NIST Cybersecurity Framework Core: Informative Reference Standards

ISA 62443-3-3:2013
ANSI/ISA-62443-3-3 (99.03.03)-2013

Security for industrial automation
and control systems
Part 3-3: System security requirements
and security levels

Approved 12 August 2013
Throughout this standard, the SR normative language states that "the control system shall provide the capability to..." support some specific security requirement. The control system shall provide the capability, but it might be performed by an external component. In such a case, the control system shall provide an 'interface' to that external component. Some examples of compensating countermeasures include user identification (including centralized versus distributed), password strength enforcement, signature validity checking, security event correlation and device decommissioning (information persistence).

NOTE 1 The control system security requirements detailed in this document pertain to all technical functions relevant to a control system including tools and applications. However, as noted here, some of these functions can be handled by an external resource.

NOTE 2 In some high resource availability applications (high SL-T(RA,control system)), compensating countermeasures external to the control system (such as additional physical security measures and/or enhanced personnel background checks) will be needed. In these cases, it may be possible to see a normally high resource availability SL control system at a lower IAC SL 1 or 2 rating, depending upon the compensating countermeasures. Lockout or loss of control due to security measures is increased, not decreased for very high availability SL control system. Thus higher SLs are not always "better", even where cost is not a significant factor.

4.4 Least privilege

The capability to enforce the concept of least privilege shall be provided, with granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability should be available when required.

5 FR 1 – Identification and authentication control

5.1 Purpose and SL-C(IAC) descriptions

Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.

- SL 1 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against casual or coincidental access by unauthenticated entities.
- SL 2 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

5.2 Rationale

Asset owners will have to develop a list of all users (humans, software processes and devices) and to determine for each control system component the required level of IAC protection. The goal of IAC is to protect the control system by verifying the identity of any user requesting access to the control system before activating the communication. Recommendations and guidelines should include mechanisms that will operate in mixed modes. For example, some control system components require strong IAC, such as strong authentication mechanisms, and others do not.

5.3 SR 1.1 – Human user identification and authentication

5.3.1 Requirement

The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide
human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

5.3.2 Rationale and supplemental guidance

All human users need to be identified and authenticated for all access to the control system. Authentication of the identity of these users should be accomplished by using methods such as passwords, tokens, biometrics or, in the case of multifactor authentication, some combination thereof. The geographic location of human users can also be used as part of the authentication process. This requirement should be applied to both local and remote access to the control system. In addition to identifying and authenticating all human users at the control system level (for example, at system logon), identification and authentication mechanisms are often employed at the application level.

Where human users function as a single group (such as control room operators), user identification and authentication may be role-based or group-based. For some control systems, the capability for immediate operator interaction is critical. It is essential that local emergency actions as well as control system essential functions not be hampered by identification or authentication requirements (see clause 4 for a more complete discussion). Access to these systems may be restricted by appropriate physical security mechanisms (see ISA-62443-2-1 (99.02.01)). An example of such a situation is a critical operations room where strict physical access control and monitoring is in place and where shift plans allocate responsibility to a group of users. These users may then be using the same user identity. In addition, the designated operator workstation clients should be authenticated (see 5.4, SR 1.2 – Software process and device identification and authentication) or the use of this shared account should be limited to the constrained environment of the control room.

In order to support IAC policies, as defined according to ISA-62443-2-1 (99.02.01), the control system verifies the identity of all human users as a first step. In a second step, the permissions assigned to the identified human user are enforced (see 6.3, SR 2.1 – Authorization enforcement).

5.3.3 Requirement enhancements

(1) Unique identification and authentication

The control system shall provide the capability to uniquely identify and authenticate all human users.

(2) Multifactor authentication for untrusted networks

The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).

NOTE See 5.7.3 (1), SR 1.5 – Authenticator management, RE (1) for enhanced authenticator management for software processes.

(3) Multifactor authentication for all networks

The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.

5.3.4 Security levels

The requirements for the four SL levels that relate to SR 1.1 – Human user identification and authentication are:

- SL-C(IAC, control system) 1: SR 1.1
- SL-C(IAC, control system) 2: SR 1.1 (1)
- SL-C(IAC, control system) 3: SR 1.1 (1) (2)
5.4 **SR 1.2 – Software process and device identification and authentication**

5.4.1 **Requirement**

The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.

5.4.2 **Rationale and supplemental guidance**

The function of identification and authentication is to map an ID to an unknown software process or device (henceforth referred to an entity in this sub-clause) so as to make it known before allowing any data exchange. Allowing rogue entities to send and receive control system specific data can result in detrimental behavior of the legitimate control system.

All entities need to be identified and authenticated for all access to the control system. Authentication of the identity of such entities should be accomplished by using methods such as passwords, tokens or location (physical or logical). This requirement should be applied to both local and remote access to the control system. However, in some scenarios where individual entities are used to connect to different target systems (for example, remote vendor support), it may be technically infeasible for an entity to have multiple identities. In these cases, compensating countermeasures would have to be applied.

Identification and authentication mechanisms for all entities are needed to protect against attacks such as man-in-the-middle or message spoofing. In some cases, these mechanisms may involve multiple software processes running on the same physical server, each having their own identity. In other cases, the identity may be bound to the physical device, such as all processes running on a given PLC.

Special attention needs to be made when identifying and authenticating portable and mobile devices. These types of devices are a known method of introducing undesired network traffic, malware and/or information exposure to control systems, including otherwise isolated networks.

Where entities function as a single group, identification and authentication may be role-based, group-based or entity-based. It is essential that local emergency actions as well as control system essential functions not be hampered by identification or authentication requirements (see clause 4 for a more complete discussion). For example, in common protection and control schemes, a group of devices jointly execute the protection functions and communicate with multicast messages among the devices in the group. In these cases, group authentication based on shared accounts or shared symmetric keys are commonly used.

In order to support identification and authentication control policies as defined according to ISA-62443-2-1 (99.02.01), the control system verifies the identity of all entities as a first step. In a second step, the permissions assigned to the identified entity are enforced (see 6.3, SR 2.1 – Authorization enforcement).

5.4.3 **Requirement enhancements**

(1) **Unique identification and authentication**

The control system shall provide the capability to uniquely identify and authenticate all software processes and devices.
5.4.4 Security levels
The requirements for the four SL levels that relate to SR 1.2 – Software process and device identification and authentication are:

- SL-C(IAC, control system) 1: Not Selected
- SL-C(IAC, control system) 2: SR 1.2
- SL-C(IAC, control system) 3: SR 1.2 (1)
- SL-C(IAC, control system) 4: SR 1.2 (1)

5.5 SR 1.3 – Account management
5.5.1 Requirement
The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.

5.5.2 Rationale and supplemental guidance
Account management may include grouping of accounts (for example, individual, role-based, device-based and control system), establishment of conditions for group membership and assignment of associated authorizations. In certain IACS instances, where individual accounts are determined to be unnecessary from a risk-analysis and/or regulatory aspect, shared accounts are acceptable as long as adequate compensating countermeasures (such as limited physical access or organizational measures for approval) are in place and documented.

Non-human user accounts (sometimes termed service accounts) that are utilized for software process-to-process communication (for example, control server to historian and PLC to control server) typically require different security policies and procedures from human user accounts. For enhanced security, management of accounts should be done according to unified policies and deployed locally in the relevant components of the control system. Unused default system accounts used for the first installation of the system should be removable. Security enhancement lies in the simplification and consistent application of account management.

5.5.3 Requirement enhancements
(1) Unified account management
The control system shall provide the capability to support unified account management.

5.5.4 Security levels
The requirements for the four SL levels that relate to SR 1.3 – Account management are:

- SL-C(IAC, control system) 1: SR 1.3
- SL-C(IAC, control system) 2: SR 1.3
- SL-C(IAC, control system) 3: SR 1.3 (1)
- SL-C(IAC, control system) 4: SR 1.3 (1)

5.6 SR 1.4 – Identifier management
5.6.1 Requirement
The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.

5.6.2 Rationale and supplemental guidance
Identifiers are distinguished from the privileges which they permit an entity to perform within a specific control system control domain or zone (see 6.3, SR 2.1 – Authorization enforcement). Where human users function as a single group (such as control room operators), user
identification may be role-based, group-based or device-based. For some control systems, the
capability for immediate operator interaction is critical. Local emergency actions for the control
system should not be hampered by identification requirements. Access to these systems may be
restricted by appropriate compensating countermeasures. Identifiers may be required on portions
of the control system but not necessarily the entire control system. For example, wireless
devices typically require identifiers, whereas wired devices may not.

The management of identifiers will be determined by local policies and procedures established in
compliance with ISA-62443-2-1 (99.02.01).

5.6.3 Requirement enhancements
None

5.6.4 Security levels
The requirements for the four SL levels that relate to SR 1.4 – Identifier management are:

- SL-C(IAC. control system) 1: SR 1.4
- SL-C(IAC. control system) 2: SR 1.4
- SL-C(IAC. control system) 3: SR 1.4
- SL-C(IAC. control system) 4: SR 1.4

5.7 SR 1.5 – Authenticator management

5.7.1 Requirement
The control system shall provide the capability to:

a) initialize authenticator content;
b) change all default authenticators upon control system installation;
c) change/refresh all authenticators; and
d) protect all authenticators from unauthorized disclosure and modification when stored and
   transmitted.

5.7.2 Rationale and supplemental guidance
In addition to an identifier (see 5.6, SR 1.4 – Identifier management) an authenticator is required
to prove identity. Control system authenticators include, but are not limited to, tokens, symmetric
keys, private keys (part of a public/private key pair), biometrics, passwords, physical keys and
key cards. Human users should take reasonable measures to safeguard authenticators, including
maintaining possession of their individual authenticators, not loaning or sharing authenticators
with others and reporting lost or compromised authenticators immediately.

Authenticators have a lifecycle. When an account is created automatically a new authenticator
needs to be created, in order for the account owner to be able to authenticate. For example, in a
password-based system, the account has a password associated with it. Definition of the initial
authenticator content could be interpreted as the administrator defining the initial password
which the account management system sets for all new accounts. Being able to configure these
initial values makes it harder for an attacker to guess the password between account creation
and first account use (which should involve the setting of a new password by the account owner).
Some control systems are installed with unattended installers which create all necessary
accounts with default passwords and some embedded devices are shipped with default
passwords. Over time, these passwords often become general knowledge and are documented
on the Internet. Being able to change the default passwords protects the system against
unauthorized users using default passwords to gain access. Passwords can be obtained from
storage or from transmission when used in network authentication. The complexity of this can be
increased by cryptographic protections such as encryption or hashing or by handshake protocols
which don’t require transmission of the password at all. Still, passwords might be subject to attacks, for example brute force guessing or breaking the cryptographic protection of passwords in transit or storage. The window of opportunity can be reduced by changing/refreshing the passwords periodically. Similar considerations apply to authentication systems based on cryptographic keys. Enhanced protection can be achieved by using hardware mechanisms such as hardware security modules like trusted platform modules (TPMs).

The management of authenticators should be specified in applicable security policies and procedures, for example, constraints to change default authenticators, refresh periods, specification of the protection of authenticators or firecall (see 3.1.24) procedures.

Lockout or loss of control due to security measures is not acceptable. If the control system is required to have a high level of availability, measures should be taken to maintain this high level of availability (such as compensating physical countermeasures, duplicate keys and supervisory override).

Besides the capabilities for authenticator management specified in this requirement, the strength of the authentication mechanism depends on the strength of the chosen authenticator (for example password complexity or key length in public key authentication) and the policies for validating the authenticator in the authentication process (for example how long a password is valid or which checks are performed in public key certificate validation). For the most common authentication mechanisms password-based and public key authentication 5.9, SR 1.7 – Strength of password-based authentication, 5.10. SR 1.8 – Public key infrastructure (PKI) certificates and 5.11, SR 1.9 – Strength of public key authentication provide further requirements.

5.7.3 Requirement enhancements

(1) Hardware security for software process identity credentials

For software process and device users, the control system shall provide the capability to protect the relevant authenticators via hardware mechanisms.

5.7.4 Security levels

The requirements for the four SL levels that relate to SR 1.5 – Authenticator management are:

- SL-C(IAC, control system) 1: SR 1.5
- SL-C(IAC, control system) 2: SR 1.5
- SL-C(IAC, control system) 3: SR 1.5 (1)
- SL-C(IAC, control system) 4: SR 1.5 (1)

5.8 SR 1.6 – Wireless access management

5.8.1 Requirement

The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

5.8.2 Rationale and supplemental guidance

Any wireless technology can, and in most cases should, be considered just another communication protocol option, and thus subject to the same IACS security requirements as any other communication type utilized by the IACS. However, from a security point of view, there is at least one significant difference between wired and wireless communications: physical security countermeasures are typically less effective when using wireless. For this and possibly other reasons (for example regulatory differences), a risk analysis might legitimately result in a higher SL-T(IAC,control system) for wireless communications versus a wired protocol being used in an identical use case.
Wireless technologies include, but are not limited to, microwave, satellite, packet radio, Institute of Electrical and Electronics Engineers (IEEE) 802.11x, IEEE 802.15.4 (ZigBee, IEC 62591 – WirelessHART®, ISA-100.11a), IEEE 802.15.1 (Bluetooth), wireless LAN mobile routers, mobile phones with tethering and various infrared technologies.

5.8.3 Requirement enhancements

(1) Unique identification and authentication

The control system shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

5.8.4 Security levels

The requirements for the four SL levels that relate to SR 1.6 – Wireless access management are:

- SL-C(IAC, control system) 1: SR 1.6
- SL-C(IAC, control system) 2: SR 1.6 (1)
- SL-C(IAC, control system) 3: SR 1.6 (1)
- SL-C(IAC, control system) 4: SR 1.6 (1)

5.9 SR 1.7 – Strength of password-based authentication

5.9.1 Requirement

For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.

5.9.2 Rationale and supplemental guidance

User authentication based on a username and a secret password is a very commonly used mechanism. Many attacks on such mechanisms focus on guessing the password (for example, dictionary attacks or targeted social engineering) or breaking the cryptographic protection of the stored password representation (for example, using rainbow tables or brute-forcing a hash collision).

Increasing the size of the set of valid passwords by increasing the number of allowed characters makes such attacks more complex, but only if the increased set size is actually used (generally users would tend to not include special characters in a password as they are perceived as harder to remember). Limiting the lifetime of a password decreases the window of opportunity for an attacker to breach a given password’s secrecy. In order to prevent users from circumventing this control by once changing their password to a new one and then immediately changing back to their original password, a minimum lifetime for a password is commonly enforced as well. A notification to change the password prior the expiration allows the user to change the password at a convenient time according to process operations conditions.

This protection can be further enhanced by limiting the reuse of passwords (preventing small sets of alternating passwords), which further decreases the usefulness of a once-breached password. Extended protection beyond password based mechanisms can be achieved using multifactor authentication (see 5.3, SR 1.1 – Human user identification and authentication and 5.4, SR 1.2 – Software process and device identification and authentication).

5.9.3 Requirement enhancements

(1) Password generation and lifetime restrictions for human users

The control system shall provide the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the control system shall provide the capability to enforce password minimum and maximum lifetime restrictions
for human users. These capabilities shall conform with commonly accepted security industry practices.

NOTE The control system should provide the capability to prompt the user to change his password upon a configurable time prior to expiration.

(2) Password lifetime restrictions for all users

The control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for all users.

5.9.4 Security levels

The requirements for the four SL levels that relate to SR 1.7 – Strength of password-based authentication are:

- SL-C(IAC, control system) 1: SR 1.7
- SL-C(IAC, control system) 2: SR 1.7
- SL-C(IAC, control system) 3: SR 1.7 (1)
- SL-C(IAC, control system) 4: SR 1.7 (1) (2)

5.10 SR 1.8 – Public key infrastructure (PKI) certificates

5.10.1 Requirement

Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.

5.10.2 Rationale and supplemental guidance

Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. Any latency induced from the use of public key certificates should not degrade the operational performance of the control system.

The selection of an appropriate PKI should consider the organization’s certificate policy which should be based on the risk associated with a breach of confidentiality of the protected information. Guidance on the policy definition can be found in commonly accepted standards and guidelines, such as the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647 [31] for X.509-based PKI. For example, the appropriate location of a certification authority (CA), whether within the control system versus on the Internet, and the list of trusted CAs should be considered in the policy and depends on the network architecture (see also ISA-62443-2-1 (99.02.01)).

5.10.3 Requirement enhancements

None

5.10.4 Security levels

The requirements for the four SL levels that relate to SR 1.8 – Public key infrastructure (PKI) certificates are:

- SL-C(IAC, control system) 1: Not Selected
- SL-C(IAC, control system) 2: SR 1.8
- SL-C(IAC, control system) 3: SR 1.8
- SL-C(IAC, control system) 4: SR 1.8
5.11 SR 1.9 – Strength of public key authentication

5.11.1 Requirement
For control systems utilizing public key authentication, the control system shall provide the capability to:

a) validate certificates by checking the validity of the signature of a given certificate;
b) validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued;
c) validate certificates by checking a given certificate’s revocation status;
d) establish user (human, software process or device) control of the corresponding private key; and
e) map the authenticated identity to a user (human, software process or device).

5.11.2 Rationale and supplemental guidance
Public/private key cryptography strongly depends on the secrecy of a given subject's private key and proper handling of the trust relationships. When verifying a trust between two entities based on public key authentication, it is essential to trace the public key certificate to a trusted entity. A common implementation error in certificate validation is to only check the validity of a certificate's signature, but not checking the trust in the signer. In a PKI setting, a signer is trusted if they are a trusted CA or have a certificate issued by a trusted CA, thus all verifiers need to trace certificates presented to them back to a trusted CA. If such a chain of trusted CAs cannot be established, the presented certificate should not be trusted.

If self-signed certificates are used instead of a PKI, the certificate subject itself signed its certificate, thus there never is a trusted third-party or CA. This should be compensated by deploying the self-signed public key certificates to all peers that need to validate them via an otherwise secured mechanism (for example, configuration of all peers in a trusted environment). Trusted certificates need to be distributed to peers through secure channels. During the validation process, a self-signed certificate should only be trusted if it is already present in the list of trusted certificates of the validating peer. The set of trusted certificates should be configured to the minimum necessary set.

In both cases, validation needs to also consider the possibility that a certificate is revoked. In a PKI setting this is typically done by maintaining certificate revocation lists (CRLs) or running an online certificate status protocol (OCSP) server. When revocation checking is not available due to control system constraints, mechanisms such as a short certificate lifetime can compensate for the lack of timely revocation information. Note that short lifetime certificates can sometimes create significant operational issues in a control system environment.

5.11.3 Requirement enhancements

1) Hardware security for public key authentication
The control system shall provide the capability to protect the relevant private keys via hardware mechanisms according to commonly accepted security industry practices and recommendations.

5.11.4 Security levels
The requirements for the four SL levels that relate to SR 1.9 – Strength of public key authentication are:

- SL-C(IAC, control system) 1: Not Selected
- SL-C(IAC, control system) 2: SR 1.9
• SL-C(IAC, control system) 3: SR 1.9 (1)
• SL-C(IAC, control system) 4: SR 1.9 (1)

5.12 **SR 1.10 – Authenticator feedback**

5.12.1 **Requirement**

The control system shall provide the capability to obscure feedback of authentication information during the authentication process.

5.12.2 **Rationale and supplemental guidance**

Obscuring feedback protects the information from possible exploitation by unauthorized individuals, for example, displaying asterisks or other random characters when a human uses types in a password obscures feedback of authentication information. Other examples include the entry of wired equivalent privacy (WEP) keys, secure socket shell (SSH) token entry and RSA one-time passwods. The authenticating entity should not provide any hint as to the reason for the authentication failure, such as "unknown user name".

5.12.3 **Requirement enhancements**

None

5.12.4 **Security levels**

The requirements for the four SL levels that relate to SR 1.10 – Authenticator feedback are:

• SL-C(IAC, control system) 1: SR 1.10
• SL-C(IAC, control system) 2: SR 1.10
• SL-C(IAC, control system) 3: SR 1.10
• SL-C(IAC, control system) 4: SR 1.10

5.13 **SR 1.11 – Unsuccessful login attempts**

5.13.1 **Requirement**

The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded.

For system accounts on behalf of which critical services or servers are run, the control system shall provide the capability to disallow interactive logons.

5.13.2 **Rationale and supplemental guidance**

Due to the potential for denial of service, the number of consecutive invalid access attempts may be limited. If enabled, the control system may automatically reset to zero the number of access attempts after a predetermined time period established by the applicable security policies and procedures. Resetting the access attempts to zero will allow users (human, software process or device) to gain access if they have the correct login identifier. Automatic denial of access for control system operator workstations or nodes should not be used when immediate operator responses are required in emergency situations. All lockout mechanisms should consider functional requirements for continuous operations so as to mitigate adverse denial of service operating conditions which could result in total system failure or injury to personnel. Allowing interactive logins to an account used for critical services could provide a potential for denial of service or other abuse.

5.13.3 **Requirement enhancements**

None
5.13.4 Security levels
The requirements for the four SL levels that relate to SR 1.11 – Unsuccessful login attempts are:

- SL-C(IAC, control system) 1: SR 1.11
- SL-C(IAC, control system) 2: SR 1.11
- SL-C(IAC, control system) 3: SR 1.11
- SL-C(IAC, control system) 4: SR 1.11

5.14 SR 1.12 – System use notification

5.14.1 Requirement

The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

5.14.2 Rationale and supplemental guidance

Privacy and security policies and procedures need to be consistent with applicable laws, directives, policies, regulations, standards and guidance. Often the main justification for this requirement is legal prosecution of violators and proving intentional breach. This capability is thus necessary to support policy requirements, and does not improve IACS security. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the control system. A warning banner implemented as a posted physical notice in the control system facility does not protect against remote login issues.

Examples of elements for inclusion in the system use notification message are:

a) that the individual is accessing a specific control system;
b) that system usage may be monitored, recorded and subject to audit;
c) that unauthorized use of the system is prohibited and subject to criminal and/or civil penalties; and
d) that use of the system indicates consent to monitoring and recording.

5.14.3 Requirement enhancements

None

5.14.4 Security levels
The requirements for the four SL levels that relate to SR 1.12 – System use notification are:

- SL-C(IAC, control system) 1: SR 1.12
- SL-C(IAC, control system) 2: SR 1.12
- SL-C(IAC, control system) 3: SR 1.12
- SL-C(IAC, control system) 4: SR 1.12

5.15 SR 1.13 – Access via untrusted networks

5.15.1 Requirement

The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.

5.15.2 Rationale and supplemental guidance

Examples of access to the control system via untrusted networks typically include remote access methods (such as dial-up, broadband and wireless) as well as connections from a company’s
office (non-control system) network. The control system should restrict access achieved through
dial-up connections (for example, limiting dial-up access based upon the source of the request)
or protect against unauthorized connections or subversion of authorized connections (for
example, using virtual private network technology). Access via untrusted networks to
devices that control system component locations (for example, control centers and
field locations) should only be enabled when necessary and authenticated. Security policies and
procedures may require multifactor authentication for remote user access to the control system.

5.15.3 Requirement enhancements

(1) Explicit access request approval

The control system shall provide the capability to deny access requests via untrusted
networks unless approved by an assigned role.

5.15.4 Security levels

The requirements for the four SL levels that relate to SR 1.13 – Access via untrusted networks are:

- SL-C(IAC, control system) 1: SR 1.13
- SL-C(IAC, control system) 2: SR 1.13 (1)
- SL-C(IAC, control system) 3: SR 1.13 (1)
- SL-C(IAC, control system) 4: SR 1.13 (1)

6 FR 2 – Use control

6.1 Purpose and SL-C(UC) descriptions

Enforce the assigned privileges of an authenticated user (human, software process or device) to
perform the requested action on the IACS and monitor the use of these privileges.

- SL 1 – Restrict use of the IACS according to specified privileges to protect against casual
  or coincidental misuse.
- SL 2 – Restrict use of the IACS according to specified privileges to protect against
  circumvention by entities using simple means with low resources, generic skills and low
  motivation.
- SL 3 – Restrict use of the IACS according to specified privileges to protect against
  circumvention by entities using sophisticated means with moderate resources, IACS
  specific skills and moderate motivation.
- SL 4 – Restrict use of the IACS according to specified privileges to protect against
  circumvention by entities using sophisticated means with extended resources, IACS
  specific skills and high motivation.

6.2 Rationale

Once the user is identified and authenticated, the control system has to restrict the allowed
actions to the authorized use of the control system. Asset owners and system integrators will
have to assign, to each user (human, software process or device), group, role, etc. (see 5.6, SR
1.4 – Identifier management) the privileges defining the authorized use of the IACS. The goal of
use control is to protect against unauthorized actions on the control system resources by
verifying that the necessary privileges have been granted before allowing a user to perform the
actions. Examples of actions are reading or writing data, downloading programs and setting
configurations. Recommendations and guidelines should include mechanisms that will operate in
mixed modes. For example, some control system resources require strong use control protection,
such as restrictive privileges, and others do not. By extension, use control requirements need to
be extended to data at rest. User privileges may vary based on time-of-day/date, location and means by which access is made.

6.3 **SR 2.1 – Authorization enforcement**

6.3.1 Requirement

On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.

6.3.2 Rationale and supplemental guidance

Use control policies (for example, identity-based policies, role-based policies and rule-based policies) and associated read/write access enforcement mechanisms (for example, access control lists, access control matrices and cryptography) are employed to control usage between users (humans, software processes and devices) and assets (for example, devices, files, records, software processes, programs and domains).

After the control system has verified the identity of a user (human, software process or device) (see 5.3, SR 1.1 – Human user identification and authentication and 5.4, SR 1.2 – Software process and device identification and authentication), it also has to verify that a requested operation is actually permitted according to the defined security policies and procedures. For example, in a role-based access control policy, the control system would check which roles are assigned to a verified user or asset and which privileges are assigned to these roles – if the requested operation is covered by the permissions, it is executed, otherwise rejected. This allows the enforcement of segregation of duties and least privileges. Usage enforcement mechanisms should not be allowed to adversely affect the operational performance of the control system.

Planned or unplanned changes to control system components can have significant effects on the overall security of the control system. Accordingly, only qualified and authorized individuals should obtain the use of control system components for purposes of initiating changes, including upgrades and modifications.

6.3.3 Requirement enhancements

(1) Authorization enforcement for all users

On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all users (humans, software processes and devices) for controlling use of the control system to support segregation of duties and least privilege.

(2) Permission mapping to roles

The control system shall provide the capability for an authorized user or role to define and modify the mapping of permissions to roles for all human users.

NOTE 1 Roles should not be limited to fixed nested hierarchies in which a higher level role is a super set of a lesser privileged role. For example, a system administrator should not necessarily encompass operator privileges.

NOTE 2 This RE should be applicable to software processes and devices as well.

(3) Supervisor override

The control system shall support supervisor manual override of the current human user authorizations for a configurable time or event sequence.

NOTE Implementation of a controlled, audited and manual override of automated mechanisms in the event of emergencies or other serious events is often needed. This allows a supervisor to enable an operator to quickly react to unusual conditions without closing the current session and establishing a new session as a higher privilege human user.
(4) Dual approval

The control system shall support dual approval where an action can result in serious impact on the industrial process.

NOTE Dual approval should be limited to actions which require a very high level of confidence that they will be performed reliably and correctly. Requiring dual approval provides emphasis to the seriousness of consequences that would result from failure of a correct action. An example of a situation in which dual approval is required would be a change to a set point of a critical industrial process. Dual approval mechanisms should not be employed when an immediate response is necessary to safeguard HSE consequences, for example, emergency shutdown of an industrial process.

6.3.4 Security levels

The requirements for the four SL levels that relate to SR 2.1 – Authorization enforcement are:

- SL-C(UC, control system) 1: SR 2.1
- SL-C(UC, control system) 2: SR 2.1 (1) (2)
- SL-C(UC, control system) 3: SR 2.1 (1) (2) (3)
- SL-C(UC, control system) 4: SR 2.1 (1) (2) (3) (4)

6.4 SR 2.2 – Wireless use control

6.4.1 Requirement

The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices.

6.4.2 Rationale and supplemental guidance

Any wireless technology can, and in most cases should, be considered just another communication protocol option, and thus subject to the same IACS security requirements as any other communication type utilized by the IACS. However, a risk analysis may result in a requirement for wireless IACS components to support higher use control capabilities than are typically required of wired systems for the same use case and SL-T. Regulatory differences may also result in different required capabilities between wired and wireless communications.

As noted in 5.8, SR 1.6 – Wireless access management, wireless technologies include, but are not limited to, microwave, satellite, packet radio, IEEE 802.11x, IEEE 802.15.4 (ZigBee, IEC 62591 – WirelessHART®, ISA-100.11a), IEEE 802.15.1 (Bluetooth), wireless LAN mobile routers, mobile phones with tethering and various infrared technologies.

6.4.3 Requirement enhancements

(1) Identify and report unauthorized wireless devices

The control system shall provide the capability to identify and report unauthorized wireless devices transmitting within the control system physical environment.

6.4.4 Security levels

The requirements for the four SL levels that relate to SR 2.2 – Wireless use control are:

- SL-C(UC, control system) 1: SR 2.2
- SL-C(UC, control system) 2: SR 2.2
- SL-C(UC, control system) 3: SR 2.2 (1)
- SL-C(UC, control system) 4: SR 2.2 (1)
6.5   SR 2.3 – Use control for portable and mobile devices

6.5.1   Requirement
The control system shall provide the capability to automatically enforce configurable usage restrictions that include:

a) preventing the use of portable and mobile devices;
   b) requiring context specific authorization; and
   c) restricting code and data transfer to/from portable and mobile devices.

6.5.2   Rationale and supplemental guidance
Portable and mobile devices may introduce undesired network traffic, malware and/or information exposure, so there should be specific control associated with their usage in the typical control system environment. Security policies and procedures may not allow certain functions or activities via portable and/or mobile devices. Refer to ISA-62443-2-1 (99.02.01) for guidance on when and where portable and mobile devices usage should be permitted.

Protecting information residing on portable and mobile devices (for example, employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered elsewhere (see clause 8, FR 4 – Data confidentiality).

6.5.3   Requirement enhancements
(1) Enforcement of security status of portable and mobile devices
The control system shall provide the capability to verify that portable or mobile devices attempting to connect to a zone comply with the security requirements of that zone.

6.5.4   Security levels
The requirements for the four SL levels that relate to SR 2.3 – Use control for portable and mobile devices are:

- SL-C(UC, control system) 1: SR 2.3
- SL-C(UC, control system) 2: SR 2.3
- SL-C(UC, control system) 3: SR 2.3 (1)
- SL-C(UC, control system) 4: SR 2.3 (1)

6.6   SR 2.4 – Mobile code

6.6.1   Requirement
The control system shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system that include:

a) preventing the execution of mobile code;
   b) requiring proper authentication and authorization for origin of the code;
   c) restricting mobile code transfer to/from the control system; and
   d) monitoring the use of mobile code.

6.6.2   Rationale and supplemental guidance
Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, portable document format (PDF), Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control
system. For example, mobile code exchanges may be disallowed directly with the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.

6.6.3 Requirement enhancements

(1) Mobile code integrity check

The control system shall provide the capability to verify integrity of the mobile code before allowing code execution.

6.6.4 Security levels

The requirements for the four SL levels that relate to SR 2.4 – Mobile code are:

- SL-C(U, control system) 1: SR 2.4
- SL-C(U, control system) 2: SR 2.4
- SL-C(U, control system) 3: SR 2.4 (1)
- SL-C(U, control system) 4: SR 2.4 (1)

6.7 SR 2.5 – Session lock

6.7.1 Requirement

The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation. The session lock shall remain in effect until the human user who owns the session or another authorized human user re-establishes access using appropriate identification and authentication procedures.

6.7.2 Rationale and supplemental guidance

The entity responsible for a control system should employ session lock to prevent access to specified workstations or nodes. The control system should activate session lock mechanisms automatically after a configurable time period for designated workstations or nodes. In some cases, session lock for control system operator workstations or nodes is not advised (for example, sessions which are required for immediate operator responses in emergency situations). Session locks are not a substitute for logging out of the control system. In situations where the control system cannot support session lock, the responsible entity should employ appropriate compensating countermeasures (for example, providing increased physical security, personnel security and auditing measures).

6.7.3 Requirement enhancements

None

6.7.4 Security levels

The requirements for the four SL levels that relate to SR 2.5 – Session lock are:

- SL-C(U, control system) 1: SR 2.5
- SL-C(U, control system) 2: SR 2.5
- SL-C(U, control system) 3: SR 2.5
- SL-C(U, control system) 4: SR 2.5

6.8 SR 2.6 – Remote session termination

6.8.1 Requirement

The control system shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.
6.8.2 Rationale and supplemental guidance
A remote session is initiated whenever a control system is accessed across the boundary of a zone defined by the asset owner based on their risk assessment. This requirement may be limited to sessions that are used for control system monitoring and maintenance activities (not critical operations) based on the risk assessment of the control system and security policies and procedures. Some control systems or components may not allow sessions to be terminated.

6.8.3 Requirement enhancements
None

6.8.4 Security levels
The requirements for the four SL levels that relate to SR 2.6 – Remote session termination are:
- SL-C(UC, control system) 1: Not Selected
- SL-C(UC, control system) 2: SR 2.6
- SL-C(UC, control system) 3: SR 2.6
- SL-C(UC, control system) 4: SR 2.6

6.9 SR 2.7 – Concurrent session control

6.9.1 Requirement
The control system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions.

6.9.2 Rationale and supplemental guidance
A resource starvation DoS might occur if a limit is not imposed. There is a trade-off between potentially locking out a specific user versus locking out all users and services due to a lack of control system resources. Product supplier and/or system integrator guidance is likely required to provide sufficient information as to how the number of sessions value should be assigned.

6.9.3 Requirement enhancements
None

6.9.4 Security levels
The requirements for the four SL levels that relate to SR 2.7 – Concurrent session control are:
- SL-C(UC, control system) 1: Not Selected
- SL-C(UC, control system) 2: Not Selected
- SL-C(UC, control system) 3: SR 2.7
- SL-C(UC, control system) 4: SR 2.7

6.10 SR 2.8 – Auditable events

6.10.1 Requirement
The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.
6.10.2 Rationale and supplemental guidance

The purpose of this requirement is to record the occurrence of important events which need to be audited as significant and relevant to the security of the control system. Auditing activity can affect control system performance. The security audit function is usually coordinated with the network health and status monitoring function which may be in a different zone. Commonly recognized and accepted checklists and configuration guides should be considered when compiling a list of auditable events. The security policies and procedures should define auditable events that are adequate to support after-the-fact investigations of security incidents. In addition, audit records should be sufficient to monitor the effectiveness and proper operation of the security mechanisms utilized to meet the requirements in this standard.

It should be noted that the requirement for event recording is applicable within the given system functionality, specifically given system security requirements on a given level. For example, the requirement for recording of authentication events (in the access control category) on a SL 1 system is only applicable to the level of authentication functionality required for SL 1 according to the requirements in clause 5. Events may occur in any control system component (for example login events) or may be observed by dedicated monitors. For example, port scanning might be detected by an intrusion detection system (IDS) or intrusion prevention system (IPS).

6.10.3 Requirement enhancements

(1) Centrally managed, system-wide audit trail

The control system shall provide the capability to centrally manage audit events and to compile audit records from multiple components throughout the control system into a system-wide (logical or physical), time-correlated audit trail. The control system shall provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools, for example, security information and event management (SIEM).

6.10.4 Security levels

The requirements for the four SL levels that relate to SR 2.8 – Auditable events are:

- SL-C(UC, control system) 1: SR 2.8
- SL-C(UC, control system) 2: SR 2.8
- SL-C(UC, control system) 3: SR 2.8 (1)
- SL-C(UC, control system) 4: SR 2.8 (1)

6.11 SR 2.9 – Audit storage capacity

6.11.1 Requirement

The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.

6.11.2 Rationale and supplemental guidance

The control system should provide sufficient audit storage capacity, taking into account retention policy, the auditing to be performed and the online audit processing requirements. Guidelines to be considered could include the NIST Special Publication (SP) 800-92 [29]. The audit storage capacity should be sufficient to retain logs for a period of time required by applicable policies and regulations or business requirements.
6.11.3 Requirement enhancements
(1) Warn when audit record storage capacity threshold reached

The control system shall provide the capability to issue a warning when the allocated audit record storage volume reaches a configurable percentage of maximum audit record storage capacity.

6.11.4 Security levels
The requirements for the four SL levels that relate to SR 2.9 – Audit storage capacity are:

- SL-C(UC, control system) 1: SR 2.9
- SL-C(UC, control system) 2: SR 2.9
- SL-C(UC, control system) 3: SR 2.9 (1)
- SL-C(UC, control system) 4: SR 2.9 (1)

6.12 SR 2.10 – Response to audit processing failures

6.12.1 Requirement
The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

6.12.2 Rationale and supplemental guidance
Audit generation typically occurs at the source of the event. Audit processing involves transmission, possible augmentation (such as the addition of a timestamp) and persistent storage of the audit records. Audit processing failures include, for example, software or hardware errors, failures in the audit capturing mechanisms and audit storage capacity being reached or exceeded. Guidelines to be considered when designing appropriate response actions may include the NIST SP800-92. It should be noted that either overwriting the oldest audit records or halting audit log generation are possible responses to audit storage capacity being exceeded but imply the loss of potentially essential forensic information.

6.12.3 Requirement enhancements
None

6.12.4 Security levels
The requirements for the four SL levels that relate to SR 2.10 – Response to audit processing failures are:

- SL-C(UC, control system) 1: SR 2.10
- SL-C(UC, control system) 2: SR 2.10
- SL-C(UC, control system) 3: SR 2.10
- SL-C(UC, control system) 4: SR 2.10

6.13 SR 2.11 – Timestamps

6.13.1 Requirement
The control system shall provide timestamps for use in audit record generation.

6.13.2 Rationale and supplemental guidance
Timestamps (including date and time) of audit records should be generated using internal system clocks. If system-wide time synchronization is not present (which is typical in many installations),
known offsets would be needed to support analysis of a sequence of events. In addition, synchronization of internally generated audit records with external events might require synchronization with a generally recognized external time source (such as the Global Positioning System (GPS), Global Navigation Satellite System (GLONASS) and Galileo). The time source should be protected from unauthorized alteration.

6.13.3 Requirement enhancements
(1) Internal time synchronization
   The control system shall provide the capability to synchronize internal system clocks at a configurable frequency.
(2) Protection of time source integrity
   The time source shall be protected from unauthorized alteration and shall cause an audit event upon alteration.

6.13.4 Security levels
The requirements for the four SL levels that relate to SR 2.11 – Timestamps are:

- SL-C(UCC, control system) 1: Not selected
- SL-C(UCC, control system) 2: SR 2.11
- SL-C(UCC, control system) 3: SR 2.11 (1)
- SL-C(UCC, control system) 4: SR 2.11 (1) (2)

6.14 SR 2.12 – Non-repudiation

6.14.1 Requirement
The control system shall provide the capability to determine whether a given human user took a particular action.

6.14.2 Rationale and supplemental guidance
Examples of particular actions taken by a user include performing operator actions, changing control system configurations, creating information, sending a message, approving information (such as indicating concurrence) and receiving a message. Non-repudiation protects against later false claims by a user of not having taken a specific action, by an author of not having authored a particular document, by a sender of not having transmitted a message, by a receiver of not having received a message or by a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from a user, if a user took specific actions (for example, sending an email and approving a work order) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (for example, digital signatures, digital message receipts and timestamps).

6.14.3 Requirement enhancements
(1) Non-repudiation for all users
   The control system shall provide the capability to determine whether a given user (human, software process or device) took a particular action.

6.14.4 Security levels
The requirements for the four SL levels that relate to SR 2.12 – Non-repudiation are:

- SL-C(UCC, control system) 1: Not Selected
- SL-C(UCC, control system) 2: Not Selected
- SL-C(UCC, control system) 3: SR 2.12
7 FR 3 – System integrity

7.1 Purpose and SL-C(SI) descriptions
Ensure the integrity of the IACS to prevent unauthorized manipulation.

- SL 1 – Protect the integrity of the IACS against casual or coincidental manipulation.
- SL 2 – Protect the integrity of the IACS against manipulation by someone using simple means with low resources, generic skills and low motivation.
- SL 3 – Protect the integrity of the IACS against manipulation by someone using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Protect the integrity of the IACS against manipulation by someone using sophisticated means with extended resources, IACS specific skills and high motivation.

7.2 Rationale
IACS often go through multiple testing cycles (unit testing, factory acceptance testing (FAT), site acceptance testing (SAT), certification, commissioning, etc.) to establish that the systems will perform as intended before they even begin production. Once operational, asset owners are responsible for maintaining the integrity of the IACS. Using their risk assessment methodology, asset owners may assign different levels of integrity protection to different systems, communication channels and information in their IACS. The integrity of physical assets should be maintained in both operational and non-operational states, such as during production, when in storage or during a maintenance shutdown. The integrity of logical assets should be maintained while in transit and at rest, such as being transmitted over a network or when residing in a data repository.

7.3 SR 3.1 – Communication integrity

7.3.1 Requirement
The control system shall provide the capability to protect the integrity of transmitted information.

7.3.2 Rationale and supplemental guidance
Many common network attacks are based on the manipulation of data in transmission, for example manipulation of network packets. Switched or routed networks provide a greater opportunity for attackers to manipulate packets as undetected access to these networks is generally easier and the switching and routing mechanisms themselves can also be manipulated in order to get more access to transmitted information. Manipulation in the context of a control system could include the change of measurement values communicated from a sensor to a receiver or the alteration of command parameters sent from a control application to an actuator.

Depending on the context (for example transmission within a local network segment versus transmission via untrusted networks) and the network type used in the transmission (for example transmission control protocol (TCP) / internet protocol (IP) versus local serial links), feasible and appropriate mechanisms will vary. On a small network with direct links (point-to-point), physical access protection to all nodes may be sufficient on lower SLs if the endpoints' integrity is protected as well (see 7.6, SR 3.4 – Software and information integrity), while on a network distributed in areas with regular physical presence of staff or on a wide area network physical access is likely not enforceable. If a commercial service is used to provide communication services as a commodity item rather than a fully dedicated service (for example a leased line versus a T1 link), it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for communication integrity (for example because of legal restrictions). When it is infeasible or impractical to meet the necessary security
requirements it may be appropriate to implement either appropriate compensating countermeasures or explicitly accept the additional risk.

Industrial equipment is often subject to environmental conditions that can lead to integrity issues and/or false positive incidents. Many times the environment contains particulates, liquids, vibration, gases, radiation, and electromagnetic interference (EMI) that can cause conditions that affect the integrity of the communication wiring and signals. The network infrastructure should be designed to minimize these physical/environmental effects on communication integrity. For example, when particulate, liquids, and/or gases are an issue, it may be necessary to use a sealed registered jack 45 (RJ-45) or M12 connector instead of a commercial-grade RJ-45 connector on the wire. The cable itself may need to use a different jacket instead to handle the particulate, liquid, and/or gas as well. In cases where vibration is an issue, M12 connectors may be necessary to prevent the spring pins on an RJ-45 connector from disconnecting during use. In cases where radiation and/or EMI are an issue, it may be necessary to use shielded twisted pair or fiber cables to prevent any effect on the communication signals. It may also be necessary to perform a wireless spectrum analysis in these areas if wireless networking is planned to verify that it is a viable solution.

7.3.3 Requirement enhancements

(1) Cryptographic integrity protection

The control system shall provide the capability to employ cryptographic mechanisms to recognize changes to information during communication.

NOTE The use of cryptographic mechanisms to provide message authentication and integrity should be determined after careful consideration of the security needs and the potential ramifications on system performance and capability to recover from system failure.

7.3.4 Security levels

The requirements for the four SL levels that relate to SR 3.1 – Communication integrity are:

- SL-C(SI, control system) 1: SR 3.1
- SL-C(SI, control system) 2: SR 3.1
- SL-C(SI, control system) 3: SR 3.1 (1)
- SL-C(SI, control system) 4: SR 3.1 (1)

7.4 SR 3.2 – Malicious code protection

7.4.1 Requirement

The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.

7.4.2 Rationale and supplemental guidance

The control system should use protection mechanisms to prevent, detect, mitigate and report instances of detected malicious code (for example, viruses, worms, Trojan horses and spyware) transported by electronic mail, electronic mail attachments, Internet access, removable media (for example, universal serial bus (USB) devices, diskettes or compact disks), PDF documents, web services, network connections and infected laptops or other common means.

Detection mechanisms should be able to detect integrity violations of application binaries and data files. Techniques may include, but are not limited to, binary integrity and attributes monitoring, hashing and signature techniques. Mitigation techniques may include, but are not limited to, file cleaning, quarantining, file deletion, host communication restriction and IPSs.

Prevention techniques may include, but are not limited to, application blacklisting and whitelisting techniques, removable media control, sandbox techniques and specific computing platforms
mechanisms such as restricted firmware update capabilities, No Execute (NX) bit, data execution prevention (DEP), address space layout randomization (ASLR), stack corruption detection and mandatory access controls. See 10.4, SR 6.2 – Continuous monitoring for an associated requirement involving control system monitoring tools and techniques.

Prevention and mitigation mechanisms may include those designed for host elements (such as computers and servers) and network-based mechanisms (such as IDSs and IPSs) and those mechanisms focused on control system specific components (such as PLCs and HMIs).

7.4.3 Requirement enhancements

(1) Malicious code protection on entry and exit points

The control system shall provide the capability to employ malicious code protection mechanisms at all entry and exit points.

NOTE Mechanisms at this level may include removable media, firewalls, unidirectional gateways, web servers, proxy servers and remote-access servers.

(2) Central management and reporting for malicious code protection

The control system shall provide the capability to manage malicious code protection mechanisms.

NOTE Such mechanisms may be provided by endpoint infrastructure centralized management and SIEM solutions.

7.4.4 Security levels

The requirements for the four SL levels that relate to SR 3.2 – Malicious code protection are:

- SL-C(SI, control system) 1: SR 3.2
- SL-C(SI, control system) 2: SR 3.2 (1)
- SL-C(SI, control system) 3: SR 3.2 (1) (2)
- SL-C(SI, control system) 4: SR 3.2 (1) (2)

7.5 SR 3.3 – Security functionality verification

7.5.1 Requirement

The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.

7.5.2 Rationale and supplemental guidance

The product supplier and/or system integrator should provide guidance on how to test the designed security controls. Asset owners need to be aware of the possible ramifications of running these verification tests during normal operations. Details of the execution of these verifications need to be specified with careful consideration of the requirements for continuous operations (for example, scheduling or prior notification).

Examples of security verification functions include:

- Verification of antivirus measures by European Institute for Computer Antivirus Research (EICAR) testing of the control system file system. Antivirus software should detect this and appropriate incident handling procedures should be triggered.
- Verification of the identification, authentication and use control measures by attempting access with an unauthorized account (for some functionality this could be automated).
- Verification of IDSs as a security control by including a rule in the IDS that triggers on irregular, but known non-malicious traffic. The test could then be performed by introducing
traffic that triggers this rule and the appropriate IDS monitoring and incident handling procedures.

- Confirmation that audit logging is occurring as required by security policies and procedures and has not been disabled by an internal or external entity.

7.5.3 Requirement enhancements

(1) Automated mechanisms for security functionality verification

The control system shall provide the capability to employ automated mechanisms to support management of security verification during FAT, SAT and scheduled maintenance.

(2) Security functionality verification during normal operation

The control system shall provide the capability to support verification of the intended operation of security functions during normal operations.

NOTE This RE needs to be carefully implemented to avoid detrimental effects. It may not be suitable for safety systems.

7.5.4 Security levels

The requirements for the four SL levels that relate to SR 3.3 – Security functionality verification are:

- SL-C(SI, control system) 1: SR 3.3
- SL-C(SI, control system) 2: SR 3.3
- SL-C(SI, control system) 3: SR 3.3 (1)
- SL-C(SI, control system) 4: SR 3.3 (1) (2)

7.6 SR 3.4 – Software and Information Integrity

7.6.1 Requirement

The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.

7.6.2 Rationale and supplemental guidance

Unauthorized changes are changes for which the entity attempting the change does not have the required privileges. This SR complements related SRs from FRs 1 and 2. FRs 1 and 2 involve enforcing the roles, privileges and use patterns as designed. Integrity verification methods are employed to detect, record, report and protect against software and information tampering that may occur if other protection mechanisms (such as authorization enforcement) have been circumvented. The control system should employ formal or recommended integrity mechanisms (such as cryptographic hashes). For example, such mechanisms could be used to monitor field devices for their latest configuration information to detect security breaches (including unauthorized changes).

7.6.3 Requirement enhancements

(1) Automated notification about integrity violations

The control system shall provide the capability to use automated tools that provide notification to a configurable set of recipients upon discovering discrepancies during integrity verification.

7.6.4 Security levels

The requirements for the four SL levels that relate to SR 3.4 – Software and information integrity are:

- SL-C(SI, control system) 1: Not Selected
7.7 **SR 3.5 – Input validation**

### Requirement

The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system.

### Rationale and supplemental guidance

Rules for checking the valid syntax of control system inputs such as set points should be in place to verify that this information has not been tampered with and is compliant with the specification. Inputs passed to interpreters should be pre-screened to prevent the content from being unintentionally interpreted as commands. Note that this is a security SR, thus it does not address human error, for example supplying a legitimate integer number which is outside the expected range.

Generally accepted industry practices for input data validation include out-of-range values for a defined field type, invalid characters in data fields, missing or incomplete data and buffer overflow. Additional examples where invalid inputs lead to system security issues include SQL injection attacks, cross-site scripting or malformed packets (as commonly generated by protocol fuzzers). Guidelines to be considered could include the Open Web Application Security Project (OWASP) [33] Code Review Guide.

### Requirement enhancements

None

### Security levels

The requirements for the four SL levels that relate to SR 3.5 – Input validation are:

- SL-C(SI, control system) 1: SR 3.5
- SL-C(SI, control system) 2: SR 3.5
- SL-C(SI, control system) 3: SR 3.5
- SL-C(SI, control system) 4: SR 3.5

7.8 **SR 3.6 – Deterministic output**

### Requirement

The control system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.

### Rationale and supplemental guidance

The deterministic behavior of control system outputs as a result of threat actions against the control system is an important characteristic to ensure the integrity of normal operations. Ideally, the control system continues to operate normally while under attack, but if the control system cannot maintain normal operation, then the control system outputs need to fail to a predetermined state. The appropriate predetermined state of control system outputs is application dependent and could be one of the following user configurable options:

- Unpowered – the outputs fail to the unpowered state
- Hold – the outputs fail to the last-known good value
7.8.3 Requirement enhancements
None

7.8.4 Security levels
The requirements for the four SL levels that relate to SR 3.6 – Deterministic output are:

- SR-C(SI, control system) 1: SR 3.6
- SR-C(SI, control system) 2: SR 3.6
- SR-C(SI, control system) 3: SR 3.6
- SR-C(SI, control system) 4: SR 3.6

7.9 SR 3.7 – Error handling

7.9.1 Requirement
The control system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.

7.9.2 Rationale and supplemental guidance
The structure and content of error messages should be carefully considered by the product supplier and/or system integrator. Error messages generated by the control system should provide timely and useful information without revealing potentially harmful information that could be used by adversaries to exploit the IACS. Since it may be unclear whether a particular error condition is due to a security event, all error messages may need to be easily accessible during incident response. Disclosure of this information should be justified by the necessity for timely resolution of error conditions. Guidelines to be considered could include the OWASP Code Review Guide.

7.9.3 Requirement enhancements
None

7.9.4 Security levels
The requirements for the four SL levels that relate to SR 3.7 – Error handling are:

- SL-C(SI, control system) 1: Not Selected
- SL-C(SI, control system) 2: SR 3.7
- SL-C(SI, control system) 3: SR 3.7
- SL-C(SI, control system) 4: SR 3.7

7.10 SR 3.8 – Session integrity

7.10.1 Requirement
The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs.

7.10.2 Rationale and supplemental guidance
This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being
transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking, insertion of false information into a session or replay attacks. Use of session integrity mechanisms can have a significant overhead and therefore their use should be considered in light of requirements for real-time communications.

7.10.3 Requirement enhancements

(1) Invalidation of session IDs after session termination

The control system shall provide the capability to invalidate session IDs upon user logout or other session termination (including browser sessions).

(2) Unique session ID generation

The control system shall provide the capability to generate a unique session ID for each session and treat all unexpected session IDs as invalid.

(3) Randomness of session IDs

The control system shall provide the capability to generate unique session IDs with commonly accepted sources of randomness.

NOTE: Session hijacking and other man-in-the-middle attacks or injections of false information often take advantage of easy-to-guess session IDs (keys or other shared secrets) or use of session IDs which were not properly invalidated after session termination. Therefore the validity of a session authenticator needs to be tightly connected to the lifetime of a session. Employing randomness in the generation of unique session IDs helps to protect against brute-force attacks to determine future session IDs.

7.10.4 Security levels

The requirements for the four SL levels that relate to SR 3.8 – Session integrity are:

- SL-C(SI, control system) 1: Not Selected
- SL-C(SI, control system) 2: SR 3.8
- SL-C(SI, control system) 3: SR 3.8 (1) (2)
- SL-C(SI, control system) 4: SR 3.8 (1) (2) (3)

7.11 SR 3.9 – Protection of audit information

7.11.1 Requirement

The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.

7.11.2 Rationale and supplemental guidance

Audit information includes all information (for example, audit records, audit settings and audit reports) needed to successfully audit control system activity. The audit information is important for error correction, security breach recovery, investigations and related efforts. Mechanisms for enhanced protection against modification and deletion include the storage of audit information to hardware-enforced write-once media.

7.11.3 Requirement enhancements

(1) Audit records on write-once media

The control system shall provide the capability to produce audit records on hardware-enforced write-once media.

7.11.4 Security levels

The requirements for the four SL levels that relate to SR 3.9 – Protection of audit information are:

- SL-C(SI, control system) 1: Not selected
8 FR 4 – Data confidentiality

8.1 Purpose and SL-C(DC) descriptions

Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.

- SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
- SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

8.2 Rationale

Some control system-generated information, whether at rest or in transit, is of a confidential or sensitive nature. This implies that some communication channels and data-stores require protection against eavesdropping and unauthorized access.

8.3 SR 4.1 – Information confidentiality

8.3.1 Requirement

The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.

8.3.2 Rationale and supplemental guidance

Protection of information, at rest or in transit, can be maintained through physical means, compartmentalization or encryption, among other techniques. It is crucial that the technique chosen considers the potential ramifications on control system performance and the capability to recover from system failure or attack.

The decision whether the confidentiality of a given piece of information should be protected or not depends on the context and cannot be made at product design. However, the fact that an organization limits access to information by configuring explicit read authorizations in the control system is an indicator that this information is considered confidential by the organization. Thus, all information for which the control system supports the capability to assign explicit read authorizations should be considered potentially confidential and thus the control system should also provide the capability to protect it.

Different organizations and industries may require different levels of encryption strength for different categories of information, based on the sensitivity of the information as well as industry standards and regulatory requirements (see 8.5, SR 4.3 – Use of cryptography). In some situations network configuration information stored and processed in switches and routers may be considered as confidential.

Communications involving exposed information transfer may be vulnerable to eavesdropping or tampering. If the control system is depending upon an external communications service provider,
it may be more difficult to obtain the necessary assurances regarding the implementation of needed security requirements for communication confidentiality. In such cases, it may be appropriate to implement compensating countermeasures or explicitly accept the additional risk.

Entities should also be cognizant of information confidentiality when portable and mobile devices are utilized (for example, engineering laptops and USB sticks).

As required by 5.7, SR 1.5 – Authenticator management, authentication information, such as passwords, should be considered confidential, and thus never be sent in the clear.

### 8.3.3 Requirement enhancements

(1) Protection of confidentiality at rest or in transit via untrusted networks

The control system shall provide the capability to protect the confidentiality of information at rest and remote access sessions traversing an untrusted network.

**NOTE** Cryptography is a common mechanism for ensuring information confidentiality.

(2) Protection of confidentiality across zone boundaries

The control system shall provide the capability to protect the confidentiality of information traversing any zone boundary.

### 8.3.4 Security levels

The requirements for the four SL levels that relate to SR 4.1 – Information confidentiality are:

- SL-C(DC, control system) 1: SR 4.1
- SL-C(DC, control system) 2: SR 4.1 (1)
- SL-C(DC, control system) 3: SR 4.1 (1)
- SL-C(DC, control system) 4: SR 4.1 (1) (2)

### 8.4 SR 4.2 – Information persistence

#### 8.4.1 Requirement

The control system shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.

#### 8.4.2 Rationale and supplemental guidance

Removal of a control system component from active service should not provide the opportunity for unintentional release of information for which explicit read authorization is supported. An example of such information would include ‘join keys’ (in the case of some wireless field devices) stored in non-volatile storage or other cryptographic information that would facilitate unauthorized or malicious activity.

Information produced by the actions of a user or role (or the actions of a software process acting on behalf of a user or role) should not be disclosed to a different user or role in an uncontrolled fashion. Control of control system information or data persistence prevents information stored on a shared resource from being unintentionally disclosed after that resource has been released back to the control system.

#### 8.4.3 Requirement enhancements

(1) Purging of shared memory resources

The control system shall provide the capability to prevent unauthorized and unintended information transfer via volatile shared memory resources.

**NOTE** Volatile memory resources are those which generally do not retain information after being released to memory management. However, there are attacks against random access memory (RAM) which might extract key
material or other confidential data before it is actually over-written. Therefore, when volatile shared memory is released back to the control system for use by a different user, all unique data and connections to unique data need to be purged from the resource so it is not visible or accessible to the new user.

### 8.4.4 Security levels

The requirements for the four SL levels that relate to SR 4.2 – Information persistence are:

- **SL-C(DC, control system) 1**: Not Selected
- **SL-C(DC, control system) 2**: SR 4.2
- **SL-C(DC, control system) 3**: SR 4.2 (1)
- **SL-C(DC, control system) 4**: SR 4.2 (1)

### 8.5 SR 4.3 – Use of cryptography

#### 8.5.1 Requirement

If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.

#### 8.5.2 Rationale and supplemental guidance

The selection of cryptographic protection should match the value of the information being protected, the consequences of the confidentiality of the information being breached, the time period during which the information is confidential and control system operating constraints. This can involve either information at rest, in transit, or both. Note that backups are an example of information at rest, and should be considered as part of a data confidentiality assessment process. The control system product supplier should document the practices and procedures relating to cryptographic key establishment and management. The control system should utilize established and tested encryption and hash algorithms, such as the advanced encryption standard (AES) and the secure hash algorithm (SHA) series, and key sizes based on an assigned standard. Key generation needs to be performed using an effective random number generator. The security policies and procedures for key management need to address periodic key changes, key destruction, key distribution and encryption key backup in accordance with defined standards. Generally accepted practices and recommendations can be found in documents such as NIST SP800-57 [27]. Implementation requirements can be found for example in Federal Information Processing Standard (FIPS) 140-2 [23].

This SR, along with 5.10, SR 1.8 – Public key infrastructure (PKI) certificates may be applicable when meeting many other requirements defined within this standard.

#### 8.5.3 Requirement enhancements

None

#### 8.5.4 Security levels

The requirements for the four SL levels that relate to SR 4.3 – Use of cryptography are:

- **SL-C(DC, control system) 1**: SR 4.3
- **SL-C(DC, control system) 2**: SR 4.3
- **SL-C(DC, control system) 3**: SR 4.3
- **SL-C(DC, control system) 4**: SR 4.3
9  FR 5 – Restricted data flow

9.1 Purpose and SL-C(RDF) descriptions
Segment the control system via zones and conduits to limit the unnecessary flow of data.

- SL 1 – Prevent the casual or coincidental circumvention of zone and conduit segmentation.
- SL 2 – Prevent the intended circumvention of zone and conduit segmentation by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

9.2 Rationale
Using their risk assessment methodology, asset owners need to determine necessary information flow restrictions and thus, by extension, determine the configuration of the conduits used to deliver this information. Derived prescriptive recommendations and guidelines should include mechanisms that range from disconnecting control system networks from business or public networks to using unidirectional gateways, stateful firewalls and DMZs to manage the flow of information.

9.3 SR 5.1 – Network segmentation

9.3.1 Requirement
The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

9.3.2 Rationale and supplemental guidance
Network segmentation is used by organizations for a variety of purposes, including cyber security. The main reasons for segmenting networks are to reduce the exposure, or ingress, of network traffic into a control system and reduce the spread, or egress, of network traffic from a control system. This improves overall system response and reliability as well as provides a measure of cyber security protection. It also allows different network segments within the control system, including critical control systems and safety-related systems, to be segmented from other systems for an additional level of protection.

Access from the control system to the World Wide Web should be clearly justified based on control system operational requirements.

Network segmentation and the level of protection it provides will vary greatly depending on the overall network architecture used by an asset owner in their facility and even system integrators within their control systems. Logically segmenting networks based on their functionality provides some measure of protection, but may still lead to single-points-of-failure if a network device is compromised. Physically segmenting networks provides another level of protection by removing that single-point-of-failure case, but will lead to a more complex and costly network design. These trade-offs will need to be evaluated during the network design process (see ISA-62443-2-1 (99.02.01)).

In response to an incident, it may be necessary to break the connections between different network segments. In that event, the services necessary to support essential operations should
be maintained in such a way that the devices can continue to operate properly and/or shutdown in an orderly manner. This may require that some servers may need to be duplicated on the control system network to support normal network features, for example dynamic host configuration pro:ocol (DHCP), domain name service (DNS) or local CAs. It may also mean that some critical control systems and safety-related systems be designed from the beginning to be completely isolated from other networks.

9.3.3 Requirement enhancements

(1) Physical network segmentation

The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.

(2) Independence from non-control system networks

The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.

(3) Logical and physical isolation of critical networks

The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.

9.3.4 Security levels

The requirements for the four SL levels that relate to SR 5.1 – Network segmentation are:

- SL-C(RDF, control system) 1: SR 5.1
- SL-C(RDF, control system) 2: SR 5.1 (1)
- SL-C(RDF, control system) 3: SR 5.1 (1) (2)
- SL-C(RDF, control system) 4: SR 5.1 (1) (2) (3)

9.4 SR 5.2 – Zone boundary protection

9.4.1 Requirement

The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.

9.4.2 Rationale and supplemental guidance

Any connections to external networks or other control systems should occur through managed interfaces consisting of appropriate boundary protection devices (for example, proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels) arranged in an effective architecture (for example, firewalls protecting application gateways residing in a DMZ). Control system boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, higher impact control systems should be partitioned into separate zones utilizing conduits to restrict or prohibit network access in accordance with security policies and procedures and an assessment of risk. SL-T(system) categorization guides the selection of appropriate candidates for zone partitioning (see ISA-62443-3-2 [99.03.02] [10]).

9.4.3 Requirement enhancements

(1) Deny by default, allow by exception

The control system shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).
(2) Island mode

The control system shall provide the capability to prevent any communication through the control system boundary (also termed island mode).

NOTE Examples of when this capability may be used include where a security violation and/or breach has been detected within the control system, or an attack is occurring at the enterprise level. This island mode needs to support essential functions (see also clause 4.2, Support of essential functions).

(3) Fail close

The control system shall provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close). This ‘fail close’ functionality shall be designed such that it does not interfere with the operation of a SIS or other safety-related functions.

NOTE Examples of when this capability may be used include scenarios where a hardware failure or power failure causes boundary protection devices to function in a degraded mode or fail entirely. This fail close needs to support essential functions (see also clause 4.2, Support of essential functions).

9.4.4 Security levels

The requirements for the four SL levels that relate to SR 5.2 – Zone boundary protection are:

- SL-C(RDF, control system) 1: SR 5.2
- SL-C(RDF, control system) 2: SR 5.2 (1)
- SL-C(RDF, control system) 3: SR 5.2 (1) (2) (3)
- SL-C(RDF, control system) 4: SR 5.2 (1) (2) (3)

9.5 SR 5.3 – General purpose person-to-person communication restrictions

9.5.1 Requirement

The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system.

9.5.2 Rationale and supplemental guidance

General purpose person-to-person communications systems include but are not limited to: email systems, forms of social media (Twitter, Facebook, picture galleries, etc.) or any message systems that permit the transmission of any type of executable file. These systems are usually utilized for private purposes which are not related to control system operations, and therefore the risks imposed by these systems normally outweigh any perceived benefit.

These types of general purpose communications systems are commonly used attack vectors to introduce malware to the control system, pass information for which read authorization exists to locations external to the control system, and introduce excessive network loading that can be used to create security problems or launch attacks on the control system. Application of a broad range of other system requirements covering, for example, usage restrictions and limiting data flow as described elsewhere in this document to general purpose person-to-person communication systems can provide adequate compensating countermeasures to meet this requirement.

The control system may provide the capability to utilize these types of two-way communication systems, but only between servers and/or workstations within the control system. Note that this SR needs to support the requirements associated with 8.3, SR 4.1 – Information confidentiality.

The control system may also restrict email or other messaging solutions that provide internal computer-to-external computer communications using outbound messages. These internal-to-external communications may be limited to the purpose of sending system alerts or other computer generated information messages to users or systems external to the control system. To prevent the passing of information for which explicit read authorization is supported, pre-
configured messages (perhaps with the ability to include some limited text) should be used to transmit the alert's or status information. Users may not be given the ability to attach files or other information to these outbound-only messages at the time the messages are created by the system.

9.5.3 Requirement enhancements
(1) Prohibit all general purpose person-to-person communications

The control system shall provide the capability to prevent both transmission and receipt of general purpose person-to-person messages.

9.5.4 Security levels
The requirements for the four SL levels that relate to SR 5.3 – General purpose person-to-person communication restrictions are:

- SL-C(RDF, control system) 1: SR 5.3
- SL-C(RDF, control system) 2: SR 5.3
- SL-C(RDF, control system) 3: SR 5.3 (1)
- SL-C(RDF, control system) 4: SR 5.3 (1)

9.6 SR 5.4 – Application partitioning

9.6.1 Requirement
The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.

9.6.2 Rationale and supplemental guidance
Partitioning may be accomplished via physical or logical means through the use of different computers, different central processing units, different instances of the operating system, different network addresses and combinations of these methods or other methods as appropriate. Examples of applications and services that could be considered for different partitions include, but are not limited to, emergency and/or safety systems, closed-loop control applications, operator workstations and engineering workstations.

9.6.3 Requirement enhancements
None

9.6.4 Security levels
The requirements for the four SL levels that relate to SR 5.4 – Application partitioning are:

- SL-C(RDF, control system) 1: SR 5.4
- SL-C(RDF, control system) 2: SR 5.4
- SL-C(RDF, control system) 3: SR 5.4
- SL-C(RDF, control system) 4: SR 5.4

10 FR 6 – Timely response to events

10.1 Purpose and SL-C(TRE) descriptions
Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.

- SL 1 – Monitor the operation of the IACS and respond to incidents when they are discovered by collecting and providing the forensic evidence when queried.
• SL 2 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and periodically reporting forensic evidence.

• SL 3 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and pushing forensic evidence to the proper authority.

• SL 4 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and pushing forensic evidence to the proper authority in near real-time.

10.2 Rationale
Using their risk assessment methodology, asset owners should establish security policies and procedures and proper lines of communication and control needed to respond to security violations. Derived prescriptive recommendations and guidelines should include mechanisms that collect, report, preserve and automatically correlate the forensic evidence to ensure timely corrective action. The use of monitoring tools and techniques should not adversely affect the operational performance of the control system.

10.3 SR 6.1 – Audit log accessibility
10.3.1 Requirement
The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

10.3.2 Rationale and supplemental guidance
The control system generates audit records about events occurring in the system (see 6.10, SR 2.8 – Auditable events). Access to these audit logs is necessary to support filtering audit logs, identifying and removing information that is redundant, reviewing and reporting activity during after-the-fact investigations of security incidents. This access should not alter the original audit records. In general, audit reduction and report generation should be performed on a separate information system. Manual access to the audit records (such as screen views or printouts) is sufficient for meeting the base requirement, but is insufficient for higher SLs. Programmatic access is commonly used to provide the audit log information to analysis mechanisms such as SIEM. See relevant SRs in clauses 5, 6 and 9 regarding the creation of, protection of and access to audit logs.

10.3.3 Requirement enhancements
(1) Programmatic access to audit logs

The control system shall provide programmatic access to audit records using an application programming interface (API).

10.3.4 Security levels
The requirements for the four SL levels that relate to SR 6.1 – Audit log accessibility are:

• SL-C(TRE, control system) 1: SR 6.1
• SL-C(TRE, control system) 2: SR 6.1
• SL-C(TRE, control system) 3: SR 6.1 (1)
• SL-C(TRE, control system) 4: SR 6.1 (1)

10.4 SR 6.2 – Continuous monitoring
10.4.1 Requirement
The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.
NOTE: Response time is a local matter outside the scope of this standard.

10.4.2 Rationale and supplemental guidance

Control system monitoring capability can be achieved through a variety of tools and techniques (for example, IDS, IPS, malicious code protection mechanisms and network monitoring mechanisms). As attacks become more sophisticated, these monitoring tools and techniques will need to become more sophisticated as well, including for example behavior-based IDS/IPS.

Monitoring devices should be strategically deployed within the control system (for example, at selected perimeter locations and near server farms supporting critical applications) to collect essential information. Monitoring mechanisms may also be deployed at ad hoc locations within the control system to track specific transactions.

Monitoring should include appropriate reporting mechanisms to allow for a timely response to events. To keep the reporting focused and the amount of reported information to a level that can be processed by the recipients, mechanisms such as SIEM are commonly applied to correlate individual events into aggregate reports which establish a larger context in which the raw events occurred.

Additionally, these mechanisms can be used to track the effect of security changes to the control system (see 6.10, SR 2.8 – Auditable events). Having forensic tools pre-installed can facilitate incident analysis.

10.4.3 Requirement enhancements

None

10.4.4 Security levels

The requirements for the four SL levels that relate to SR 6.2 – Continuous monitoring are:

- SL-C(TRE, control system) 1: Not Selected
- SL-C(TRE, control system) 2: SR 6.2
- SL-C(TRE, control system) 3: SR 6.2
- SL-C(TRE, control system) 4: SR 6.2

11 FR 7 – Resource availability

11.1 Purpose and SL-C(RA) descriptions

Ensure the availability of the control system against the degradation or denial of essential services.

- SL 1 – Ensure that the control system operates reliably under normal production conditions and prevents DoS situations caused by the casual or coincidental actions of an entity.
- SL 2 – Ensure that the control system operates reliably under normal and abnormal production conditions and prevents DoS situations by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Ensure that the control system operates reliably under normal, abnormal, and extreme production conditions and prevents DoS situations by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Ensure that the control system operates reliably under normal, abnormal, and extreme production conditions and prevents DoS situations by entities using sophisticated means with extended resources, IACS specific skills and high motivation.
11.2 Rationale
The aim of this series of SRs is to ensure that the control system is resilient against various types of DoS events. This includes the partial or total unavailability of system functionality at various levels. In particular, security incidents in the control system should not affect SIS or other safety-related functions.

11.3 SR 7.1 – Denial of service protection

11.3.1 Requirement
The control system shall provide the capability to operate in a degraded mode during a DoS event.

11.3.2 Rationale and supplemental guidance
A variety of technologies exist to limit, or in some cases, eliminate the effects of DoS situations. For example, boundary protection devices can filter certain types of packets to protect devices on an internal, trusted network from being directly affected by DoS events or restricting the information flow to be unidirectional outbound. Specifically, as noted in clause 4, a DoS event on the control system should not adversely impact any safety-related systems.

11.3.3 Requirement enhancements
(1) Manage communication loads
The control system shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.

(2) Limit DoS effects to other systems or networks
The control system shall provide the capability to restrict the ability of all users (humans, software processes and devices) to cause DoS events which affect other control systems or networks.

11.3.4 Security levels
The requirements for the four SL levels that relate to SR 7.1 – Denial of service protection are:

- SL-C(RA, control system) 1: SR 7.1
- SL-C(RA, control system) 2: SR 7.1 (1)
- SL-C(RA, control system) 3: SR 7.1 (1) (2)
- SL-C(RA, control system) 4: SR 7.1 (1) (2)

11.4 SR 7.2 – Resource management

11.4.1 Requirement
The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.

11.4.2 Rationale and supplemental guidance
Resource management (for example, network segmentation or priority schemes) prevents a lower-priority software process from delaying or interfering with the control system servicing any higher-priority software process. For example, initiating network scans, patching and/or antivirus checks on an operating system can cause severe disruption to normal operations. Traffic rate limiting schemes should be considered as a mitigation technique.

11.4.3 Requirement enhancements
None
11.4.4 Security levels
The requirements for the four SL levels that relate to SR 7.2 – Resource management are:

- SL-C(RA, control system) 1: SR 7.2
- SL-C(RA, control system) 2: SR 7.2
- SL-C(RA, control system) 3: SR 7.2
- SL-C(RA, control system) 4: SR 7.2

11.5 SR 7.3 – Control system backup

11.5.1 Requirement
The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.

11.5.2 Rationale and supplemental guidance
The availability of up-to-date backups is essential for recovery from a control system failure and/or mis-configuration. Automating this function ensures that all required files are captured, reducing operator overhead. Although not usually required for control system recovery, information required for post-incident forensic activity (for example, audit logs) should be specifically included in the backup (see 10.4, SR 6.2 – Continuous monitoring). If the resulting backups contain confidential information, encryption should be considered (see 8.5, SR 4.3 – Use of cryptography).

11.5.3 Requirement enhancements
(1) Backup verification
The control system shall provide the capability to verify the reliability of backup mechanisms.

(2) Backup automation
The control system shall provide the capability to automate the backup function based on a configurable frequency.

11.5.4 Security levels
The requirements for the four SL levels that relate to SR 7.3 – Control system backup are:

- SL-C(RA, control system) 1: SR 7.3
- SL-C(RA, control system) 2: SR 7.3 (1)
- SL-C(RA, control system) 3: SR 7.3 (1) (2)
- SL-C(RA, control system) 4: SR 7.3 (1) (2)

11.6 SR 7.4 – Control system recovery and reconstitution

11.6.1 Requirement
The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.

11.6.2 Rationale and supplemental guidance
Control system recovery and reconstitution to a known secure state means that all system parameters (either default or configurable) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded and the system is fully tested and functional.
11.6.3 Requirement enhancements
None

11.6.4 Security levels
The requirements for the four SL levels that relate to SR 7.4 – Control system recovery and reconstitution are:

- SL-C(RA, control system) 1: SR 7.4
- SL-C(RA, control system) 2: SR 7.4
- SL-C(RA, control system) 3: SR 7.4
- SL-C(RA, control system) 4: SR 7.4

11.7 SR 7.5 – Emergency power

11.7.1 Requirement
The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.

11.7.2 Rationale and supplemental guidance
There may be instances where compensating countermeasures such as physical door access control may be affected by loss of base power supply, in which case the emergency power supply should cover those associated systems. If this is not possible, other compensating countermeasures may be needed during such an emergency situation.

11.7.3 Requirement enhancements
None

11.7.4 Security levels
The requirements for the four SL levels that relate to SR 7.5 – Emergency power are:

- SL-C(RA, control system) 1: SR 7.5
- SL-C(RA, control system) 2: SR 7.5
- SL-C(RA, control system) 3: SR 7.5
- SL-C(RA, control system) 4: SR 7.5

11.8 SR 7.6 – Network and security configuration settings

11.8.1 Requirement
The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.

11.8.2 Rationale and supplemental guidance
These configuration settings are the adjustable parameters of the control system components. In order to be able to detect and correct any deviations from the approved and/or recommended configuration settings, the control system needs to support monitoring and control of changes to the configuration settings in accordance with security policies and procedures. For enhanced security, an automated check may be performed where the current settings are automatically collected by an agent and compared to approved settings.
11.8.3 Requirement enhancements

(1) Machine-readable reporting of current security settings

The control system shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.

11.8.4 Security levels

The requirements for the four SL levels that relate to SR 7.6 – Network and security configuration settings are:

- SL-C(RA, control system) 1: SR 7.6
- SL-C(RA, control system) 2: SR 7.6
- SL-C(RA, control system) 3: SR 7.6 (1)
- SL-C(RA, control system) 4: SR 7.6 (1)

11.9 SR 7.7 – Least functionality

11.9.1 Requirement

The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.

11.9.2 Rationale and supplemental guidance

Control systems are capable of providing a wide variety of functions and services. Some of the functions and services provided may not be necessary to support essential functions. Therefore, by default, functions beyond a baseline configuration should be disabled. Additionally, it is sometimes convenient to provide multiple services from a single component of a control system, but doing so increases risk over limiting the services provided by any one component. Many functions and services commonly provided by commercial-off-the-shelf (COTS) equipment may be candidates for elimination, for example, email, voice over internet protocol (VoIP), instant messaging (IM), file transfer protocol (FTP), hypertext transfer protocol (HTTP) and file sharing.

11.9.3 Requirement enhancements

None

11.9.4 Security levels

The requirements for the four SL levels that relate to SR 7.7 – Least functionality are:

- SL-C(RA, control system) 1: SR 7.7
- SL-C(RA, control system) 2: SR 7.7
- SL-C(RA, control system) 3: SR 7.7
- SL-C(RA, control system) 4: SR 7.7

11.10 SR 7.8 – Control system component inventory

11.10.1 Requirement

The control system shall provide the capability to report the current list of installed components and their associated properties.

11.10.2 Rationale and supplemental guidance

A control system component inventory may include but is not limited to component ID, capability and revision level. The component inventory should be consistent with the SuC. A formal process of configuration management should be deployed to keep control of the changes in the component inventory baseline (see ISA-62443-2-1 (99.02.01)).
11.10.3 Requirement enhancements

None

11.10.4 Security levels

The requirements for the four SL levels that relate to SR 7.8 – Control system component inventory are:

- SL-C(RA, control system) 1: Not Selected
- SL-C(RA, control system) 2: SR 7.8
- SL-C(RA, control system) 3: SR 7.8
- SL-C(RA, control system) 4: SR 7.8