Engineering Standard

SAES-Z-010 26 October 2005

Process Automation Networks Connectivity

Saudi Aramco DeskTop Standards

Table of Contents

Primary contact: Fouad M. Al-Khabbaz on 873-6401

1 Scope

1.1 This standard establishes the requirements for design, installation, configuration and commissioning of Process Automation Networks (PANs).

1.2 A PAN covers all process automation networks based on a standard communication protocol. A PAN does not include propriety Process Control Networks (PCN) provided as part of a vendor's process control system.

Geographically spread Remote Terminal Units (RTU's) are not in the scope of this standard.

1.3 The requirements and guidelines governing the engineering, design and installation of proprietary Process Control Systems is covered in SAES-Z-001.

1.4 The requirement for design, specification, installation, configuration, commissioning and maintenance for FOUNDATION™ Fieldbus based control systems are covered in SAES-J-904.

2 Conflicts and Deviations

2.1 Any conflicts between this Standard and other applicable Saudi Aramco Engineering Standards (SAES's), Materials System Specifications (SAMSS's) Standard Drawings (SASDs), or industry standards, codes, and forms shall be resolved in writing by the Company or Buyer Representative through the General Supervisor, Process Control Division, Process & Control Systems Department of Saudi Aramco, 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 General Supervisor, Process Control Division, Process & Control Systems Department of Saudi Aramco, Dhahran.

3 References

The selection of material and equipment and the design, construction, maintenance, and repair of equipment and facilities covered by this standard shall comply with the latest edition of the references listed below, unless otherwise noted.

3.1 Saudi Aramco References

Saudi Aramco Engineering Procedure

SAEP-302	*Instructions for Obtaining a Waiver of a Mandatory Saudi Aramco Engineering Requirement*

Saudi Aramco Engineering Standards

SAES-J-904	*Foundation Fieldbus (FF) Systems*
SAES-J-902	*Electrical Systems for Instrumentation*
SAES-P-103	*UPS and DC Systems*
SAES-Z-001	*Process Control Systems*

Saudi Aramco Materials System Specification

34-SAMSS-820	*Instrument Control Cabinet - Indoor*

Information Protection Standards and Guidelines Manual (IPSAG)

IPSAG-007	*Computer Accounts Security Standards & Guidelines*

3.2 Industry Codes and Standards

American National Standards Institute/Institute of Electrical & Electronics Engineers

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.

Bandwidth: In digital communications, describes the amount of data that can be transmitted over a channel in bits-per-seconds.

Ethernet: A local-area network architecture based on IEEE 802.3. It uses a bus or star topology and supports data transfer rates of 10, 100, 1000, and 10,000 Mbps.

Firewall: A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks.

Gigabit Ethernet: Ethernet that operates at 1000 Megabits per second.

Human Machine Interface (HMI): The display, data entry devices and supporting software to allow a user access to applications.

L3 Switch: A network device that joins multiple computers together at the network protocol layer of the Open System Interconnection (OSI) model eliminating the need for a router. L2 network switches operate at layer two (Data Link Layer) of the 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, such as personal computers, often via twisted pair or coaxial cable.

Logs: Files or prints of information in chronological order.

Process Automation Network (PAN): is a plant wide network interconnecting Process Control Networks (PCN) and provides an interface to the WAN. A PAN does not include proprietary process control networks provided as part of a vendor's standard process control system.

Process Control Network (PCN): A proprietary process control networks provided as part of a vendor's standard process control system.

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

Wide Area Network (WAN): an extension of LAN technology to include more nodes and greater distances between nodes; can be formed by interconnection of individual LANs.

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

Abbreviations:

CCTV	-	Closed Circuit Television
DCS	-	Distributed Control Systems
LAN	-	Local Area Network
OSI	-	Open Systems Interconnection
OSPAS	-	Oil Supply Planning & Scheduling
SCADA	-	Supervisory Control & Data Acquisition
TMS	-	Terminal Management System
VLAN	-	Virtual LAN
VMS	-	Vibration Monitoring System
WAN	-	Wide Area Network

5 System Design

5.1 The PAN shall be based on IEEE 802.3 CSMA/CD (Ethernet) standard. The backbone shall be based on Layer 3 multi-protocol switches utilizing 1 Gigabits per second (Gbps) throughput as minimum. Nodes, such as servers/ workstations, shall be connected to 10/100 Mbps ports. See Figure A.

PAN Backbone & firewall redundancy is mandatory for control applications.

Commentary Note:

PAN backbone & firewall redundancy is preferred for all applications. A cable splitter may be used to connect nodes not capable of having two Network Interface Cards (NICs) to the primary & secondary switches simultaneously.

5.2 The network design shall provide physical and logical separation between PAN and Corporate Network below firewall. Logical separation, at minimum, is mandatory for network connections above firewall. A minimum bandwidth of 5 Megabits/s requirements shall always be made available for any given WAN connection.

5.3 PAN Systems include those that exist below the firewall separating the PAN from the WAN. These systems include, but are not limited to Data Historian (SCAN Node), Distributed Control Systems (DCS) nodes, Vibration Monitoring System (VMS), Smart Valve Monitoring Systems (SVMS), SCADA system, Terminal Management System (TMS), and CCTV flare monitoring system.

5.4 PAN Systems requiring access by users on the WAN shall be placed on corporate network and follow corporate guidelines for information protection. Network traffic through the firewall should be limited to server-to-server connections and through selected IP ports. A server in this context is defined as dedicated un-manned data provider.

A proxy server with Remote Desktop Protocol (RDP) could be setup on the WAN as a portal for systems that are not feasible to be placed on the corporate network. Such server shall have adequate resources to support 64 concurrent sessions as minimum.

The remote desktop accessibility rights shall be assigned to a user group controlled by the PAN administrator. The PAN administrator shall restrict remote desktop sessions to those authorized and ensure that the "Everyone" group access rights are removed.

5.5 The PAN backbone switches shall assume the routing functionality internally for the PAN and interface with Saudi Aramco wide area network WAN router through a dedicated firewall hardware. The firewall shall be configured to limit Internet Protocol (IP) routes advertisement to the WAN router to those servers requiring access by other servers/users on the WAN. Other subnets assigned to PAN systems shall not be advertised to the WAN router.

5.6 PAN to PAN communication over the WAN shall be permitted through the firewall for control applications only. For none control applications, a server-to-server communication above the firewall shall be utilized.

5.7 PAN shall not interface as gateways to non-Saudi Aramco networks such as Internet.

5.8 All TCP/IP addressing shall be obtained from Network Management, Information Technology.

5.9 All nodes on the PAN shall be assigned static IP addresses. Dynamic Host Configuration Protocol (DHCP) shall not be used any where on the PAN.

Plant Network Design

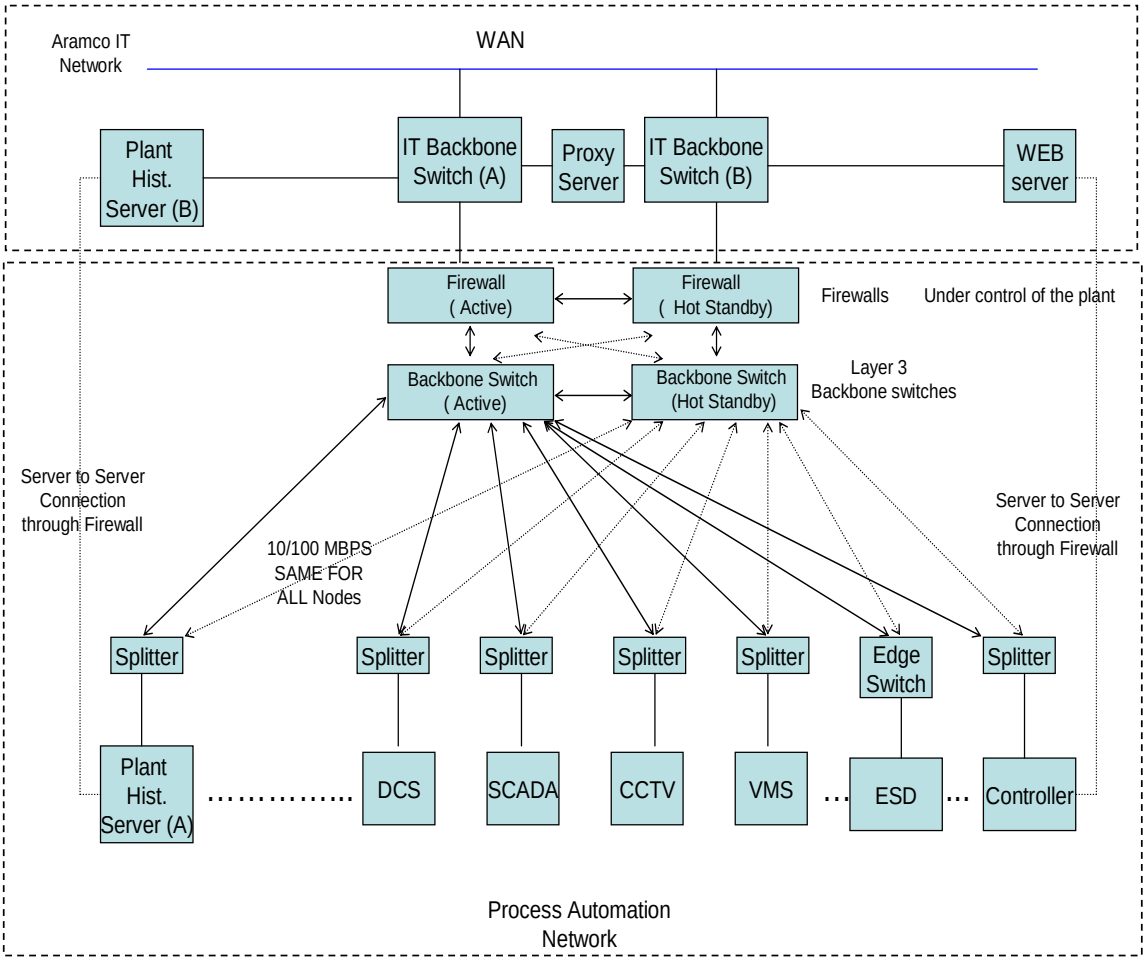

Figure A

6 Wiring System

6.1 PAN cabling shall conform to "The Data Link" requirements in SAES-J-902 (Electrical Systems for Instrumentation).

6.2 PAN cabinets shall be designed in accordance with Saudi Aramco Materials System Specification 34-SAMSS-820.

6.3 UPS/Battery capability and software implemented to provide for a controlled shutdown of services in PAN components shall be configured according to SAES-P-103, "UPS and DC Systems".

Commentary Note:

Network protocol analyzers are recommended for detailed network maintenance and troubleshooting. The protocol analyzer shall have the capability to be able to decode all PAN protocols. In a switched environment, a network analyzer can only see a single segment at a time; therefore, a mechanism to overcome this obstacle shall be made available.

7 System Access and Access Monitoring

Commentary Note:

Detailed network and systems security guidelines are outlined in the "Manual for Minimum Security Requirements for Plants Networks and Systems".

The PAN shall not allow any users on the local network other than the Operators and Engineers who will administer the network and perform system configuration and system monitoring.

7.1 User ID Types

Every User ID shall have a password. The minimum default settings shall be:

- Minimum password length 6
- Force periodic changes Yes
- Days between changes 120
- Grace login limit No
- Require unique passwords Yes

User ID password shall not be stored in user or unprotected files. All vendor-supplied default passwords for predefined IDs shall be changed immediately after installation or upgrade.

7.1.1 An application User ID are those associated with applications. The password for such IDs shall always be used in encrypted/protected and encapsulated form and shall not be coded into the application in plain text.

7.1.2 System User IDs are those used by the system itself. Such IDs shall be administered & managed by the PAN administrator. If the system User ID needs to be assigned to a group where no alternative solution is feasible, the group shall be restricted to those authorized persons who

shall use it. The limited group shall be documented and updated regularly.

7.1.3 Operator User IDs are those used by Operators to access the system. Such IDs shall have a restricted user profile so that a user will not be able to install programs or change software configuration, access floppy disk or CD drives, or any removable media. A PAN administrator shall have full access privileges on all PAN components. GUEST accounts shall be disabled on all systems.

7.1.4 Super/Privileged User IDs are those used by System Administrators. Such IDs shall be assigned in combination with a normal User ID to ensure accountability. The use of Super/Privileged User IDs shall be limited for system support purposes and system troubleshooting and only when necessary. These accounts shall be certified every 12 months. Super/Privileged User IDs should be locked when not needed.

7.1.5 Operator, Application, and System IDs shall be excluded from automatic password change policy, however, the PAN administrator shall make sure that Application, and System IDs passwords are changed manually every 12 months.

7.2 User ID Format

All PAN User IDs format shall conform to Section 8.6.1 "Saudi Aramco Network User IDs" in IPSAG-007, "Computer Accounts Security Standards and Guidelines, revision number 001 and dated August 2003.

7.3 System Access

7.3.1 System Login scripts, if any, shall be configured to prevent a user bypassing them.

7.3.2 Repeated login failures shall be logged with the location, date, time and user account used. An alert message should be sent to the PAN administrator in the event of repeated login failures.

7.3.3 At login time, every user should be given information reflecting the last login time and date, if supported by the system or application. This will allow unauthorized system usage to be detected.

7.3.4 The use of the same User ID from multiple workstations shall be restricted to only one workstation.

7.3.5 A PAN shall not enable dial in connections for remote control purposes. A vendor remote troubleshooting and testing is the only exception

provided that such activity shall be strictly monitored, documented, and on temporarily basis.

7.3.6 A PAN shall not be configured to access the following IT services: Email, Internet, and File Sharing.

7.4 PAN Hardware Maintenance

When a PAN system installed or upgraded, the PAN administrator shall change all vendor supplied default passwords for predefined system IDs and should create a backup copy of the current system.

The data files and application software shall be backed up on a daily basis, if possible, and are made available for recovery. Any sensitive information shall be removed or wiped off of storage devices before hardware is removed from the premises to prevent unauthorized release. In addition, the following measures shall be considered:

7.4.1 Any hardware shall not be connected to PAN without the prior authorization of the PAN administrator.

7.4.2 Operating system or network software changes shall not be implemented without prior authorization of the PAN administrator. Implementing of application software which modified configuration files shall be reviewed prior to installation by the PAN administrator to ensure that no network conflicts happen.

7.4.3 PAN shall be configured to report unexpected login failures to the PAN Administrator.

7.4.4 PAN shall be configured to report suspected unauthorized access of their IDs to the PAN Administrator.

7.4.5 PAN shall be configured to notify the PAN Administrator of any expected long-term absences, to allow the ID to be temporarily disabled.

7.5 Monitoring and Review

The PAN shall be configured for the monitoring of:

- Unexpected users logged on the system.
- Users from unexpected hosts logged on.
- Users logged on at unexpected times.
- Login failures.
- Logins from unknown hosts.

- Failed access to system files.
- Changes to the system date and/or time.
- System reboots and shutdowns.
- Use of remote console facility.
- Integrity of system security files.
- Users without passwords.
- Users with passwords similar to their login names.
- Users with passwords of fewer than six characters.
- Users who are not required to change their passwords every 120 days.
- Users who are not required to use unique passwords.
- Inappropriate accesses to system files.

7.6 Physical Access

The PAN hardware components such as cables, switches, routers and modems are vulnerable to vandalism and electronic eavesdropping and shall be physically secured.

Physical access to these components shall be restricted to those persons authorized for administrative access. Unused offices/partitions shall not have live network ports.

8 System Testing

8.1 Testing shall address all Plant components, networking and interfaces to external systems and to legacy applications/system. Formal testing shall minimally comprise Factory Acceptance Test (FAT), Site Acceptance Tests (SAT), and Performance Acceptance Tests (PAT).

8.2 Comprehensive test plans and test specifications shall be followed for all plant platforms, networking, applications, integration components, interfaces to external systems and legacy applications/systems, and any additional technology content of the plant project.

9 Documentation

Comprehensive documentation shall be provided to ensure that the PAN 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 the system mapped to individual Medium Access Control (MAC) addresses. The documentation shall also

include physical locations of systems components like routers, switches, servers and workstations.

The following shall be made available:

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

9.2 Equipment configuration data bases in Microsoft Excel, Access or Intools.

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

9.4 A plant network drawings layout showing the PAN logical and physical design and its interconnection to the WAN.

Revision Summary

28 April 2004	New Saudi Aramco Engineering Standard.
26 October 2005	Minor revision.