12.7.1 *Systems audit controls*

Control

Audit requirements and activities involving verification should be carefully planned and agreed to minimize disruptions to business processes.

Preservation of:	*CIA*	*Control focus:*	*p*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
The following guidelines should be observed:				
a) audit requirements for access to systems and data should be agreed with appropriate management;	*DEO*	*DEO*	*DEO*	*DEO*
b) the scope of the technical audit tests should be agreed and controlled;	*DEO*	*DEO*	*DEO*	*DEO*
c) audit tests should be limited to read-only access to software and data;	*DEO*	*DEO*	*DEO*	*DEO*
d) access other than read-only should only be *permitted* for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;	*DEO*	*DEO*	*DEO*	*DEO*
f) audit tests that could affect system availability should be run *on a test system* only;	*DEO*	*DEO*	*DEO*	*DEO*
g) all access should be monitored and logged to produce a reference trail.	*DEO*	*DEO*	*DEO*	*DEO*
Tools: Not identified				
Legacy: Not identified				

13 Communications security

Clause 13 of this document contains extracts and modifications from ISO/IEC 27002:2013, Clause 13, as described in 4.3.2.

13.1 Network security management

Objective:

To ensure the protection of information in networks and its supporting information processing facilities *and the I&C systems*.

13.1.1 Network controls

Control

Networks should be managed and controlled to protect information in systems and applications.

Implementation guidance

Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorized access. In particular, the following items should be considered*.*

Other information

Additional information on network security can be found in ISO/IEC 27033 (all parts).

13.1.1.1 a) Responsibilities and procedures for the management of networking equipment

Control

Responsibilities and procedures for the management of networking equipment should be established;

Preservation of:	*CIA*	*Control focus:*	*pdc*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) Responsibilities and procedures for the management of networking equipment should be established;	*DEO*	*DEO*	*DEO*	*DEO*
(B) The respective I&C organization should have the responsibility for the management of *I&C* networking equipment. *It should especially ensure that the I&C border protections remain up to date and fulfil the requirements that are needed to protect the I&C system against connected 3rd party I&C systems or non-I&C systems (e. g. connection between I&C and office system). It is not recommended to delegate this responsibility to the general IT- department, since I&C specific protection needs I&C specialist know how and a broad knowledge of generic I&C concepts.*	$E_{gvsic}O$	$E_{gvsic}O$	$E_{gvsic}O$	$E_{gvsic}O$
Tools: Not identified				
Legacy: Not identified				

13.1.1.2 b) Operational responsibility for networks

Control

Operational responsibility for network should be separated from computer operations where appropriate.

Preservation of:	*CIA*	*Control focus:*	*pdc*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) Operational responsibility for network should be separated from computer operations where appropriate.	*(DEO)*	*DEO*	*DEO*	*DEO*
(B) Operational responsibility for the security of I&C networks and I&C systems in the test bed or on the NPP site should be with one and the same party.	$(E_{gvsic}O)$	$E_{gvsic}O$	$E_{gvsic}O$	$E_{gvsic}O$
Tools: Not identified				
Legacy: Not identified				

13.1.1.3 c) Confidentiality and integrity of *passing data to the I&C system*

Control

Data should not be passed over public networks directly to the I&C system.

Preservation of:	*CIA*	*Control focus:*	*p*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) All data (e. g. system software, engineering data, documentation, etc.) that will be brought into the I&C system using public or company internal networks or removable media needs to be analysed to ensure integrity. *A digital signature based on cryptographic algorithm is recommended to ensure both integrity (no tampering) and origin of data, to prevent receiving data with technically correct hash but from a false provider (identity spoofing) (e. g. the provider can base his data signature on a cryptographic asymmetrical algorithm using his own private key, and then provide end users with public keys to allow them to perform integrity and origin checks)* *As the security level of a specific algorithm used for hash calculation and/or signature decreases with time due to computing performances increase, the algorithms to be used should be based on official national security agencies' current recommendations.* *A minimum number of secure entry points (ideally a single one) within the I&C system should be reserved for receiving data from the outside. These entry points need to prevent the intrusion of malicious software. Integrity check mechanisms should be implemented.* *NOTE Outside means outside of the I&C system. In the plant, outside of the I&C system is typically still in the plant, e.g. receiving data from the plant office area. However outside data can also be data provided by the company delivering the I&C system.* *The entry points should be a dedicated and accordingly equipped with equipment only connected to the I&C system internal networks. After analysis the data should then be distributed from the dedicated computer to the target system via I&C system internal networks.* *If the distribution to the target system is not possible via I&C system internal networks, the data should be transported via a dedicated and accordingly equipped device that will then be temporarily and locally connected to the target system.* *Both dedicated computers should not have a connection to outside networks or to wireless networks.*	$\underline{E_{gvsic}O}$	$\underline{E_{gvsic}O}$	$\underline{E_{gvsic}O}$	$\underline{E_{gvsic}O}$
Tools: Not identified				
Legacy: Not identified				

13.1.1.4 d) Appropriate logging and monitoring

Control

Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, *cybersecurity*;

Preservation of:	*CIA*	*Control focus:*	*d*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) For the development and engineering environment appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to *cybersecurity*;	*(DE_d)*	*(DE_d)*	*DE_d*	*DE_d*

13.1.1.4.1 *d1) NUC – Removal and connection of devices from and to the network*

Control

Removal and connection of devices from and to the I&C network should be detected and logged.

Preservation of:	*IC*	*Control focus:*	*d*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) The I&C system should be able to detect and log the removal of a connected device from and the subsequent connection of a new or the same device to the I&C network. In addition, it should be possible to configure the I&C system in such way that an alarm will be generated and annunciated to the designated staff in order to initiate an analysis without any delay.	$(E_{gvsic}O)$	$(E_{gvsic}O)$	$E_{gvsic}O$	$E_{gvsic}O$
Tools: The detection of the removal or reconnection of supporting devices and the generation of alarms is not requested in case the supporting devices are needed only temporarily, e.g. for updating set-points. In these cases, appropriate measures should be in place that limit the access by the supporting equipment or that require the explicit granting of additional permission for use of the supporting equipment.				
Legacy: Manual logs for legacy devices – for example, a log book for persons accessing these devices, a log of any oddity (broken seal or change in operation). The integrity of these logs can be assured using the two-person principle.				

13.1.1.4.2 *d2) NUC – Other security incidents that should be logged and signalled*

Control

All security related incidents should be logged in the I&C

Preservation of:	*CIA*	*Control focus:*	*d*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) All security related incidents should be logged. The following incidents are examples: • *removal of devices* • *unsuccessful login attempts* • *malware detection* • *modification of executables* • *communication telegrams that contain inconsistent data* *NOTE It may only be feasible that just a certain history of security incidents can be logged (e. g. just information that a telegram was inconsistent without logging the telegram content).*	$(E_{gvsic}O)$	$(E_{gvsic}O)$	$E_{gvsic}O$	$E_{gvsic}O$
(B) For severe security events (severity could be based on threat and risk assessment) an alarm should be raised to the designated staff.	$(E_{gvsic}O)$	$(E_{gvsic}O)$	$E_{gvsic}O$	$E_{gvsic}O$
(C) In case of a security incident alarm, the designated staff should notify the I&C maintenance staff for further analysis.	$(E_{ic}O)$	$(E_{ic}O)$	$E_{ic}O$	$E_{ic}O$
Tools: Not identified				
Legacy: Not identified				

13.1.1.4.3 *d3) NUC – Central logging of security incidents*

Control

All security incidents should be centrally logged for the whole I&C. This is needed for forensic readiness.

Preservation of:	*CIA*	*Control focus:*	*dc*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) A Security Event and Incident logging function should be installed for each individual I&C. It should collect all security related messages from all I&C components belonging to the individual I&C (PCs, server, network devices, etc.).	$(E_{gvsic}O)$	$(E_{gvsic}O)$	$E_{gvsic}O$	$E_{gvsic}O$
(B) The Security Event and Incident logging function should be architected as a high availability system, as local log sources will only have the capability to storing a limited amount of information.	$(E_{gvsic}O)$	$(E_{gvsic}O)$	$E_{gvsic}O$	$E_{gvsic}O$
(C) Security events should also be logged within the components of the individual I&C systems. This is not to lose security events if the Event and Incident logging function of the individual I&C system is temporarily unavailable.	$(E_{gvsic}O)$	$(E_{gvsic}O)$	$E_{gvsic}O$	$E_{gvsic}O$
(D) For the plant I&C a SIEM function for analysing Security Event and Incident logs from the underlying individual I&C systems for detecting abnormal events should be available. *NOTE It is not necessary that each individual I&C system has its own SIEM analysis tool. One central SIEM analysis tool that collects and analyses the logs from all underlying individual I&C systems is sufficient.*	$(E_{ic}O)$	$(E_{ic}O)$	$E_{ic}O$	$E_{ic}O$
(E) The plant I&C SIEM function should have the capability to alarm configurable types of security incidents to the designated staff.	$(E_{ic}O)$	$(E_{ic}O)$	$E_{ic}O$	$E_{ic}O$
(F) The SIEM function should provide tools for analysing the security incident event log.	$(E_{ic}O)$	$(E_{ic}O)$	$E_{ic}O$	$E_{ic}O$
(G) For monitoring and responding to cybersecurity incidents, the plant operator should have a Security Operations Centre (SOC) in place.	$(E_{ic}O)$	$(E_{ic}O)$	$E_{ic}O$	$E_{ic}O$
Tools: Security Event and Incident Monitoring (SIEM) – COTS				
Legacy: Manual collection and analysis of logs from each I&C system component				

13.1.1.5 e) Management activities should be closely coordinated

Control

Management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure;

Preservation of:	*CIA*	*Control focus:*	*p*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) Management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure;	*DEO*	*DEO*	*DEO*	*DEO*
Tools: Not identified				
Legacy: Not identified				

13.1.1.6 f) Systems on the network should be authenticated

Control

I&C Systems on the network should be authenticated;

Preservation of:	*I*	*Control focus:*	*pd*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) For the development and engineering environment systems on the network should be authenticated;	(DE_d)	DE_d	DE_d	DE_d
(B) *I&C Systems* on the network should be authenticated;	$(E_{gvsic}O)$	$(E_{gvsic}O)$	$(E_{gvsic}O)$	$(E_{gvsic}O)$
(C) For I&C: Access to the authentication data should be locally available (without the need to connect to a server in the intranet or internet).	$(E_{ic}O)$	$E_{ic}O$	$E_{ic}O$	$E_{ic}O$
Tools: Not identified				
Legacy (1): Limited access to the physical locations containing the network interfaces.				
Legacy (2): Two-person authentication for legacy devices, after they have undergone a security assessment and approved for connection				

13.1.1.7 g) Systems connection to the network should be restricted

Control

Systems connection to the network should be restricted.

Preservation of:	*I*	*Control focus:*	*p*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) For the development and engineering environment systems connection to the network should be restricted.	*(DE_d)*	*DE_d*	*DE_d*	*DE_d*
(B) For I&C: All unused I&C network ports and all other unused I&C component standard interfaces (e. g. serial interfaces, interfaces for removable media, etc.) of I&C network devices (network switches, firewalls, etc.) and I&C devices (e. g. computers, controllers) should be disabled by device configuration. *Although devices could be physically connected, this measure ensures that devices, which are connected to unused network ports or component standard interfaces without authorization, cannot tamper with the I&C system.*	*($E_{gvsic}O$)*	*($E_{gvsic}O$)*	*$E_{gvsic}O$*	*$E_{gvsic}O$*
(C) For I&C, if (B) cannot be implemented: Besides the physical protection of the device itself, it may be possible to mechanically lock the standard interfaces. *Another possibility is the usage of seals. This way it can be detected if somebody has broken the seal to access the respective interface.*	*($E_{gvsic}O$)*	*($E_{gvsic}O$)*	*$E_{gvsic}O$*	*$E_{gvsic}O$*
Tools: Not identified				
Legacy: See (C)				

13.1.1.8 *NUC – Only needed communication services*

Control

In the I&C platform only needed communication services should be available.

Preservation of:	*CIA*	*Control focus:*	*p*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) For I&C: All communication services that are not used by the I&C should be either • *removed from the operating system, or if not possible* • *be disabled.*	*($E_{bvsic}O$)*	*($E_{bvsic}O$)*	*$E_{bvsic}O$*	*$E_{bvsic}O$*
Tools: Not identified				
Legacy: Not identified				

13.1.1.9 *NUC – Restrictive network extendibility*

Control

In the I&C system the network extendibility should be restrictive.

Preservation of:	*CIA*	*Control focus:*	*p*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) The network configuration should be restricted regarding extendibility.	*N./A.*	*N./A.*	*N./A.*	$\underline{E_{gvsic}O}$
(B) During operation, only static network configuration should be used. Policies and technical guidance for the replacement and configuration of network interface cards or communication devices should not allow new or modified communication architectures.	*N./A.*	$\underline{(E_{gvsic}O)}$	$\underline{E_{gvsic}O}$	$\underline{E_{gvsic}O}$
Tools: Not identified				
Legacy: Not identified				

13.1.1.10 *NUC – Physical securing of network interfaces*

Control

In the I&C system the network network interfaces should be physically secured.

Preservation of:	*CIA*	*Control focus:*	*p*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) Connected interfaces should be physically secured by placing the network interface cards or communication equipment within electronics cabinets or housings that can be locked.	*N./A.*	$\underline{(E_{gvsic}O)}$	$\underline{E_{gvsic}O}$	$\underline{E_{gvsic}O}$
(B) Permanently or temporarily unused physical network interfaces should be enclosed in a cabinet that can be locked and should be secured by a specific locking device (e.g. for USB interfaces or RJ45 network interfaces) provided the respective ports cannot be disabled by configuration.	*N./A.*	$\underline{(E_{gvsic}O)}$	$\underline{E_{gvsic}O}$	$\underline{E_{gvsic}O}$
Tools: Not identified				
Legacy: In cases this is not possible for legacy system, compensating stringent access control rules to the respective I&C rooms have to be enforced.				

13.1.2 Security of network services

Control

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

Preservation of:	*CIA*	*Control focus:*	*p*

Implementation guidance

Implementation	*BR*	*S3*	*S2*	*S1*
(A) The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.	*DEO*	*DEO*	*DEO*	*DEO*
(B) The security arrangements necessary for particular services, such as security features, service levels and management requirements, should be identified. The organization should ensure that network service providers implement these measures.	*DEO*	*DEO*	*DEO*	*DEO*
(C) For I&C: The network service provider should be an in-house provider. Due to cybersecurity reasons the service provider should not be outsourced.	*($E_{gvsic}O$)*	*$E_{gvsic}O$*	*$E_{gvsic}O$*	*$E_{gvsic}O$*
Tools: SLA and other such contracts/agreements				
Legacy: SLA and other such contracts/agreements				

Other information

Network services include the provision of connections, *in-house* network services and value-added networks and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

Security features of network services could be:

a) technology applied for security of network services, such as authentication, encryption and network connection controls;

b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;

c) procedures for the network service usage to restrict access to network services or applications, where necessary.

13.1.2.1 *NUC – Utilization of secure network protocols*

Control

Communication within the I&C and communication between the I&C and systems outside should be based on secure network protocols (i.e. data is encrypted).

Preservation of:	*CI*	*Control focus:*	*p*

Implementation guidance

Implementation	*BR*	*S3*	*S2*	*S1*
(A) Standard communication protocols: Only secure standard protocols should be used (ssh, https)	*DEO*	*DEO*	*DEO*	*DEO*
(B) I&C platform specific-communication protocols should be encrypted. However, this might not be feasible, e.g. due to constraints that come from safety related requirements (e.g. predictability).	*($E_{gvsic}O$)*	*($E_{gvsic}O$)*	*($E_{gvsic}O$)*	*($E_{gvsic}O$)*
Tools: Not identified				
Legacy: Not identified				

13.1.2.2 *NUC – Lock communication service after configurable number of failed remote authentications*

Control

Lock communication service after configurable number of failed remote authentications.

Preservation of:	*CIA*	*Control focus:*	*p*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) After a configurable number of failed remote authentications to a communication service the respective account should be locked. The administrator should be able to unlock the account. *This is to prevent brute force cyberattacks.*	*(DEO)*	*(DEO)*	*(DEO)*	*(DEO)*
Tools: Not identified				
Legacy: Not identified				

13.1.2.3 *NUC – Network Intrusion detection*

Control

A network intrusion detection system should be installed within the perimeter of an individual I&C system.

Preservation of:	*CIA*	*Control focus:*	*p*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) In order to detect abnormal and malicious communication from inside or from outside the I&C network all network traffic of an individual I&C system should be monitored by an intrusion detection system. However, it needs to be implemented in such a way that the safety related properties of the I&C system stay within the required level. *NOTE This control should be implemented in such a way that is does not actively influence or jeopardize safety related networks.*	*(E$_{gvsic}$O)*	*(E$_{gvsic}$O)*	*(E$_{gvsic}$O)*	*(E$_{gvsic}$O)*
(B) If an abnormal condition is detected this should be logged and an alarm should be displayed to the designated staff. *Remark: It is recognized that an intrusion detection system can produce false positives.*	*(E$_{gvsic}$O)*	*(E$_{gvsic}$O)*	*(E$_{gvsic}$O)*	*(E$_{gvsic}$O)*
Tools: Not identified				
Legacy: Not identified				

13.1.3 Segregation in networks

Control

Groups of information services, users and information systems should be segregated on networks.

Preservation of:	*CIA*	*Control focus:*	*p*