

Requirements	Classification: Internal
Status: ● Relevant	
Version: 1.0	

TR3033 Industrial Automation and Control Systems Network

Project development
Requirements, TR3033, Version 1.0,

Document replaces version 0

Relevant versions:

- [1.0](#) (2021-05-14 17:42)

1.1 Objective	4
1.2 Target group	4
1.3 Provision	4
2 Introduction	4
3 Network engineering and design	5
3.1 General	5
3.1.1 Criticality assessment	7
3.2 Level 3 Technical network	7
3.3 Level 2 Technical network	8
3.4 Level 3 SAS network	8
3.5 Level 2 SAS network	8
3.6 Level 1 SAS field network	9
3.6.1 General	9
3.6.2 Field Network traffic segregation	9
3.6.3 PRP field networks	9
3.6.3.1 Non-IEC 61850 PRP field network topology	10
3.6.3.2 IEC 61850 PRP network	10
4 Software	11
4.1 General	11
4.2 Equipment message logging	12
4.3 Message log monitoring software	12
4.4 Management software	12
4.5 Identity and access management software	13
5 Components	13
5.1 General	13
5.2 Standardisation	14
5.3 Network equipment	14
5.3.1 Firewalls	14
5.4 Computers	15
5.4.1 Servers	15
5.4.2 Clients	15
5.4.3 Virtual computers	15
5.5 Provisioning of new devices / replacement of devices	16
6 Backup and recovery	16
7 Testing	16
7.1 Test during implementation	16
7.2 Test during commissioning	16
8 Additional information	16

8.1 Definition and abbreviations 16

 8.1.1 Definitions 16

 8.1.2 Abbreviations 22

8.2 Changes from previous version 23

8.3 References 23

1 Objective, target group and provision

1.1 Objective

The objective of this document is to define design requirements for the on-premise Industrial Automation and Control Systems (IACS) Ethernet-based networks, and technical requirements for network and client / server equipment used in IACS. Many of the requirements in this document will aid compliance with TR1658.

IACS covers in this context all networked systems installed on-premise to facilitate the production facility operations, e.g. Industrial Control Systems (ICS), condition monitoring systems, telecommunication infrastructure, operational management systems, etc.

For modifications to systems in operation some requirements in this document may conflict with the installed solution. Conflicts are to be assessed during the front-end engineering phase, and where local design will be maintained, substitution/addendum requirements should be made in accordance with TR0002 "Management system principles".

The project must identify whether Company provided items should be utilized for parts of deliveries, e.g. monitoring and management software, software licenses, equipment hardware etc.

1.2 Target group

The target group for this document is personnel that specify, engineer, fabricate, install, maintain, modify, upgrade or operate IACS networks.

1.3 Provision

Provision is made in Company Management System (TR3030 "Automation, Technical requirements and standards").

2 Introduction

The IACS are critical for enabling a safe, efficient and sustainable operation of the production facility, and therefore have high demands regarding network availability and data integrity. Due to the IACS critical function they also are a high risk target for cyber threats.

It is therefore important that the network design and the components used in the network, enables secure resilient quality network services. Figure 1 below visualise a basic network architecture for an upstream oil & gas production facility that incorporate security through zones and conduits, and availability through pre-defined network types. Note that additional conduits may apply based on design choices made.

Supervisory monitoring and network management is a prerequisite to enable an safe and efficient operation of the networks. This requires standardisation.

As such the main strategy is to require strong and resilient IACS network infrastructure, and require the use of firewalls, VLANs and QoS to protect the IACS components to the greatest practical degree from cyber threats and disturbances in the network.

Such a strong network infrastructure generally requires managed and redundant networks, preferably with zero fail-over time in case of a network failure or network maintenance. Each IACS device or computer is connected directly to a switch to allow the network to control the traffic going to the device.

In order to ensure cyber security and the integrity of the IACS system, the IACS network infrastructure is structured

according to IEC 62264-1:2013-05 clause 5.2.1, also known as the Purdue Architecture for IACS". The different levels can be seen in figure 1 below. Note the locations of the firewalls, and that it is generally permitted for control and service traffic to share the same physical network where necessary.

The document also states some common requirements to computers used for engineering and monitoring purposes. This to ensure we utilize shared resources where applicable, increased standardization and simplify operation/maintenance of the equipment.

Please note that additional requirements may apply as specified in other discipline technical requirement documents.

3 Network engineering and design

3.1 General

SR-77004 - The following physical IACS network infrastructures shall be available at the facility:

1. Level 3 Technical Network
2. Level 3 SAS network
3. Level 2 Technical Network
4. Level 2 SAS HMI and Control networks
5. Level 1 SAS Field networks as applicable
6. Additional ICS internal networks as required by system specific requirement

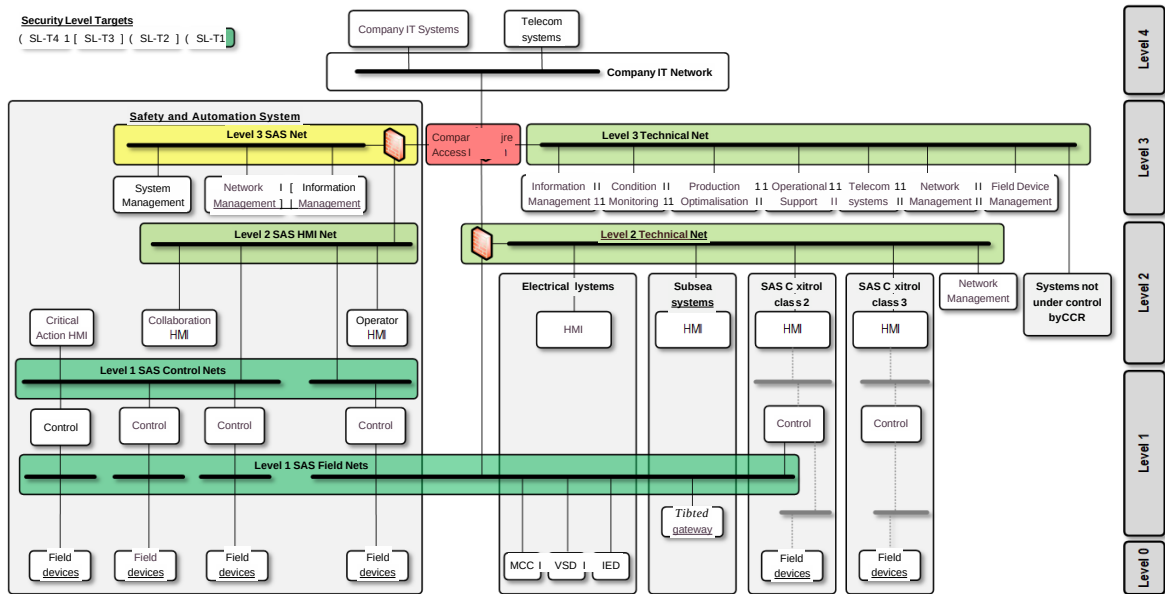


Figure 1 Example of Upstream Oil & Gas facility zones and conduits model. SL-T levels in the figure are only guidance. TR1658 shall be followed to assess which SL-T to be used and placement of conduits.

Not all network connections in the figure between "control zones" are necessarily used for control traffic, some information and general alarms may be transported through the same physical layer, e.g. for CC3 connections to the Field network, as such information normally is received through the control nodes by the SAS system.

If connectivity is needed between HIPPS/FWP/EmG to ensure monitoring and possible remote this may be solved by a control mechanism in a conduit.

SR-77134 - The IACS networks shall support integrated security concepts as defined by TR1658.

SR-86592 - The IACS network design shall safeguard aspects for facility operation, system independence, system performance and technology used.

SR-86591 - Effort shall be made to share infrastructure within the individual physical infrastructures where possible based on risk assessments done. Requirements to the following needs to be maintained in the design:

1. System independency, reliability, availability, maintainability, and performance
2. Cyber security
3. Network monitoring and management

SR-76647 - Separate network management solutions customized to Company operational model shall be designed for:

1. Level 3 Technical network and firewall equipment, including connected EPU control system edge network switches
2. Level 2 Technical network and firewall equipment, including connected EPU control system edge network switches
3. Level 3, 2 and 1 SAS network and firewall equipment

The system specific TRs may put additional requirements to management solution for additional IACS internal networks.

SR-86589 - The high availability networks design shall be limited to use the following network protocols in accordance with IEC 62439:

- Parallel Redundancy Protocol (PRP) when zero fail over time is required
- High-availability Seamless Redundancy (HSR) when zero fail over time is required
- Media Redundancy Protocol (MRP)

SR-86756 - RSTP shall not be used as a network redundancy protocol in high availability networks, but may be used to add redundancy to equipment connection on edge switch ports.

SR-92089 - Network edge switch ports (where Devices or Computers are connected) shall have BPDU guard enabled.

SR-86588 - The networks shall have a high availability design when the data communicated is critical for safety or production, or if the connected networked component requires a high availability data link.

SR-86587 - The networks shall have capacity to handle the data load for all operational modes.

SR-77150 - The IACS networks shall be scalable with respect to capability and capacity.

SR-77160 - The IACS networks shall be based on recognised open industry standards.

SR-77459 - The IACS networks shall support Quality of Service (QoS) functionality.

SR-86585 - The networks shall support Virtual Local Area Network (VLAN) functionality.

SR-77669 - The IACS networks shall prioritise IACS dependent data traffic over non-dependent data traffic if deployed on a shared physical network infrastructure.

SR-86586 - The IACS networks design shall protect the networked components from unwanted network traffic where relevant.

SR-77163 - The IACS networks shall be able to distribute time to networked components.

SR-77648 - Time in redundant network configurations shall be sourced from redundant Real Time Clocks.

SR-77133 - The IACS networks shall support end-to-end connectivity for management data where required.

SR-79218 - The network IP plan shall be pre-approved by Company.

SR-78009 - Computers, except server hardware used for virtual hosts, shall not be connected to different networks by-passing installed firewalls.

SR-91917 - Server hardware used for virtual hosts shall not be connected across different Purdue levels.

SR-86593 - If encrypted data links are used between networks on different levels, the traffic shall be decrypted before entering end-point firewalls with DPI and IDS enabled.

SR-86697 - The IACS systems shall be designed so that the use of (Supplier) laptops and similar portable computers is not required for configuration, operation or maintenance.

SR-86696 - Software applications necessary for maintenance, configuration and parameterisation of the IACS systems shall be included and installed on Engineering work stations.

3.1.1 Criticality assessment

SR-76646 - Data links shall be identified and classified in accordance with its consequence for facility safety, information security and production.

The framework described in NOG 123 can be used for this assessment.

SR-77911 - Cyber Security Risk assessment for the System under Consideration (SuC, ref TR1658) shall be done to identify the network infrastructure to be utilized.

3.2 Level 3 Technical network

The Level 3 Technical network should be used for systems with facility functions and to provide network connection to off-premise Company IT solutions through the Company secure access solution.

SR-86613 - Systems critical for facility safety or production shall not be dependent of the Level 3 Technical network to execute its function.

SR-86612 - The Level 3 Technical core network layer shall have a fault tolerant design.

A Level 3 Technical distribution network layer should be used where there is a need for aggregating network layers and provide unique connectivity services within a distribution network segment.

SR-86617 - The Level 3 Technical network shall provide distribution, policy control, and isolation points between the network segment and the rest of the IACS networks.

SR-86616 - The Level 3 Technical network shall have a fault tolerant design towards the core or distribution network.

SR-86615 - The Level 3 Technical network shall be connected to a high availability firewall solution in the Company secure access solution for secure data traffic within and to/from the network.

SR-77773 - The Level 3 Technical network components shall be compatible and integrated with Company centralised Level 3 Technical network management system.

3.3 Level 2 Technical network

The Level 2 Technical network should be used for operational management solutions in IACS other than SAS that is considered high critical based on the Cyber Security risk assessment, and to provide network connection to solutions in the Level 3 IACS network.

SR-86620 - Systems critical for facility safety or production shall not be dependent of the Level 2 Technical network to execute its function.

SR-86619 - The Level 2 Technical core network layer shall have a fault tolerant design.

A Level 2 Technical distribution network layer should be used where there is a need for aggregating network layers and provide unique connectivity services within a distribution network segment.

SR-86623 - The Level 2 Technical network shall have a fault tolerant design towards the core or distribution network.

SR-86622 - The Level 2 Technical network shall have a high availability firewall solution installed to restrict data traffic within and to/from the network.

3.4 Level 3 SAS network

The Level 3 SAS network should be used for operational management solutions in SAS and to provide network connection to solutions in the Level 3 Technical network.

SR-86636 - Systems critical for facility safety or production shall not be dependent of the Level 3 SAS network to execute its function.

SR-86635 - The Level 3 SAS core network layer shall have a fault tolerant design.

SR-86634 - The Level 3 SAS network shall provide distribution, policy control, and isolation points between the network segment and the rest of the network.

SR-86633 - The Level 3 SAS network shall have a fault tolerant design towards the core network.

SR-86632 - The Level 3 SAS network shall have a high availability firewall solution installed for secure data traffic within and to/from the network.

3.5 Level 2 SAS network

The Level 2 SAS HMI network should be used for the HMI system in SAS and to provide connection to solutions in the Level 3 and 1 SAS networks.

SR-86631 - The Level 2 SAS HMI core network layer shall have a high availability design.

SR-86627 - The Level 2 SAS HMI edge switches shall have a high availability design towards the core network.

The Level 2 SAS control networks should be used for controller to controller data traffic and to provide network connection to solutions in the Level 2 SAS network and Level 1 SAS field networks.

SR-86625 - The Level 2 SAS control core network layer shall have a high availability design.

SR-86626 - The Level 2 SAS control edge switches shall have a high availability design towards the core network.

3.6 Level 1 SAS field network

3.6.1 General

The Level 1 SAS field networks should be used for data traffic to/from field devices and to provide network connection to solutions in the Level 2 SAS control networks.

SR-86639 - The Level 1 SAS field networks layer shall have a high availability design.

SR-86644 - A SAS Level 1 field distribution network layer shall be used where there is a need for aggregating network layers and provide unique connectivity services within a distribution network segment.

SR-86643 - Where independent A and B cable routing is required, separate Level 1 SAS core network switches shall be used.

SR-86642 - The Level 1 SAS PCS field networks shall have a redundant firewall solution installed for enabling secure data links between the field devices and the management solutions.

SR-86687 - The level 1 IEC 61850 network shall use PRP, specified in Clause 4 of IEC 62439-3:2012, both for Station Bus and (if implemented) Process Bus.

3.6.2 Field Network traffic segregation

SR-86683 - Each SAS logic solver shall have a separate VLAN for field network communication.

Such VLAN may be shared for PROFINET and Modbus TPC if a common port is used. VLAN may be shared between controllers required to communicate with the same devices.

SR-78573 - Non-SAS logic solvers in Class 2 packages, which use the field network to communicate to e.g. MCCs, shall have separate VLANs for this purpose.

SR-78572 - Level 2 Technical network traffic shall be in separate VLANs to the SAS VLANs, where the device supports this.

3.6.3 PRP field networks

SR-77672 - PRP field networks shall have a dual star design as indicated in the figure below.

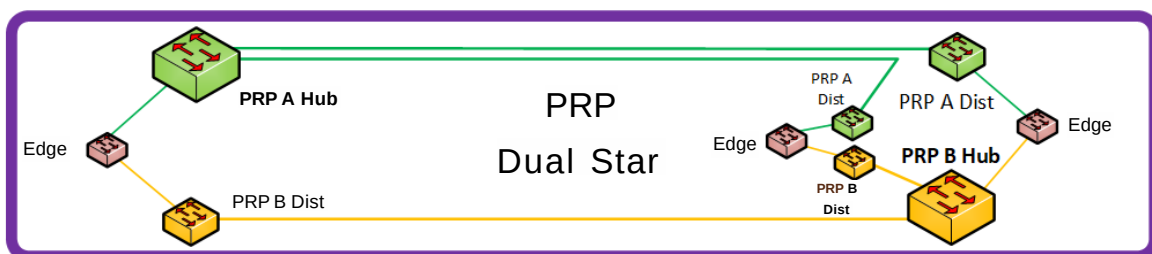


Figure 2 Diagram showing principle of locating the two PRP hubs physically separate

SR-78496 - Devices and computers which does not support PRP shall be connected using a redbox.

SR-78494 - Devices and computers shall be connected to a port on a switch.

SR-78553 - If the SAS logic solver does not support PRP, one redbox shall be used for connecting PRP A and PRP B to the SAS A network, and another redbox shall be used for similar connection to the SAS B network.

SR-78551 - Communication to Level 2 Technical network shall be done through a separate redbox.

3.6.3.1 Non-IEC 61850 PRP field network topology

In order to implement shared network infrastructure for the field ne works (IEC 61850 and non-IEC 61850) the non-IEC 61850 network should be implemented with PRP.

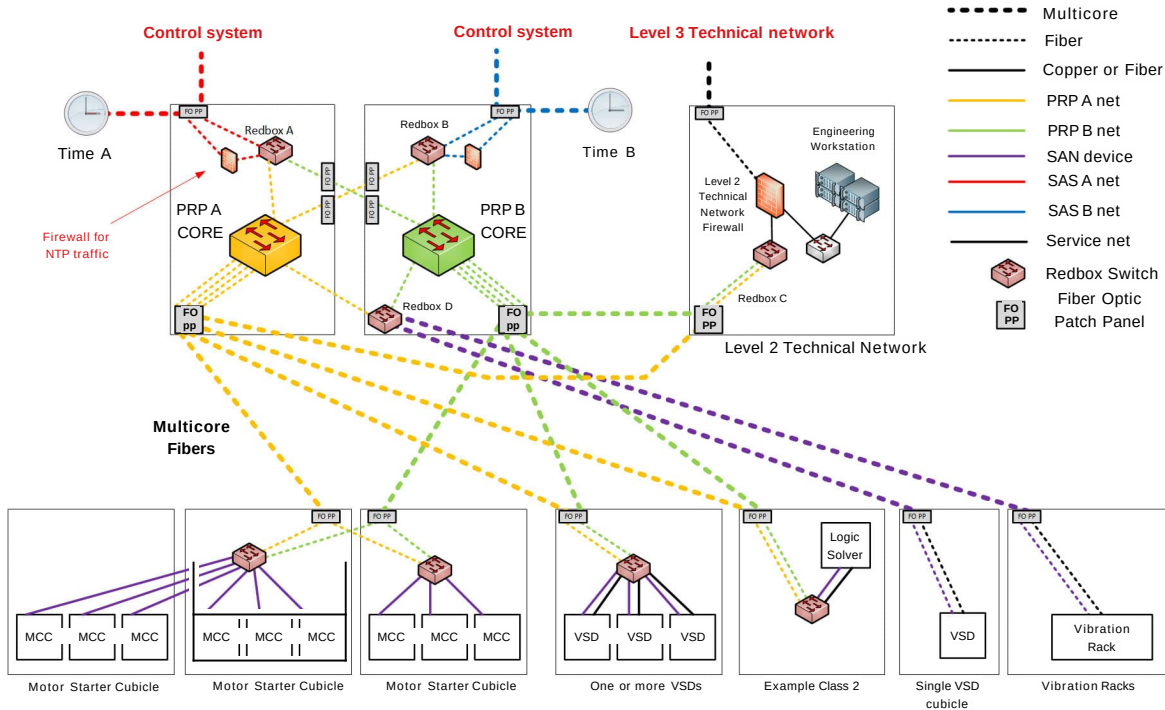


Figure 3 Principle drawing for non-IEC 61850 field network based on PRP, typically used for PROFINET and Modbus TCP.

Individual Class 2 packages with dedicated SAS logic solvers may have individual links to e.g. a VSD, but communicate via the PCS field network to equipment from other packages (e.g. MCCs in electro packages).

3.6.3.2 IEC 61850 PRP network

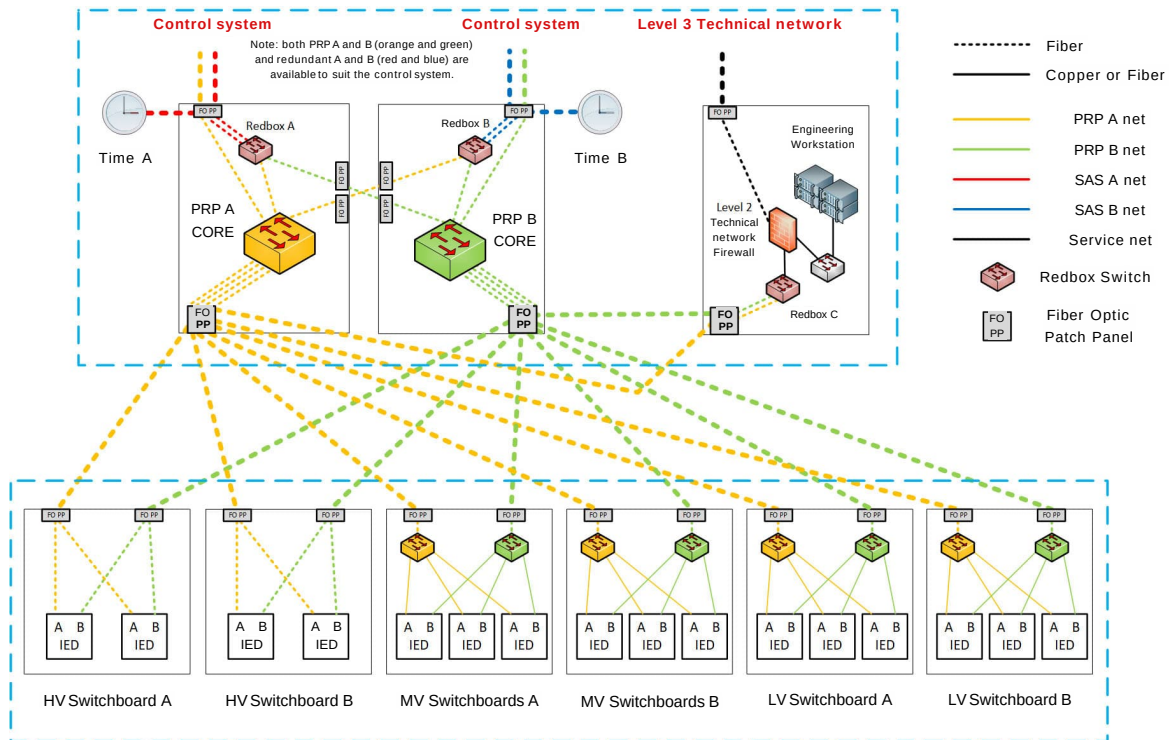


Figure 4 Principle drawing for IEC61850 station bus network topology using PRP

IEDs should connect to the network using PRP, without the use of a redbox.

SR-78543 - Switches used in IEC 61850 networks shall not enable write MMS support.

SR-78542 - Where PTP is required, switches used in IEC 61850 networks shall support PTP.

4 Software

4.1 General

SR-83694 - The project shall in due time get a final acceptance from Company on the software products chosen.

SR-83693 - The agreed official software version for all software components shall be available for installation before project handover to operation.

SR-83695 - All agreed official software patches shall be installed before project handover to operation.

SR-83692 - The operating system shall be of Long-term Support (LTS) version where available.

SR-78030 - Software licenses shall be registered to Company and activated before project handover to operation.

4.2 Equipment message logging

SR-78483 - The network equipment and networked devices message logs shall be based on recognised open standards. The message logs shall also cover security related alarms and events, including remote desktop protocol usage.

For network equipment Syslog (RFC 5424) or SNMP traps are examples of such standards

For clients and servers running Microsoft Windows operating system, the Default Audit logging must enable Success/Failure on account logon events, account management, logon events, object access, policy change, system events.

SR-78482 - The network and networked equipment shall provide data for inventory, backup status, health and performance.

Use of staging should be considered to avoid unnecessary exposure to external networks.

4.3 Message log monitoring software

SR-81821 - The message log monitoring software and protocols shall be based on recognised open standards.

SR-78484 - The facility shall have a message log monitoring solution for capture and storage of message logs from all networked IACS.

SR-78477 - The message log monitoring solution shall provide a secure interface for communicating message log data to other Company systems.

SR-78478 - The message log monitoring solution shall be able to save all messages to files on a Company file share.

SR-78464 - The message log monitoring solution shall include a historian module for capturing and storing time stamped equipment data.

SR-78470 - The message log monitoring solution shall as a minimum provide the following information:

1. Equipment capacity and performance
2. Equipment health condition
3. Equipment hardware and software inventory
4. Network infrastructure topology
5. Backup status
6. Cyber security related alarms and events, including remote desktop protocol usage

4.4 Management software

The management software covers configuration management of network equipment and client/server equipment.

The management software should be based on recognised open standards.

SR-86597 - The management software communication with equipment in scope shall utilise secure protocols.

SR-81833 - The management software shall support the life-cycle of services needed to install, configure, troubleshoot, repair and maintain equipment throughout the life of the facility.

SR-81838 - The management software shall include a module for capturing changes to the hardware configuration, back-up the configurations and ability to load them to the hardware component.

SR-81837 - It shall be possible to recover configuration data on the management software from backups.

4.5 Identity and access management software

The Identity and access management software covers user access management and security management of network equipment and client/server equipment.

SR-86601 - The system shall support different levels of user access rights to prevent unauthorised access to system and application software.

SR-86600 - The system shall have a role-based access allowing assignment of users/user groups to roles.

SR-86599 - It shall be possible to configure the access roles to limited parts of the system and/or limited parts of the application software.

SR-86598 - The identity and access management software shall include functionality for cyber security controls including audit controls. As a minimum the following are to be included:

1. Identity management: Manage identities for accessing the network management, manage external account service connection.
2. Access management: Manage accesses, roles, privileges for roles, mapping to identities
3. Accounts: Manage accounts that access the system management server resources
4. Credentials Management; Manage identity proof levels, interactions with Identity/account service
5. Certificates; Certificate Authority
6. Access Management; Manage role-based privileges

5 Components

5.1 General

SR-86605 - The project shall in due time get a final acceptance from Company on the network equipment and computer hardware standardisation chosen.

SR-79188 - Replacement of redundant hardware components shall be possible during normal operation, without any loss of functionality or production.

SR-86604 - The network equipment and networked computers shall be able to export message logs including alarm and events (security events included).

SR-86603 - The networked components shall support connectivity without need of extensive manual integration services.

SR-86608 - The networked components shall communicate by the use of Ethernet.

SR-86607 - All unused communication ports on network equipment and networked components shall be locked, disabled or protected by software means. If not possible through software, a physical port lock product shall be used.

SR-86606 - The network equipment and networked components shall handle wire-speed network storms gracefully, i.e. network port may be shut down temporarily but shall automatically be re-enabled when the storm has ended.

SR-86699 - Devices with a Ethernet service port; these shall be connected to the network.

SR-78500 - Devices with a serial/USB service port; these shall be connected to the network using a serial/IP server.

It is not necessary to connect multiple service ports if the functionality is already taken care of for the device.

SR-78501 - Devices with only one network interface shall support both control and service traffic.

5.2 Standardisation

The network equipment for use in protected area should be from one manufacturer and of the same product family.

The network equipment for use outside protected area should be from one manufacturer and of the same product family.

SR-79191 - The client hardware shall be from one manufacturer and of the same product family within a system.

SR-79186 - The server hardware shall be from one manufacturer and of the same product family within a system.

SR-86610 - The network equipment and computer hardware shall be commercial of the shelf products that are suitable for its intended use.

5.3 Network equipment

SR-86611 - The network equipment shall support the communication protocol used.

SR-79202 - The network equipment shall have rack or DIN rail mount.

SR-79200 - The network equipment shall have minimum 2 up-link ports.

SR-79199 - The internal power supplies in the network equipment shall be active redundant.

SR-79208 - The network equipment for use outside protected area shall be fan-less.

SR-79207 - The network equipment used in the core or distribution networks shall have minimum 1 Gigabit/s bandwidth on uplinks and edge ports.

SR-79210 - The network equipment shall be able to be managed from the management software.

SR-79212 - The network equipment shall do automatic startup with correct configuration without any user intervention after loss of power.

SR-79209 - The network equipment's configuration shall be available for online or offline upload after replacement of component.

SR-81377 - Where redbox functionality is needed; the edge switch shall support redbox functionality.

5.3.1 Firewalls

SR-78016 - Firewalls shall deny data flow by default.

SR-78015 - All data flows shall explicitly be configured in the firewall rulesets.

SR-78021 - The main firewall solutions at Level 3 Technical network, Level 3 SAS Technical network and Level 2 Technical network shall be redundant firewall cluster solutions with state synchronisation that support Deep Package Inspection (DPI) and Intrusion Detection System (IDS).

SR-84565 - The management interface of the firewalls shall be protected.

SR-86649 - The main firewall at Level 2 Technical network shall be integrated with an independent managed barrier solution, including a HMI panel from the user's work desk, for open/close of predefined firewall rulesets.

5.4 Computers

5.4.1 Servers

SR-77781 - Server hardware with server operating system shall be used as run-time environment when Level 2 or Level 3 application software demands for 24x7 operation.

SR-77780 - Server hardware shall run a virtualisation environment.

SR-78010 - Server hardware shall include a dedicated out-of-band management interface.

SR-79217 - The server hardware shall have rack or DIN rail mount.

SR-79216 - The server hardware shall be fault tolerant against disk failures and with automatic online recovery when replacing a disk.

SR-79215 - The internal power supplies and fans in the server hardware shall be active redundant.

SR-78032 - All application software with a demand for 24x7 operation installed in the server shall run as a service in the background, independently whether interface user is logged in or out to the applications.

5.4.2 Clients

SR-77779 - Client hardware with end user operating system shall be used when functionality is to provide HMI to users working in protected area.

Some HMIs may be delivered as built-in panels, included as part of PLCs etc, thereby not using standard client hardware.

SR-77782 - Clients shall run as bare metal installation, no virtualisation required.

The client hardware may be removed if the system solves the same with a virtual computer as part of a Server hardware.

5.4.3 Virtual computers

SR-86609 - Virtual machines shall run on a server hardware.

SR-78012 - A dedicated physical network port shall be used in the server hardware for connecting the Hypervisor management interface to the relevant management system.

SR-92430 - If a Hypervisor cluster is installed for redundancy, redundancy on management shall be implemented according to best practice from the applicable Hypervisor vendor.

SR-78008 - Virtual machines shall be supplied in Open Virtualization Format (OVF) if the virtual machine is to be implemented on a Hypervisor from another delivery.

SR-78007 - All virtual disks shall be thick provisioned Lazy zeroed.

Thick provisioned Eager zeroed virtual disks may be used if vendor application requires it.

SR-92429 - Virtual hardware allocation shall be in accordance to actual needs and have the capacity to handle predicted growth.

5.5 Provisioning of new devices / replacement of devices

SR-78024 - Supplier shall provide a procedure, and necessary hardware and software (e.g. cables, converters, drivers), used for initial provisioning of replacement parts (i.e. a new out-of-the-box device).

SR-78023 - The provisioning of the new device shall be done using applications on the EWS.

SR-78027 - The provisioning procedure shall include enabling of ports, configuring IP addresses and other details necessary for the new device to be inserted into the network and receive its main configuration from the EWS.

SR-78026 - Initial configuration using a network cable shall be preferred over USB.

6 Backup and recovery

SR-78034 - The facility shall provide for shared backup solution for the network connected systems.

SR-78033 - Larger infrastructures (e.g. SAS) shall provide their own internal backup solution which may utilize the shared facility solution for offline backup.

SR-78036 - To reduce the amount of data being synchronized to onshore centralized storage for offsite backup, systems shall use block level backup rotation when offline backup is copied to the shared facility solution.

SR-79219 - The components configuration shall be available for online or offline upload after replacement of equipment.

7 Testing

7.1 Test during implementation

SR-78784 - During the implementation of a system it shall be planned for a Cyber Security and Network test.

SR-78788 - It is required that supplier tests specifications are extended to include test procedure and expected results.

7.2 Test during commissioning

SR-78787 - When the system is delivered and to be powered up for commissioning activities it shall be planned for necessary activities to ensure remaining interface and communication connections are done.

SR-78786 - To ensure the integrity of the delivered system before connecting it to the network a Cyber Security procedure for update and scanning shall be made and executed.

8 Additional information

8.1 Definition and abbreviations

8.1.1 Definitions

Application

In this document, this word refers to software applications which are installed on a general-purpose Operating System.

Application software

Production facility specific run-time applications / configuration

Availability

Property of ensuring timely and reliable access to and use of control system information and functionality. (Source: IEC

62443-1-1:2007)

Block level backup

In block-level incremental backups, the backup software identifies the data blocks that have been changed since the most recent backup job and copies them to the backup repository. Block-level tracking allows a more granular approach compared to backing up entire files, as in file-level incremental backup.

BPDU guard

PortFast BPDU guard prevents loops by moving a non-trunking port into an "errdisable state" when a BPDU is received on that port. When you enable BPDU guard on the switch, spanning tree shuts down PortFast-configured interfaces that receive BPDUs instead of putting them into the spanning tree blocking state.

Can

Statements of possibility and capability, whether material, physical or causal. (Source: Company Management system)

Client

When preceding the word "Computer", a "Client Computer" means a computer which is typically used to access other Components, for operation or maintenance tasks such as troubleshooting, diagnostics or configuration.

A Client Computer does not need to run 24/7, and applications can depend on a user session (i.e. a human user logged in) to be started.

The word "Client" may also be used about one of the two roles ("Client" or "Server") in a network protocol connection, such as "SSH Client". In this meaning, the protocol name is always preceding the word "Client".

The term "Client Application" may also be used. This means that the application has a Client / Server architecture, and the "Client Application" refers to one of the two peers of this application architecture.

Company

Equinor

Components

A common term for Computers, Devices and Network Equipment.

Computer

A Commercial-Off-The-Shelf (COTS) computer running a general-purpose operating system like Windows Server, Windows LTSC or Linux based operating systems such as (but not limited to) Ubuntu Server, RedHat Server etc. The word "Computer" reflects an instance of an operating system, and this can be installed either on a dedicated, physical computer, or on a virtual computer (also referred to as a "Virtual Machine").

Note that a rugged / industrial computer built on the Intel / AMD CPU architecture, and running the Operating Systems mentioned above, are also considered a "Computer".

Conduit

A conduit regulates communication between one or more devices in the same security zone or different security zones. A conduit within a security zone could be the control center LAN. A conduit between two zones could be the WAN connection between the primary and backup control centers. Conduits can be trusted or untrusted. Each conduit is assigned a security level.

From IEC62443-1-1 (chap 10.2.3): Information must flow into, out of, and within a security zone. Even in a non-networked system, some communication exists (e.g., intermittent connection of programming devices to create and maintain the systems). To cover the security aspects of communication and to provide a construct to encompass the unique requirements of communications, this standard is defining a special type of security zone: a communications conduit.

A conduit can be a single service (i.e., a single Ethernet network) or can be made up of multiple data carriers (multiple network cables and direct physical accesses). As with zones, it can be made of both physical and logical constructs. Conduits may connect entities within a zone or may connect different zones.

As with zones, conduits may be either trusted or untrusted. Conduits that do not cross zone boundaries are typically trusted by the communicating processes within the zone. Trusted conduits crossing zone boundaries must use an end-to-end secure process.

Untrusted conduits are those that are not at the same level of security as the zone endpoint. In this case the security of the communication becomes the responsibility of the individual channel. Further information on this scenario is available in the Annex.

A conduit regulates communication between one or more devices in the same security zone or different security zones. A conduit within a security zone could be the control center LAN. A conduit between two zones could be the WAN connection between the primary and backup control centers. Conduits can be trusted or untrusted. Each conduit is assigned a security level.

Data

Representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. (Source: ISO/IEC/IEEE 24765:2017).

Data link

Means of connecting one networked device to another for the purpose of transmitting and receiving digital information.

Devices

Devices, also referred to as “Embedded Devices”, are components such as (but not limited to) PLCs, VSD controllers, Motor starters, Thyristor controllers, Flow computers, IEDs, Serial servers, Communication devices, Advanced analysers etc.

A “Device” is basically any configurable / programmable Component which is not considered a “Computer” or “Network Equipment”.

Note that Windows CE (Compact Embedded), or Windows IoT Core, are not considered general-purpose Operating Systems. Components running these operating systems (typically local HMI Panels) are considered “Devices”.

Distribution network layer

The distribution layer aggregates the uplinks from the edge (also called access) layer to the core network layer. See “Network distribution switch”.

End user

In product development, an end user (sometimes end-user) is a person who ultimately uses or is intended to ultimately use a product. The end user stands in contrast to users who support or maintain the product.

Engineering Work Station

The maintenance stations for industrial control systems where system management and application software engineering, configuration, testing and surveillance are performed.

Firewall

A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network. (Source; Wikipedia)

High Availability

A characteristic of a system, which aims to ensure an agreed level of operational performance, usually uptime, for a higher than normal period. (Source; Wikipedia)

Human-Machine Interface (HMI)

Provides the physical interface between technical systems and the personnel operating and maintaining the production facility, e.g. operator stations, large screen displays, critical action panels present in control rooms, local control panels and engineering work stations.

Hypervisor

A hypervisor is a computer software, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources. (Source; Wikipedia)

Intelligent electronic device (IED)

Microprocessor-based controllers of power system equipment, such as circuit breakers, transformers and capacitor banks. IEDs receive data from sensors and power equipment and can issue control commands, such as tripping circuit breakers if they sense voltage, current, or frequency anomalies, or raise/lower voltage levels in order to maintain the desired level.

May

Indicates a course of action permissible within the limits of the document. (Source: Company Management system)

Network equipment

Electronic devices which are required for communication and interaction between devices on a computer network, also known as Networking hardware, e.g. switches, firewalls, routers, etc. (Source; Wikipedia)

Network equipment management

Services provided include fault analysis, performance management, provisioning of networks/network equipment and maintaining quality of service.

Network core switch

A core switch is a high-capacity switch generally positioned within the backbone or physical core of a network. Core switches provide the final aggregation point for the network and allow multiple aggregation modules to work together. The core is designed to be highly reliable and stable to aggregate all the elements in the operational facility, typically Layer 3 (ISO/IEC 7498) devices, with high speed connectivity, redundant links, and redundant hardware.

Network distribution switch

The distribution layer in provides policy-based connectivity and demarcation between the access layer and the core layer. In small-to-medium size networks, it is possible to collapse the core into the distribution switches.

Network edge switch

The edge switch (also called access switch) provides the demarcation between the network infrastructure and the devices that leverage that infrastructure. As such, it provides a security, QoS, and policy trust boundary. When looking at the overall IACS network design, the edge switch provides the majority of these access layer services and is a key element in enabling multiple IACS network services.

Network message log server

In computing, a log file is a file that records either events that occur in an operating system or other software runs, or

messages between different users of a communication software. Logging is the act of keeping a log. In the simplest case, messages are written to a single log file. Many operating systems, software frameworks and programs include a logging system. A widely used logging standard is syslog. The Network message log server provides storage of syslog messages / SNMP traps with functionality like forwarding, filtering, analysis etc.

Network Time Protocol (NTP)

Protocol used to synchronize clocks throughout a computer network, defined in RFC documents. The current protocol is version 4 (NTPv4), which is a proposed standard as documented in RFC 5905. It is backward compatible with version 3, specified in RFC 1305.

Operator station

HMI equipment where the operator can perform control and monitoring. One or more operator stations will form an operator workplace.

Protected area

This term is used to address location of non-explosion protected safety critical equipment such that the probability of gas exposure to ignition sources or damage is as low as reasonably practicable. Such equipment will be protected long enough to carry out safety functions. Such locations should be in the accommodation or in utility area close to the accommodation area. Probability for exposure of equipment within the enclosure to gas releases at 20% LEL, typically 10-4 per year or less. Special provisions, e.g. gas detection and means for isolating ignition sources, may be required. (Source: TR1055 v9.0)

Precision Time Protocol (PTP)

Protocol used to synchronize clocks throughout a computer network, defined in IEEE 1588 v2.

Quality of Service (QoS)

QoS refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. QoS is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. (Source; Wikipedia)

Redbox

Short form for Redundant Box. A network switch with PRP functionality, used in IEC 61850 networks, for connecting single attached devices to a PRP network.

Redundancy

The presence of auxiliary equipment in a system to perform the same or similar functions as other elements for the purpose of preventing or recovering from failures. (Source: ISO/IEC/IEEE 24765:2017)

Real Time Clock (RTC)

A computer clock (most often in the form of an integrated circuit) that keeps track of the current time. (Source; Wikipedia)

SAS Control class 2

Control and/or monitoring functions are partially integrated into SAS. Non-SAS control equipment are either directly connected to SAS network or interfaced to other SAS equipment via communication link. Systems and equipment under control are operated and monitored through SAS HMI following SAS HMI standard for uniform operation.

SAS Control class 3

Control and monitoring functions are not integrated in SAS. No interface to SAS is required, however supervisory control or monitoring from SAS HMI could be applied. Systems and equipment under control are operated and monitored through stand-alone HMI.

Scalability

The degree to which a system can have its capacities adjusted to meet system requirements. (Source: O-PAS™ Standard - Glossary and Abbreviations:2019)

Security

1. measures taken to protect a system
2. condition of a system that results from the establishment and maintenance of measures to protect a system
3. condition of a system resources being free from unauthorized access and from unauthorized or accidental change, destruction or loss
4. capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet ensure that this is not denied to authorized persons and systems
5. prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system

Note: Measures can be controls related to physical security (controlling physical access to computing assets) or logical security (capability to login to a given system and application). (Source: IEC 62443-1-1:2009)

Server

When used as a standalone word, this means a computer with an operating system like Windows Server, Ubuntu Server, RedHat Server etc. A computer that shall run 24/7, and that runs applications as services / daemons which do not depend on any human user session (i.e. a user logged in) to run. A Server can be either a dedicated, physical server, or a virtual machine.

The word "Server" may also be used about one of the two roles ("Client" or "Server") in a network protocol connection, such as "SSH Server". In this meaning, the protocol name is always preceding the word "Server".

The term "Server Application" may also be used. This means that the application has a Client / Server architecture, and the "Server Application" refers to one of the two peers of this application architecture.

Service port

An interface on a component which is used for configuration, troubleshooting, diagnostics or other maintenance needs. It may also be used for monitoring, time synchronization etc.

Shall (requirement)

Requirement strictly to be followed in order to conform to the document and from which no deviation is permitted, unless a deviation permit is approved. (Source: Company Management system)

Should (recommendation)

Indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) possibility or course of action is deprecated but not prohibited. (Source: Company Management system)

Simple Network Management Protocol (SNMP)

An Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, work stations, printers, and more.

Software components

Computer programs having a defined function required to have a computing device working properly, e.g. hardware managing software (e.g. device drivers, firmware, operating system, etc), application framework software (e.g. supplier's product software platform), application software (e.g. production facility specific run-time applications / configuration)

Syslog

A standard for message logging, defined in Internet Engineering Task Force (IETF) RFC 5424. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each

message is labeled with a facility code, indicating the software type generating the message, and assigned a severity level. May be used for system management and security auditing as well as general informational, analysis, and debugging messages.

System

A set of elements and of relations between the elements such that the set may be looked at as a whole. (Source: ISO 5127/1)

System under Consideration (SuC)

System Under Consideration. IEC62443 term.

Thick provisioning

In virtual storage, thick provisioning is a type of storage allocation in which the amount of storage capacity on a disk is pre-allocated on physical storage at the time the disk is created.

Variable Speed Drive (VSD)

A type of adjustable-speed drive used in electro-mechanical drive systems to control AC motor speed and torque by varying motor input frequency and voltage. (Source; Wikipedia)

Zone

A security zone is a logical grouping of physical, informational, and application assets sharing common security requirements.

A security zone has a border, which is the boundary between included and excluded elements.

Zones may be considered to be trusted or untrusted.

The standard requires a minimum of three security levels for security zones: high, medium and low.

Other Parts of the IEC62443 standard will define administrative and technical requirements for these security levels.

8.1.2 Abbreviations

CC	Control Class
CPU	Central Processing Unit
EmG	Emergency Generator
EPU	Equipment Package Unit
EWS	Engineering Work Station
FW	Firewall
FWP	Firewater Pump
HMI	Human Machine Interface
IACS	Industrial Automation and Control System
IED	Intelligent Electronic Device
IP	Internet Protocol
MMS	Manufacturing Message Specification
NTP	Network Time Protocol
PCS	Process Control System
PRP	Parallel Redundancy Protocol
PTP	Precision Time Protocol
QoS	Quality of Service
RTC	Real Time Clock
SAS	Safety and Automation System

VLAN	Virtual Local Area Network
VSD	Variabel Speed Drive

8.2 Changes from previous version

NA

8.3 References

Company

TR0002 Management system principles

TR1658 Information Security of Automation Systems

TR2258 Information Management System

TR3030 Automation, Technical requirements and standards

TR3034 Safety and Automation System

TR3043 Telecommunication systems

GL0628 Maintenance Engineering in Projects

International standards

IEC 60300 Dependability Management

IEC 61850 Communication networks and systems for power utility automation

IEC 62264 Enterprise-control system integration

IEC 62439 High availability automation networks

IEC 62443 Industrial communication networks - Network and system security