Engineering Standard

SAES-T-566 17 March 2013

Plant Demilitarized Zone (DMZ) Architecture

Document Responsibility: Communications Standards Committee

Saudi Aramco DeskTop Standards

Table of Contents

Previous Issue: New Next Planned Update: 17 March 2018

Primary contacts: Harbi, Saad Abdullah on +966-3-8801360 and
Ghamdi, Khalid Sulaiman +966-3-880-1354

1 Scope

This standard defines the minimum mandatory requirements governing the design, installation, configuration, and commissioning of Saudi Aramco plant Demilitarized Zone (DMZ) Architecture, which 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 plants networks and systems (PN&S).

2 Conflicts and Deviations

2.1 Any conflicts between this standard and other applicable Saudi Aramco Materials System Specifications (SAMSSs), Engineering Standards (SAESs), Engineering Procedures (SAEPs), Standard Drawings (SASDs), or other Mandatory Saudi Aramco Engineering Requirements (MSAERs) shall be resolved in writing by the Company or Buyer Representative through the Chairman, Communications Standards Committee, Process & Control Systems Department, Dhahran.

2.2 Direct all requests to deviate from this standard in writing to the Company or Buyer Representative, who shall follow internal company procedure SAEP-302 and forward such requests to the Manager, Process & Control Systems Department of Saudi Aramco, Dhahran.

3 References

3.1 Saudi Aramco References

Saudi Aramco Engineering Procedures

SAEP-99	*Process Automation Networks & 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*
SAEP-1050	*Guideline for Disaster Recovery Plan Development for Process Automation Systems*

Saudi Aramco Engineering Standards

SAES-P-126	*Power System Automation*
SAES-T-916	*Communications Building Cable*

SAES-Z-010 *Process Automation Network*

Saudi Aramco Materials System Specification

23-SAMSS-072 *Data Acquisition and Historization System (DAHS)*

Saudi Aramco Engineering Report

SAER-6123 *Process Automation Networks Firewall Evaluation Criteria*

Saudi Aramco Information Protection Manual (IPM)

IPSAG-007 *Computer Accounts Security Standards & Guidelines*

3.2 Industry Codes and Standards

Institute of Electrical and Electronics Engineers, Inc.

IEEE 802.3 *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*

4 Definitions

Backbone: A network configuration that connects various LANs together into an integrated network. In a Plant-wide network, that part of the network whose primary function is to forward data packets between the other smaller networks.

Demilitarized Zone (DMZ): A network installed as a "neutral zone" between a two networks with different security levels that require to exchange 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.

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

L2 Switch: A network device that joins multiple computers together at layer two (Data Link Layer) of the Open System Interconnection (OSI) model.

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.

Physical Separation: Physical separation is indicated by the comprehensive isolation of network assets such as switches, medium and housing cabinets to achieve highest level of security.

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, for more details please refer to 23-SAMSS-072.

PI-to-PI Interface: It is a software that transfers data from one PI server (the source server) to another PI server (the receiving server) via TCP/IP.

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

Server: A server is a dedicated un-manned data provider.

Virtual Private Network (VPN): A private communications network existing within a shared or public network platform (i.e., the Internet).

Abbreviations:

AV	Anti-Virus
CCR	Central Control Room
CMS	Condition Monitoring System
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
DCS	Distributed Control Systems
DMZ	Demilitarized Zone
IP	Internet Protocol
IT	Saudi Aramco Information Technology
LAN	Local Area Network
PAN	Process Automation Network
PMS	Power Monitoring System
PSA	Power System Automation
SCADA	Supervisory Control and Data Acquisition
TCP	Transmission Control Protocol
SDH	Synchronous Digital Hierarchy
SSH	Secure Shell Protocol
VLAN	Virtual Local Area Network

VMS Vibration Monitoring System

VPN Virtual Private Network

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. Consolidated PANs with centralized DMZ design shall be submitted to P&CSD for review and approval.

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, but not limited to, Plant Information (PI), Anti-Virus (AV), Windows Server Update Services (WSUS) and proxy server for Vibration Monitoring System (VMS) and Power System Automation (PSA) remote access 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 2 switch
- Two firewalls
- Server hardware to host:
  - Plant applications that are to be shared with Corporate users
  - Security management services such as automatic AV update, patch update management and proxy, if applicable.

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 DMZ components (i.e., firewall, switches and servers) shall be implemented with the latest security updates and patches per vendor recommendations.

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

5.8 All User ID formats should conform to corporate guidelines as highlighted in Section 11.1.1.3.6 "USER ID CONSTRUCTION" in IPSAG-007.

5.9 All nodes on the DMZ shall be assigned static IP addresses.

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

5.11 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.

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

5.13 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.

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

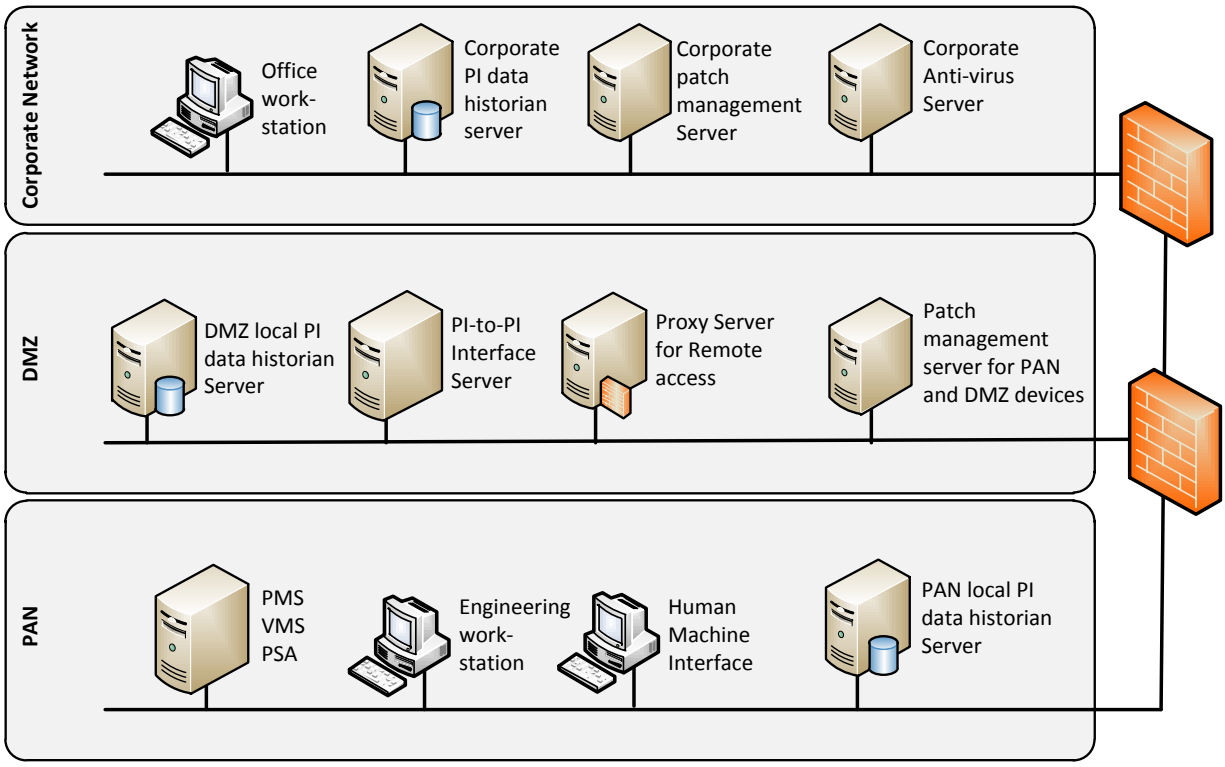

Figure 1 – Sample Logical DMZ Model Diagram

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 system logging for traffic monitoring and intrusion detection for all DMZ components.

6.5 Intrusion Prevention functionalities shall be installed on all firewalls.

6.6 The filtering mechanism shall be based on, as a minimum, source/destination IP addresses and TCP/UDP ports. Network equipment including firewalls and network devices must be hardened with the minimum security configuration baselines.

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.

7 Cabling Distribution Design

Premises distribution methods for cables and cabinets shall comply with SAES-T-916, "Communications Building Cable."

8 DMZ Applications and Services

DMZ shall host the following applications and services, but not limited to:

8.1 Patch Management

Patch management servers (such as windows security patches update and anti-virus data file) shall be located in the DMZ.

Commentary Note:

For small facilities where the number of workstation/servers is less than five, manual updates can be utilized in accordance with Saudi Aramco IT antivirus manual and relevant vendor recommendations periodically. A formal internal procedure shall be developed by the proponent.

8.2 Proxy Server

8.2.1 Proxy server shall be used as the gateway for any monitoring-application remote access requirements. Remote access from Corporate Network and Internet for control purposes shall not be permitted.

8.2.2 Remote access to resources within the PAN including networks and systems required supporting installation, upgrades, engineering, troubleshooting and remedial maintenance shall comply with the requirements of SAES-Z-010.

8.3 PI Data Exchange

8.3.1 Local PI data historian server shall be installed in either DMZ or plant PAN.

8.3.2 PI-to-PI interface node shall be installed at the DMZ to pull data from the local PI data historian server and push toward Corporate PI data historian server.

8.3.3 A separate PI-to-PI service shall be configured to read output tags and send data in a reverse direction. Allow write back to local PI server from Corporate PI server as needed by plant operational requirements.

9 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 and SAEP-1050 requirements and guidelines.

10 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. Penetration test is recommended to ensure secure design implementation.

11 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 TCP/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:

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

11.2 Equipment configuration data bases in Microsoft Excel or Access.

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

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

11.5 For all plant applications that need to traverse plant firewalls, the vendors shall provide application flow diagram that shows interpath 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

17 March 2013 New Saudi Aramco Engineering Standard.