Engineering Standard

27 October 2020

SAES-T-555
Video Surveillance Systems

Document Responsibility: Communications Standards Committee

Contact: Russel Torres (toresru)

Contents

Summary of Changes

Paragraph Number		Change Type (Addition, Modification, Deletion)	Technical Change(s)
Previous Revision (18 October 2017)	Current Revision (27 October 2020)		
3	3	Addition	- [add] SAES-J-902, SAES-O-205, SAES-Z011 - [add] , SACS-001, SACS-007, SACS-008, SACS-010, SACS-023 - [add] GI.710.002 - [add] NEMA VE1, NEMA VE2, ISO/IEC 23093, IEC 60529, IEEE 802.1, IEEE 802.3
4.2	2.2	Addition	-[add] definition of PKI, RTSP, VRS.
5.1 .1	5.1 .1	Addition	-[add] Video Recording System
5.1.5	5.1.5	Modification	[delete] delete old requirement
5.1.6	5.1.5	Addition	[add] 25 frames per second for PAL
5.1.7	5.1.6	Modification	[modify] Rephrase the requirement for more clarification.
5.1.8	5.1.7	Addition	[add] exception for Industrial Security Systems
5.1.13	5.1.12	Modification	[modify] Rephrase the requirement for more clarification.
5.1.13	5.1.13	Modification	[modify] move the physical requirement to a new subsection from the previous one.
5.3.5.4	5.3.5.4	Modification	[delete] the unneeded definition of day/light camera
5.3.6.1	5.3.6.1	Modification	[modify] detail the minimum resolution of optical camera
-	5.3.6.2	Addition	[add] thermal cameras minimum resolution
-	5.3.6.3	Addition	[add] add a requirement for AI and machine learning requirement.
5.3.6.2	5.3.6.2	Addition	[add] exception for Industrial Security Systems
6.1.2	6.1.2	Modification	[modify] IT prior approval is removed and replaced with design review.
6.1.6	-	Modification	[delete] The requirement is removed as this is IT backbone and design and engineering of IT Backbone is by IT
6.1.7	-	Modification	[delete] The requirement is removed as this is IT backbone and design and engineering of IT Backbone is by IT
6.1.8	-	Modification	[delete] The requirement is removed as this is IT backbone and design and engineering of IT Backbone is by IT
6.1.4	6.1.6	Modification	[modify] the sequence of the requirement is modified. [modify] Rephrase some of the write up for more clarity [modify] Rephrase the commentary note for more clarity
6.1.3	6.1.4	Modification	[add] the requirement of video surveillance system isolated network [add]SAES-Z-010 is added for security zone requirements.

			[delete] the requirement of control system traffic is carried over PAN.
6.1.11	6.1.11	Modification	[delete] wireless link.
6.1.17	6.1.17	Addition	[add] new requirements for wireless cameras and network are added.
6.2.7	6.2.7	Modification	[modify] replace data filtering with firewalls
7.1.1	7.1.1	Modification	[modify] the options to connect VMS have been modified from two to three [modify] the requirement to connect VMS to corporate network has been removed and replaced with applicable SACS [add] add the requirement to connect VMS with PAN
7.1.6	-	Modification	[delete] This section has been deleted as it was added to 7.1.1
7.1.7	7.1.6	Modification	[delete] The requirement was modified to ensure that organization identify the required interval time for recording and retaining.
7.3.2	7.3.2	Modification	[modify] System logs requirement within plant network
7.3.12	7.3.12	Modification	[modify]The details for the requirements to connect to corporate network have been removed and replaced with applicable Saudi Aramco Cybersecurity Standards (SACS) for alignment and details.
9.1.3	9.1.3	Modification	[delete] no additional cost is removed to avoid confusion.
9.2.6	9.2.6	Modification	[modify]the requirement is modified to conducting a coverage assessment to minimize the dead zone.
9.2.7	9.2.7	Modification	[modify] The requirement of Grounding and Bonding of poles and metallic materials have been referenced to the applicable Saudi Aramco Engineering Standards.
9.2.8	9.2.8	Modification	[modify] The applicable Saudi Aramco engineering Standard has been added.
9.3.4	9.3.4	Modification	[modify] Video Surveillance cabling requirements have been replaced with conduits requirements for underground cabling. The applicable Saudi Aramco Engineering Standards have been refernced.
9.3.5	9.3.5	Addtion	[add] new requirements for above ground cabling have been added and the applicable Saudi Aramco Engineering Standards and International standards have been refernced for alignment and details.
9.5	9.5	Addition	[add] new requirements for PoE+ are added
9.7	9.7	Addition	[add] requirements for new documents are added

1 Scope

This standard establishes the requirements for the design and installation of video surveillance system used to support plant operations, Industrial facilities and other Saudi Aramco corporate users. Examples of video surveillance system uses include monitoring process area, oil and gas wells, and security perimeter.

2 Conflicts and Deviations

Any conflict between this document and other Applicable Mandatory Saudi Aramco Engineering Requirements (MSAERs) Shall be addressed in writing to the EK&RD Coordinator.

Any deviation from the requirements herein shall follow internal company procedure SAEP-302, waiver of a Mandatory Saudi Aramco Engineering Requirement.

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 Procedures

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

Saudi Aramco Engineering Standards

SAES-B-055	*Plant Layout*
SAES-B-068	*Electrical Area Classifications*
SAES-J-003	*Instrumentation and Control Buildings - Basic Design Criteria*
SAES-J-902	*Electrical Systems for Instrumentation*
SAES-O-204	*Security Lighting*
SAES-O-201	*General Requirements of Security Directives*
SEAS-O-205	*Security Systems for Industrial Facilities*
SAES-P-100	*Basic Power System Design Criteria*
SAES-P-111	*Grounding*

SAES-T-795	*Grounding, Bonding, and Electrical Protection for Telecommunications Facilities*
SAES-T-911	*Telecommunication Conduit System Design*
SAES-T-916	*Telecommunications Building Cable Systems, Pathways and Spaces*
SAES-T-928	*Telecommunications - OSP Buried Cable*
SAES-Z-010	*Process Automation Networks*
SAES-Z-011	*Industrial Wireless Infrastructure Design*

Saudi Aramco Materials System Specification

23-SAMMS-701	*Industrial Ethernet Switch Specifications*

Saudi Aramco Cybersecurity Standards

SACS-001	Anti-Malware Cybersecurity Standard
SACS-007	*Windows Protection Standard*
SACS-008	*Patch Management Standard*
SACS-010	*Video Surveillance Cybersecurity Standard*
SACS-023	*Network Security Standard*

Saudi Aramco Cybersecurity Standards

GI.710.002	*Classification and Handling of Sensitive Information*

3.2 Industry Codes and Standards

National Electrical Manufacturers Association

NEMA ICS 6	*Enclosures for Industrial Controls and Systems*
NEMA 250	*Enclosures for Electrical Equipment (1000 Volts Maximum)*
NEMA VE1	*Metal Cable Trays Systems*
NEMA VE2	*Cable Trays Installation Guidelines*

International Organization for Standardization and International Electrotechnical Commission

ISO/IEC 23093	*Information technology — Internet of media things*

IEC 60529	*Classification of degrees of protection provided by enclosures for electrical equipment*
IEEE 802.1	*802 LAN/MAN architecture, internetworking among 802 LANs, MANs and WAN, 802 Security, 802 overall network management, and protocol layers above the MAC & LLC layers*
IEEE 802.3	*Standards for Ethernet Network*

4 Definition, Word Usage, Abbreviations

This document uses 'requirement' language. Please note the following definitions:

Shall: Mandatory

Should: Recommendation, strongly preferred

May: Permissible/optional

Can: Possible or capable

4.1 Definition

Auto Iris: An automatic method of varying the size of a lens aperture in response to change in the scene illumination.

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

Camera Access Switch (CAS): An Ethernet switch where the cameras or encoders are terminated. It is located in the nearest plant facility building to the cameras or encoders.

Contrast: A common term used in reference to the video picture dynamic range. It is the difference between the darkest and the brightest part of the image.

Day/Night Camera: A camera that can capture video in both day and night time. In low light conditions, day/night camera may switch from color to monochrome video.

Distributed Control System (DCS): A process control system that is composed of distinct modules. These modules may be physically and functionally distributed over the plant area.

Encoder: A device that convert analog video signal to digital signal.

Frame: Refers to a composition of lines that make one TV frame.

IP camera: A camera that has an IP address and complies with the standard Internet Protocol (IP).

Iris: A means of controlling the size of the lens aperture and therefore the amount of light passing through the lens.

JPEG: It stands for Joint Photographic Experts Group which is a group that has recommended a compression algorithm for still digital image.

Latency: The time required for an image captured by the camera to be presented on monitor (screen) to the user.

Lux: Light unit for measuring illumination. It is defined as the illumination of surface when the luminous flux of lumen falls on the area of 1 cm^2. It is also known as lumen per square meter.

Virtual Routing and Forwarding (VRF): It is a technology used in the IP network to segment the network logically without using additional devices.

Media Converter: It is a device that converts between different types of transmission media (cable). It is used to convert from Unshielded Twisted Pair (UTP) cable to fiber optic cable and vice versa. Media converters also are referred to as media transceivers, media translators, or media filters.

Midspan: Midspans are power injectors that stand between a regular Ethernet switch and the powered device to provide PoE functionality.

Motion JPEG: In motion JPEG, individual images are captured and compressed into JPEG still image forma then they are made available as continuous flow of images to be viewed.

MPEG-4: It stands for Moving Picture Experts Group which is a standard for audio and video compression.

H.264/MPEG-4: It is a new standard for video compression which has more advanced compression methods than the basic MPEG-4 compression.

Multicast: It is the delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the destinations split.

Multi-channel Encoder: an encoder that is capable of connecting to more than one camera. It provides more than one BNC connection for analog cameras to connect to.

Process Automation Network (PAN): It 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.

PTZ: It stands for Pan, Tilt and Zoom. Pan refers to rotating the camera around Z-axis. Tilt refers to rotating the camera around the X-axis. Zoom refers to Y-axis movement of the motorized optical lens.

Quality of Service (QoS): It refers to resource reservation control mechanisms. It can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow. Quality can be, for instance, a maintained level of bandwidth, low latency, no packet losses, etc.

Redundant Array of Independent Disk (RAID): It is data storage schemes that divide and/or replicate data among multiple hard drives. RAID arranges hard drives in such a way that the operating system sees them as one large logical hard disk. It set up spans data over multiple hard disk drives with enough redundancy so that data can be recovered if one disk fails.

Resolution: It is a measure of the ability of a camera to reproduce fine detail. The higher resolution, the more details can be seen.

Spanning Tree Protocol: It is layer-2 protocol that ensures loop free topology for any Local Area Network (LAN).

Unicast: It is the sending of information packets to a single destination.

Video Compression: It refers to reducing the quantity of data used to represent video images with the goal of retaining as much of the original's quality as possible. Compressed video can effectively reduce the bandwidth required to transmit digital video.

Video Matrix Switcher: A device for switching more than one camera or other analog based CCTV devices to more than one monitor (screen) or video printer.

Video Surveillance Component: the different type of product that makes the whole video surveillance system.

4.2 Abbreviations

CCR: Central Control Room

CCTV: Closed Circuit Television

DAS: Direct Attached Storage

IGMP: Internet Group Management Protocol

IR: Infrared

JPEG: Joint Photographic Experts Group

LDAP: Lightweight Directory Access Protocol

MPEG: Moving Picture Experts Group

MPLS: Multiprotocol Label Switching

NAC: Network Access Control/Controller

NAS: Network Attached Storage

NTP: Network Time Protocol

NVR: Network Video Recorder

PAN: Process Automation Network

PCS: Process Control System

PAS: Process Automation System

PKI: Public Key Infrastructure

PoE: Power over Ethernet

RTSP: Real Time Streaming Protocol

SCADA: Supervisory Control and Data Acquisition (SCADA) System

SNMP: Simple Network Management Protocol

STP: Spanning Tree Protocol

UPS: Uninterruptible Power Supply

UTP: Unshielded Twisted Pair

VLAN: Virtual Local Area Network

VMS: Video Management System

VRF: Virtual Routing and Forwarding

VRS: Video Recording System

5 Video Surveillance System Design Basis and Considerations

5.1 General Video Surveillance System Requirements

5.1.1 Video Surveillance system shall include (but not limited to):

a. Video camera.

b. Ethernet network switch.

c. Video Management System (VMS).

d. Video Recording System (VRS). Video Storage.

e. Displays.

5.1.2 All new installation should be IP based systems. Video matrix switcher shall not be used unless it is for an expansion of an existing system that does not support IP cameras.

5.1.3 Analog monitors shall not be used .

5.1.4 All Video Surveillance System components shall be based on open standard such as ONVIF and shall be easily integrated with open standard platforms and shall be Ethernet TCP/IP based system.

5.1.5 Video Surveillance system shall be capable of transmitting and recording video at 30 frames per second and 25 frames per second for PAL with the ability to adjust different frame rates by the system administrators and operators.

5.1.6 The Video Surveillance system shall support RTSP to transmit real time video.

5.1.7 Video Surveillance system shall be designed for high performance, flexibility, and scalability. It shall allow adding new components without significant change to the existing system infrastructure. For industrial security system, the system design shall comply with SAES-O-205.

5.1.8 Video Surveillance system shall allow for simultaneous recording and variable playback speed.

5.1.9 Lightning protection systems shall be provided in accordance to SAES-P-111.

5.1.10 Video camera should provide day/night functionality in indoor/outdoor environment.

5.1.11 The Video Surveillance system shall support at least H.264 compression standard.

5.1.12 The Video Surveillance System components shall be installed in a secure network zone (dedicated VLAN) when they share the network with other systems.

5.1.13 The video Surveillance System components shall be in a physical access controlled locations such as secured locked cabinets inside communication or server rooms.

5.2 Bandwidth and Storage Requirements Study

Bandwidth and storage requirements study are required to determine the needed bandwidth and storage. These requirements shall be calculated and determined by the system designer for the whole system in the design stage. The study shall consider the factors listed in Sections 5.3.1, 5.3.2 and 5.3.3.

5.3 System Design Considerations and Criteria

The following factors shall be considered when designing the system:

5.3.1 Bandwidth

The following parameters affect bandwidth design requirements of Video Surveillance System and shall be considered in the system design phase:

a. Required image resolution. The higher the resolution, the more bandwidth is required.

b. Required compression type and ratio.

c. Frame rate.

d. Complexity of the scene.

e. System redundancy.

5.3.2 Storage

The required storage shall be determined based on the following:

a. Number of cameras.

b. Number of hours per day the camera will be recording.

c. How long the data must be stored.

d. Whether the system uses motion detection recording, scheduled recording or continuous recording.

e. Frame rate.

f. Used compression technique.

g. Required image quality and complexity.

5.3.3 Scalability

Future expansion (if any) shall be considered and planned for during the design phase.

5.3.4 Frame Rate Control

The system shall allow for frame rate control. It shall be possible to raise and lower the frame rate. The system shall allow for sending video with different frame rate to different recipients.

5.3.5 Lighting

Lighting for Industrial Security Systems shall adhere to SAES-O-204.

All other systems shall adhere to the following:

5.3.5.1 An assessment shall be made to evaluate how lighting will affect the quality of the image. Existing light shall be evaluated to determine the need for additional external light source.

5.3.5.2 Ensure that the lighting level is adequate. At least 5 lux shall be used to capture good quality images.

5.3.5.3 In areas where lighting level falls below 5 lux, external light source such as electrical lamp or day/night camera shall be used as specified in 5.3.5.4 and 5.3.5.5 of this standard.

5.3.5.4 Electrical lamps shall be added when there is no enough light to capture good quality colored image. However, if it is acceptable by user's department to have black and white image/video, then a day/night camera should be used in low light and nighttime conditions.

5.3.5.5 In cases where the use of electrical lamp sources is restricted, a day/night camera shall be used. If needed, IR illuminator shall be used in conjunction with the day/night camera to further enhance camera's ability to produce high quality video in low light and night time conditions.

5.3.5.6 Ensure that the lighting is even and minimizes shadows for indoor cameras. Several lower powered, widely spaced lights should be used instead of using one bright light.

5.3.5.7 Electrical lamps shall be mounted so that they don't damage or weaken the image quality. When it is possible, the light sources shall be positioned above the camera.

Commentary Note:

An auto iris lens should be used with outdoor cameras to regulate how much light is received, to optimize the image quality and to protect the image sensor from being damaged by strong sunlight.

5.3.6 Video Resolution

5.3.6.1 Optical cameras shall operate at full High-Definition (HD) with minimum resolution of 1920 x 1080 pixels.

5.3.6.2 Thermal Cameras shall operate at 320 x 240 pixels or higher.

5.3.6.3 For AI and machine learning applications, an assessment shall be conducted to identify the sufficient camera resolution that will be suitable for the application.

5.3.6.4 Interlaced scanning or progressive scanning may be used except for industrial security systems where interlaced is not allowed by SAES-O-205.

5.3.6.5 If interlaced scanning is used, de-interlaced shall be used to eliminate the jaggedness for better view

5.3.6.6 Aspect ratio of 4:3, 16:9, or 16:10 shall be used based on user's requirements.

5.3.7 System Integrity

5.3.7.1 The Video Surveillance system shall have the capability of software, interconnections and component failure detection and notification.

5.3.7.2 The system shall have adequate protection against tampering.

5.3.7.3 The system shall have protection against unauthorized access.

5.3.8 Data Export

5.3.8.1 Exporting data shall not affect the recording of the Video Surveillance system primary storage. Printing images is not considered as a data export method.

5.3.8.2 Exported data shall have source identifier and time stamp.

5.4 Environmental Conditions

Video Surveillance system components shall operate continuously without damage, miss-operation, or data corruption under the environmental conditions listed in Section 8 of SAES-J-003. However, Industrial security Video Surveillance systems shall comply with the requirements in SAES-O-201 instead of SAES-J-003 environmental requirements.

6 Video Surveillance Systems Network Architecture and Requirements

6.1 Video Surveillance System Network Connectivity Structure

6.1.1 Video Surveillance Systems shall be IP-based, unless the available systems can't meet the operational requirements.

6.1.2 The design for Video Surveillance Systems installation that are connected to Saudi Aramco corporate network and not used for industrial security systems shall be reviewed and approved by Information Technology Engineering Department (ITED).

6.1.3 The following uplink requirements are applicable for IT Video surveillance systems only:

a. Traffic entering the corporate IP/MPLS backbone from the uplink port of non-IT switches shall be limited to 100 Mbps, excess traffic will be dropped.

b. IP Camera traffic shall be allocated no more than 15% of the uplink bandwidth of the IT access switch that connects directly to the corporate IP/MPLS Core Provider Edge Router.

c. Remote Sites (Bulk Plants, AFOs, etc.) that are connected through a leased IP-VPN circuits, no more than 10% of the leased circuits link bandwidth shall be consumed by IP camera traffic, provided that after adding the cameras no more than 80% of the bandwidth will be utilized at peak times. Traffic rules shall be applied on the router to ensure that no more than 10% of the bandwidth is utilized by the Video Surveillance system including any pre-existing Video surveillance system.

Commentary Note:

Industrial Security and in-plant video surveillance systems are exempted from these requirements. However, adequate bandwidth should be calculated to avoid network interruption on other critical data.

6.1.4 Video Surveillance System can be interfaced with DCS or SCADA via PAN and shall comply with SAEP-99 and SAES-Z-10. The following options shall be considered when connecting to PAN network.

a. Video Surveillance System network can be physically separated from PAN, and they shall be interfaced through plant Firewall.

b. Video Surveillance System traffic can utilize PAN infrastructure. In this case, network traffic segmentation shall comply with SAES-Z-010 where traffic shall be logically separated from other traffic within PAN by assigning Video Surveillance System traffic to a separate VLAN. The network traffic between those networks shall be routed and controlled through plant firewall.

6.1.5 Multicast should be utilized when there is a large number of viewers (more than 30) or when the aggregate bandwidth (stream bandwidth multiplied by the number of users) is large (100Mbps).

6.1.6 The use of analog cameras shall be limited to cases where it is used as an expansion to an existing system where the system supports only analog cameras.

6.1.7 The IP cameras or the encoder shall be connected to an Ethernet switch; hereinafter called Camera Access Switch (abbreviated CAS). The CAS shall be located.

a. At the nearest facility building to the cameras. Or

b. At the camera site when the camera is installed in a remote location such as oil and gas well sites were industrial Ethernet switches shall be used, 23-SAMMS-701 provides Industrial Ethernet material specifications.

The CAS may be a switch dedicated for Video Surveillance Systems, an IT switch, or a PAN switch.

6.1.8 The IP camera and the encoder can be connected to the CAS via UTP, multi-mode fiber, single mode fiber..

6.1.9 The type of the cable connecting the camera/encoder shall be determined based on the distance from the IP camera or the encoder to the CAS.

6.1.10 The CAS switch shall have the required 10/100/1000 Ethernet interface ports to connect to the IP cameras or encoders.

6.1.11 The IP camera interface and encoder interface configurations to the CAS shall be limited to 10/100 Mbps. If the encoder aggregates more than one camera channel (multi-channel encoder), then it shall interface to CAS via 100/1000 Ethernet interface.

6.1.12 The uplink of CAS to the PAN or Saudi Aramco corporate network shall be 100/1000 Mbps interface.

6.1.13 Video Surveillance System Video Management System (VMS) shall be used to view live video and to play back recorded and stored (archived) video.

6.1.14 Wireless cameras and network infrastructure can be used

6.1.14.1 Wi-Fi cameras and infrastructure shall utilize the 5 GHz frequency band to avoid interference with plant wireless sensors and shall comply with SAES-Z-011.

6.1.14.2 4G/5G technologies or other wireless solutions can also be utilized for connectivity based on allowed frequencies; however, 2.4 GHz shall not be used.

6.1.14.3 Video Surveillance System Video that are connected to corporate network shall comply to SACS-010.

6.2 Requirements of the network carrying Video Surveillance System Traffic

The requirements of the network carrying Video Surveillance System traffic are as follow:

6.2.1 Network carrying Video Surveillance System traffic shall have latency less than 200ms to allow for accurate PTZ positioning and controlling.

6.2.2 The network shall support Quality of Service (QoS) according to the best industry practice to implement traffic control and packet priority.

6.2.3 The network shall support unicast and multicast stream.

6.2.4 The network shall be capable to deliver power to IP cameras and encoders using PoE and PoE+ technology for copper installations that are shorter than a 100m.

6.2.5 The network shall support:

a. IEEE 802.1D bridging capability and loop detection.

b. IEEE 802.1Q tagged VLANs.

c. IEEE 802.1p traffic prioritization for multiple Quality of Service levels.

d. IEEE 802.1w rapid spanning tree with fast link support.

e. IEEE 802.3ad link aggregation support.

f. IGMP snooping for IP Multicast support.

g. Multicast network traffic.

h. Non-blocking configuration capable of simultaneous wire-speed switching across all ports.

i. SNMP v3 or higher.

j. For multi-viewer Video Surveillance System data streams, IP multicast technology shall be utilized.

6.2.6 The Video Surveillance System network as a minimum shall be segregated logically by use of VLAN or equivalent technology as a minimum.

6.2.7 Video Surveillance System network can be interfaced to other networks by use of firewalls to limit the data exchange to the absolute minimum required.

6.2.8 Network multicast shall be used and configured if more than one user is viewing a given stream.

7 Video Management System (VMS)

7.1 General Requirements

7.1.1 The Video Surveillance Management System (VMS) shall be one of the below three options:

a. Connected to Saudi Aramco corporate network:

The VMS servers shall comply to Saudi Aramco Cybersecurity Standards (SACS)

b. Connected to PAN:

VMS servers can be integrated with Process Automation Systems such as DCS and SCADA. The VMS servers shall comply with SAEP-99 and shall comply with security zone requirements in SAES-Z-010.

c. Connected to physically isolated network:

1. Standalone modular software based that runs on of the shelf open standard hardware platform. The hardware components of the open standard platform shall be selected to obtain required performance.

2. Integrated hardware-software platform where the software is pre-configured on the hardware.

Commentary Note:

When this standard refers to VMS server, it means the integrated hardware-software platform that hosts the Video Surveillance Management software.

7.1.2 VMS shall be based on client server architecture.

7.1.3 VMS shall provide administration, installation and configuration, operation of IP cameras and shall administer access rights and privileges to these devices.

7.1.4 VMS shall provide the following functions, but not limited to:

a. Central management, configuration, system monitoring and control of the entire system.

b. System security and central user management.

c. Network video recording capability.

7.1.5 VMS shall be the interface between IP cameras or encoders and the viewing clients for Video Surveillance System traffic management and access authorization. The video stream from IP cameras and encoder should be sent to the viewing through the VMS.

7.1.6 Organizations shall identify the required interval to record and retain the captured videos and images.

7.2 Video Surveillance System VMS Redundancy

VMS can be in a redundant configuration so that if the main VMS fails, the system immediately automatically fails over to the backup server. In a case of redundant VMS configuration, the following shall be considered:

7.2.1 The backup VMS shall be continuously synchronized with the master VMS server to ensure that it is always up to date and ready for fail over when required. When the master VMS server is restarted after fail over, it shall automatically resynchronize with the backup server.

7.2.2 The date and time on both servers shall be synchronized with an NTP server if available to ensure that all date and times associated with event in the database are consistent in between servers.

7.2.3 The Video Surveillance system functionality shall not be affected during or after the fail-over.

7.3 User Management and Security

7.3.1 The video stream from IP cameras and encoder shall be sent to user after the user is authorized through the VMS.

7.3.2 Video Surveillance systems shall generate audit logs to record system activities for business, investigation and operation needs. Logs shall be kept for one year. Systems within a plant networks shall send the logs for consolidation to plant's event log servers.

7.3.3 The VMS connected to PAN network shall comply with authentication and authorization, users account, and system access requirements established in SAEP-99.

7.3.4 The VMS shall require a user name and password that determine the level of authorization as being a user or administrator of the video management system.

7.3.5 Password used to access Video Surveillance system shall always be encrypted.

7.3.6 All exported recording and exported audit log shall be digitally signed to prove origin of the recording and audit log and to ensure that exported recording and audit log have not been altered or tampered with. VMS shall provide a default digital certificate for signing the exported recording and audit log and shall allow administrator to supply Saudi Aramco PKI generated certificate.

7.3.7 A visual indication shall be provided to show if the exported recording and audit log have been altered or tampered with.

7.3.8 Isolated VMS shall allow Video Surveillance System administrator to create, edit, or delete user groups and users at any time.

7.3.9 Isolated VMS shall allow Video Surveillance System administrator to set different authorization levels or privileges for users.

7.3.10 VMS shall provide group configuration where users only see devices for which they have access to.

7.3.11 Unrequired ports and services on the camera and Video Surveillance system shall be disabled.

7.3.12 Video Surveillance Systems connected to the corporate network shall adhere to SACS-001, SACS-007, SACS-008, SACS-010 and SACS-023.

7.4 Video View and Operation Requirements

7.4.1 VMS shall be capable of recording, analyzing, and playing back video.

7.4.2 VMS shall be capable of providing users access to video streams via web browser or Windows client.

7.4.3 VMS shall be capable of searching recorded video based on date and time.

7.4.4 VMS shall support simultaneous viewing and recording of live video from multiple cameras.

7.4.5 VMS shall provide continuous recording mechanism, on alarm and video motion detection recording mechanism, and scheduled recording mechanism.

7.4.6 VMS shall enable system administrator or system support professional to set the recording frame rate of selected cameras.

7.4.7 VMS shall support camera management. It shall allow system administrator to administer and mange camera.

8 Video Surveillance Storage and Archiving System

8.1 Video Storage and archiving system shall keep the videos for the maximum duration of data availability required by the user and justified by the business case.

8.2 When video storage and archiving system is required, it shall be based on industry standard off the shelf hardware. Vendor proprietary solutions shall not be used.

8.3 Video surveillance storage and archiving shall be provided by one of the following ways:

8.3.1 Direct Attached Storage (DAS) where additional external hard disk is attached to the VMS server for storage.

8.3.2 Network Attached Storage (NAS) where the storage is separated from the VMS server.

8.4 Storage and archiving redundancy, if required, shall be provided by hardware based RAID (Redundant Array of Independent Disk) with separate RAID controller.

8.5 Moving data across the network for the purpose of archiving shall be scheduled for off-peak hours.

9 Video Surveillance System Installation

9.1 General Consideration

9.1.1 The Video Surveillance system components installed in hazardous (classified) areas as defined by the approved area classification drawing shall meet the criteria set forth in SAES-B-055 and SAES-B-068 for classified areas.

9.1.2 The classification shall be performed using the Class /Zone/Group method per SAES-B-068.

9.1.3 Classified Video Surveillance equipment shall not be used in non-classified area unless the vendor's standard product offering is supplied as classified device.

9.1.4 The Video Surveillance equipment installed in classified areas shall be rated and labeled for use in classified locations. They shall be certified to operate in the required classified location.

9.2 Mounting and Housing

9.2.1 Weather proof and vandal proof housing shall be provided for cameras installed outdoors or in relatively hostile environment. See environmental conditions listed in Section 8 of SAES-J-003. However, Industrial security Video Surveillance Systems shall comply with the requirements in SAES-O-201.

9.2.2 Camera shall be placed on stable support to minimize camera movement. In outdoors installation, sturdy mounting equipment shall be used to avoid vibration caused by strong winds. Supports shall be rigidly embedded in a foundation to resist vibration.

9.2.3 Camera mount shall be designed to support the maximum weight of camera and enclosure assemblies.

9.2.4 Direct sunlight shall be avoided since it blinds the camera and reduces the performance of the image sensor. When it is possible, the camera shall be positioned with the sun shining from behind the camera.

9.2.5 To avoid having too much contrast caused by viewing too much of the sky with outdoor cameras, the cameras shall be adequately mounted high above the ground using a pole if needed.

9.2.6 Coverage assessment shall be conducted to identify the optimum locations for video cameras to minimize the dead zone.

9.2.7 Grounding and Bonding of poles and metallic materials shall comply with SAES-P-111 and SAES-T-795.

9.2.8 Enclosures/housing in severe corrosive environments shall be stainless steel NEMA Type 4X or IEC 60529 Type IP66. Refer to SAES-J-902 paragraph 7

9.2.9 Housing shall be large enough to mount the camera and its auxiliary components and to provide easy access for maintenance.

9.2.10 Appropriate spacing between the camera and adjacent surfaces or structure shall be left to facilitate access to the camera for maintenance services.

9.3 Cabling

9.3.1 Video Surveillance network shall use standard network cables. Acceptable cable type shall be:

a. UTP CAT 6 or better.

b. Multimode and single mode fiber optic cable.

c. If an analog camera is used, then it shall be connected to the encoder using RG 59, RG 11, or RG 6 Coax cable.

9.3.2 Outdoor industrial grade Ethernet cable shall be used for outdoor camera with proper housing/conduit.

9.3.3 A media converter (transceiver) may be used to convert between the different communication cables. However, avoid the use of media converter, whenever possible.

9.3.4 Conduits

9.3.4.1 Conduit system installations and requirements shall comply with SAES-T-911, SAES-T-916 and SAES-P-104

9.3.4.2 Metallic conduit shall be grounded as required in SAES-T-795 and SAES-P-111.

9.3.5 Cable Trays

9.3.5.1 Cable trays system installations and requirement shall comply with the following:

a. SAES-T-916 for indoor (inside buildings) installation

b. NEMA V1 for cable tray specification

c. SAES-P-104 for cable tray materials specification

d. SAES-J-902 for cable tray installation and cable protection.

e. NEC Article 392 for cable tray fill area.

f. NEMA VE-2 for cable tray installation guidelines

9.3.5.2 Cable trays shall be installed as a complete system. Cable tray systems shall not have mechanically discontinuous segments of cable tray runs.

9.3.5.3 Cable tray cover is required for additional protection, and the covers or enclosures providing the required protection shall be of a material that is compatible with the cable tray.

9.3.5.4 For cable tray supporting fiber optic armored cables shall be ventilated bottom, channel or trough cable tray type. The cable tray shall be designed, manufactured, and marked in accordance with NEMA VE 1.

9.3.5.5 For cable tray supporting fiber optic armored cables shall be ventilated bottom, channel or trough cable tray type. The cable tray shall be designed, manufactured, and marked in accordance with NEMA VE 1.

9.4 PTZ Control

9.4.1 In case of IP camera, the PTZ control signal shall be sent through the UTP cable of the IP camera with the video signal. A separate cable for PTZ control shall be unacceptable for IP camera.

9.4.2 If analog camera is used, a separate cable (RS232, RS422, or RS485) may be used for PTZ control from the encoder to the analog camera if carrying the PTZ control signal on the Coax cable (In-Coax PTZ control) with the video signal is not possible.

9.5 Power Supply

Video surveillance system electrical power requirements shall comply with SAES-P-100 and SAES-T-795.

If the distance from IP camera to the data switch/midspan is less than 100 m, power to the IP camera should be carried over the UTP cable using Power over Ethernet (PoE and PoE+) technology as defined in IEEE 802.3af and IEEE 802.3at for Cameras with UTP interfaces. IP camera will receive power from PoE and PoE+ enabled Ethernet switch or Midspan through the same UTP cable that transmits data and video. If PoE and PoE+ are used, the camera shall be PoE and PoE+ enabled.

9.6 **Labeling**

9.6.1 Video Surveillance system components and wiring shall be labeled and numbered per section 4.10 of SAES-T-916.

9.6.2 Labels utilized shall be permanent type and shall be designed for the intended use. The painting of numbers on panels or equipment shall not be acceptable.

9.6.3 The use of embossed stick-on labels shall not be acceptable.

9.7 **Documentation**

System documentation shall include the following:

9.7.1 Video Surveillance system operation, inspection and maintenance manuals.

9.7.2 Standard compliance and environmental class certifications.

9.7.3 Network Architectures and System Development Documents

9.7.4 Hardening baseline configuration for all systems

Revision Summary

30 November 2011	New Saudi Aramco Engineering Standard.
24 July 2012	Editorial revision to change the primary contact.
27 October 2017	Major Update, updated scope to include Industrial security systems.
27 October 2020	Major Update, adoption of wireless connectivity and AI's technology for the CCTV cameras, and above ground installation