Aramco plant Demilitarized Zone (DMZ) Architecture. The DMZ shall establish an intermediate network between the Saudi Aramco Process Automation Network (PAN) and Saudi Aramco Corporate Network to provide security protection for the Saudi Aramco Industrial Control Systems (ICS) in accordance with IEC 62443-3-3 guidelines.

2 Conflicts and Deviations

2.1 Any conflicts between this document and other applicable Mandatory Saudi Aramco Engineering Requirements (MSAERs) shall be addressed to the EK&RD Coordinator.

2.2 Any deviation from the requirements herein shall follow internal company procedure SAEP-302.

3 References

3.1 Saudi Aramco References

Saudi Aramco Engineering Procedures

SAEP-99	*Process Automation Networks and Systems Security*
SAEP-302	*Instructions for Obtaining a Waiver of a Mandatory Saudi Aramco Engineering Requirement*
SAEP-707	*Risk Assessment Procedure for Plant Networks and Systems*

Saudi Aramco Engineering Standards

SAES-T-916	*Telecommunications: Building Cable Systems, Pathways, and Spaces*
SAES-Z-010	*Process Automation Network*

Saudi Aramco Engineering Reports

SAER-6123	*Process Automation Networks Firewall Evaluation Criteria*
SAER-8143	*Plants' Network Bandwidth Connectivity Study*

3.2 Industry Codes and Standards

IEC 62443-3-3	*Industrial Communication Networks - Network and System Security - Part 3-3: System Security Requirements and Security Levels*

4 Definitions

Demilitarized Zone (DMZ): A network installed as a "neutral zone" between a two networks with different security levels that require exchanging information. The DMZ network prevents information and network traffic from passing directly between the two networks; in Saudi Aramco's case, between the Corporate Network and the PAN.

Hardware-based Isolation Device: This device is utilized to isolate key control systems from front-office computers. It enforces unidirectional and/or bidirectional network communications from more secure zone to the less secure zone of the security architecture perimeters.

Firewall: An inter-network connection device that controls data communication traffic between two or more connected networks.

Local Area Network (LAN): A private data communications network, used for transferring data among computers and peripherals devices; a data communications network consisting of host computers or other equipment interconnected to terminal devices.

Logs: Files or prints of information in chronological order.

Plant Information (PI) System: It is an enterprise application software or Data Acquisition and Historization System (DAHS) used for management of real-time of process data and events

Process Automation Network (PAN): A plant wide network interconnecting Process Control Systems (PCS) that provides an interface to, and be protected by the DMZ.

System-integrity-key: Is a one-way 32 digit hexadecimal hash key generated by cryptographic hash function based on device configuration. It is used by the system to protect the configuration changes integrity and validity from authorized sources.

Abbreviations:

AV	Anti-Virus
CCR	Central Control Room
DCS	Distributed Control Systems
DMZ	Demilitarized Zone

PAN	Process Automation Network
PSA	Power System Automation
SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous Digital Hierarchy
SSH	Secure Shell Protocol

5 DMZ Architecture Design

5.1 Each Saudi Aramco plant facility shall implement a DMZ at their network boundaries with Corporate Network.

Commentary Notes:

Plants comprising of multiple scattered (PANs) or small consolidated facilities is recommended to interface with the Corporate Network via a centralized DMZ network model.

To ensure proper implementation meeting the objective of DMZ, risk assessment is recommended to be conducted prior to the implementation, per SAEP-99 and SAEP-707.

5.2 DMZ network shall comply with IEEE 802.3 CSMA/CD (Ethernet) standard.

5.3 DMZ components shall be installed in the plant operating facility premises as close as practical to the PAN in locations such as CCR, Telecommunications/ Computer/ Rack room(s), in accordance with SAEP-99 requirements.

5.4 All Plant Systems and applications that are required to communicate with the Corporate Network (such as Plant Information (PI)) shall be hosted in the DMZ either by relocation or provision of a replica server.

5.5 DMZ network shall include the following components:

- Layer 3 switch, with network management capabilities, if needed.
- Two firewalls (plant firewall and IT firewall), with network management capabilities.
- Server hardware to host:
  - PI server/s for sharing plant data with corporate users.
  - Security management services such as automatic AV update, patch update management, if applicable.
  - TMS/SAP interface/s, if needed.
  - Plant support applications, if needed.

- Approved security applications such as: compliance tool, monitoring tool, NMS tool, etc.

Commentary Note:

Two redundant firewalls shall be considered when high availability of critical facilities is required. The criticality of the facility shall be determined by the proponent business case.

5.6 All default passwords for predefined accounts of all DMZ components shall be changed immediately after installation or upgrade.

5.7 All User ID formats shall conform to corporate guidelines.

5.8 All nodes on the DMZ shall be assigned static IP addresses

5.9 The DMZ subnet shall be different from corporate and plant subnets. Subnet IP address and network mask shall be obtained from Saudi Aramco IT.

5.10 DMZ components shall be deployed with the latest vendor supported security hardened operating system (i.e., apply patches, disable USB port, disable unnecessary services/tasks) in accordance with SAEP-99 and relevant Saudi Aramco security guidelines.

5.11 DMZ network equipment unused physical ports/interfaces shall be disabled.

5.12 DMZ components shall be fully interoperable with plant PAN and Corporate Network. It is recommended to align DMZ components with IT purchase agreements and maintenance contracts.

A sample of the logical DMZ model is illustrated in Figure 1.

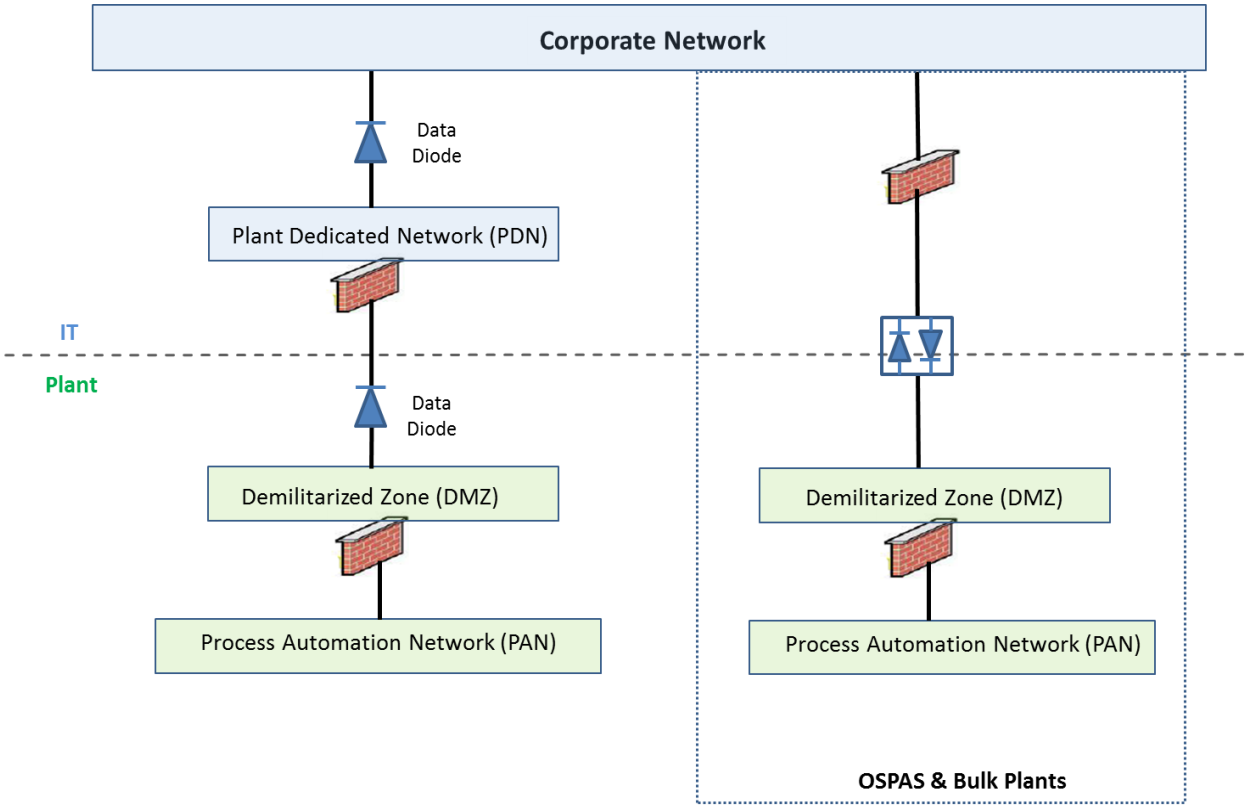

Figure 1 – Sample Logical DMZ Model Diagram

5.13 Each Saudi Aramco production plant facility shall implement the hardware-based isolation device with unidirectional network communication from Industrial Control Systems (ICS) network to Business network.

5.14 Each Saudi Aramco Bulk Plant and OSPAS shall implement the hardware-based isolation device with bidirectional network communication from Industrial Control Systems (ICS) network to Business network.

5.15 The hardware-based isolation device for plant facility shall be installed inside the DMZ and before IT firewall.

5.16 Hardware-based isolation device shall require system-integrity-key to secure device configurations. A new system-integrity-key may be generated during configuration updates or system access. The device configuration along with the system-integrity-key shall be exported to an external media (such as CD or certified flash memory) and kept in secure place with Central Control Room

operations supervisor. Some Hardware-based isolation device may not work without a valid system-integrity-key.

6 Firewalls Filtering, Blocking, and Access Control

6.1 DMZ firewall(s) shall be configured to prevent network traffic from passing directly between the Corporate Network and PAN. All Traffic from either side shall terminate at the DMZ zone.

6.2 Firewall(s) shall be configured to deny all access unless specifically permitted.

6.3 Firewall(s) filter rules shall allow only approved secure services and protocols. Insecure services and clear text protocols such as Telnet and FTP shall not be used.

6.4 Enable Security logging for traffic monitoring and intrusion detection for all DMZ components. All systems security logs shall be stored in a central location.

6.5 Intrusion Prevention functionalities shall be installed on IT firewalls as a minimum.

6.6 The filtering mechanism shall be based on, as a minimum, source/destination IP addresses and TCP/UDP ports.

6.7 Network equipment including firewalls and network devices shall be managed by predefined facility support staff through secure ports such as SSH.

6.8 SAER-6123, "Process Automation Networks Firewall Evaluation Criteria" provides additional guidelines for firewall configuration and hardware selection.

6.9 SAER-8143, "Plants' Network Bandwidth Connectivity Study" provides additional guidelines for plant connectivity bandwidth requirements.

7 Cabling Distribution Design

Premises distribution methods for cables and cabinets shall comply with SAES-T-916.

8 Backup and Recovery

A complete configuration backup of DMZ switches and systems shall be developed for new installations or upgrades of DMZ equipment per SAES-Z-010 requirements and guidelines.

9 System Testing

Formal testing procedure shall be developed by the execution agency/proponent to ensure proper DMZ configuration and installation. This shall include all hardware and software installed in the relevant plant to ensure secure communication between all plant system/applications.

10 Documentation

Comprehensive documentation shall be provided to ensure that the DMZ is installed and configured in a consistent manner. It shall include detailed layouts of IP addressing schemes and all other network protocols used in DMZ. The documentation shall also include physical locations of DMZ components such as firewalls, switches, and servers. The following shall be provided:

10.1 Standard vendor manuals and catalogs shall be provided in CD-ROM or other electronic media. Formats shall be in PDF or HTML.

10.2 Equipment configuration data bases in Microsoft Excel or Access.

10.3 Final project specific documents in two signed hard copies plus two (2) sets of CD-ROM in Microsoft Word.

10.4 A DMZ network drawings layout showing the DMZ logical and physical design and its interconnection to the Corporate Network.

10.5 For all plant applications that need to traverse plant firewalls, the vendors shall provide application flow diagram that shows inter-path connections and traffic characteristics to the plant administration. These diagrams are required to support the following objectives:

- Expedite mission critical troubleshooting
- Ensure security by verifying that only the required traffic flow is allowed.

Revision Summary

9 April 2018	Major revision to meet revision cycle and continue to align with Saudi Aramco cyber security requirements.