Secure Production Cell

Baseline of Security Conformance IEC 62443-3-3 SL1

Herbert Dirnberger

August 4, 2020

Executive Summary By applying this baseline the conformance to the minimal requirements for secure system design from targeted IEC 62443-3-3 SL 1 for industrial control and automation systems in productions cells compliant to enterprise information security policy will be enabled.

Target Group and Scope This document is primarily intended for asset owners, system integrators and service operators in all sections of the asset life cycle: Requirement Engineering, Project planning, Procurement, System Integration and System Service and Operation

Contents

1 Overview

The system under consideration is a typical ***secure production cell*** build as managed industrial network cell with industrial automaton and control systems (IACS) fully integrated in a enterprise (IT/OT) architecture with a industrial firewall into an industrial dmz (L2.5). The ***secure production cell*** covers the layer L0, L1 and L2 of the ***Purdue Enterprise Reference Architecture*** referenced to IEC 62443-1-1. (Figure 1)

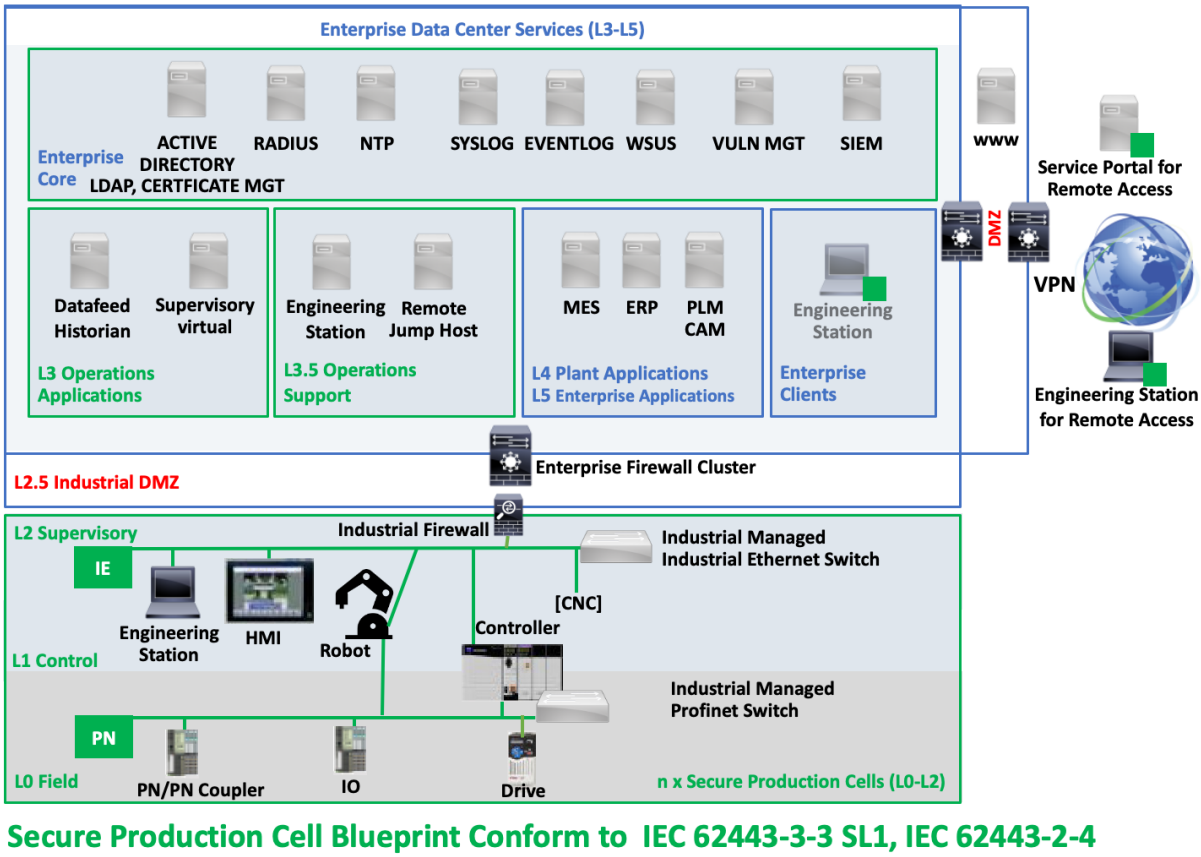

Figure 1: Secure Production Cell Blueprint

In notation of IEC 62443-3-2 the production cell (L0, L1 and L2) and the operations layer (L3 and L3.5) are definied as zone. The connection - industrial dmz (L2.5) - between production cell (L0, L1 and L2) with the enterprise network layer (L3 and L3.5) are definied as conduit.

The follow minimum system requirements from IEC 62443-3-3 SL1 are applicable to

- production cell (L0, L1 and L2)
- industrial dmz (L2.5)
- operations management (L3 and L3.5)

and also for engineering station in the production cell, enterprise client network or for remote access via vpn and remote access service portals.

In enterprise network and especially for engineering stations additional given enterprise information security (eg ISO 27001 etc) and further IT policies are obligatory considerable.

The Integration of the secure production cell is a result of a secure system integration process, which is conform to the requirements to IEC 62443-2-4. The requirements of the security program for the service provider are a prerequisite for the assurance of overall security.

Secure Production Cell Integration Industrial Automation and Control System will be integrated via managed switches (for industrial ethernet and profinet) and industrial firewalls in secure production cells in conformance to IT/OT guidelines (network settings, network ranges, network names, approved devices etc)

Time Sync System should have a uniform system time and the possibility to synchronize this system time with an external time source.

Secure Communication Protocols The communication between control device and enterprise application is secured by transport layer security protocols like OPA UA/TLS, mqtts for secure communication between enterprise application and control device. For secure file transmission smbv3, secure webdav and ftps could be used. For secure remote access RDP and ssh with TLS support could be to utilized. Not listed protocolls eg. Rest API etc need a clearance and can be integrated with secure gateways or bridges.

Support of Essential Functions An essential function is a function or capability that is required to maintain health, safety, the environment and availability for the equipment under control. Security measures shall not adversely affect essential functions of a high availability IACS unless supported by a risk assessment.

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.

- Restricted Internet Access via Proxy

Patchabilityy - Support For Updates - firmware, upgrade or update are available in the whole asset lifecylce - no outdated legacy software, operation systems

Remote Access via VPN Client 2 Side VPN for named external user

2 IEC 62443-3-3 SL1 Requirements

2.1 FR 1 Identification and Authentication Control

2.1.1 SR 1.1 Human User Identification and Authentication

Requirement The 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 system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

Implementation General engineering or service access is enabled with the host based device - engineering station - in L2 control layer of the production cell. Local access for operation users is given with embedded device HMI (Human Machine Interface). Typically administrative access for operations service management users will be established via a trusted remote jump host. Remote access for engineering or service could be used via secure remote access (trusted service cells, user firewall access and VPN) and a engineering station in the enterprise client network.

Role-based access control (RBAC) must be integrated for all user accounts and for all user access to the singular control device (embedded, host-based and network device) and systems of the production cell.

The capabilities to administrate the user accounts of system, to assign appropriate rights to users with appropriate roles for the system, including operators, engineers and viewers can be configured.

A administrator authorization is required for the management of user accounts. Regular users cannot can not administrate user accounts on any host-based, embedded or network devices.

Centralized RBAC via Active Directory and LDAP (for host based devices with Windows OS and applications) and RADIUS Server for unique identification aud authentication of the accounts for network and embedded devices is supported.

Embedded devices like controller or HMI and eg. runtime applications on host based devices should connected to domain specific central user managagement with access control tools like Simatic Logon or similar.

Should Have:

- ☐ two-factor authentication for external human users for remote access

Not Accepted:

- ☐ no aligned authentication for human user available
- ☐ usage of human user accounts for machine to machine communidation instead of a system user

2.1.2 SR 1.2

(not applicable in SL1)

2.1.3 SR 1.3 Account Management

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.

Implementation The capability of management of all accounts by authorized users is supported.

Should Have:

- ☐ capability to integrate into a higher level account management system like RADIUS, LDAP, Simatic Logon

Not Accepted:

- ☐ no account management capability
- ☐ accounts used for essential functions could be locked out, even temporarily.

2.1.4 SR 1.4 Identifier Management

Requirement The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.

Implementation the capability of management of identifiers by user, group, role or control system interface is supported

Not Accepted:

- ☐ Local emergency actions for the system hampered by identification requirements.

2.1.5 SR 1.5 Authenticator Management

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.

Implementation The required capabilities for authenticator management (to initialize, change and refresh all passwords or further credentials) are provided through the operating system and concerning applications.

Locally managed passwords are not stored in cleartext in the system (eg. salted hashes, etc), their transmission is always encrypted and the typed password is obscured by using bullets insted of characters.

Not Accepted:

- ☐ transmission and storage of cleartext passwords
- ☐ no protection against unauthorized disclosure or modification of authenticators (when stored, used, transmitted)
- ☐ not peridoc change of authenticators possible

2.1.6 SR 1.6 Wireless Access Management

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

Implementation In order to reduce the risk, the secure production cell avoids wireless communication.

If wireless communination in a prodcution cell is functional necessary the ability to identify and authenticate all users engage in wireless communication must be fulfilled.

Not Accepted:

- ☐ unmanaged and unsecured wireless LANs are used

2.1.7 SR 1.7 Strength of Password-based Authentication

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.

Implementation All host-based systems running Microsoft Windows as operation system and applications on host-based system using LDAP or Simatic Logon have the capability to enforce domain

password strength locally.

Network or embedded system must use an external Radius or Simatic Logon Service to enforce password strength.

Configurable password strength should accord to internationally recognized and proven password guidelines, e.g. NIST SP800-63-2, BSI TR-02102

Not Accepted:

- ☐ enforcement of configurable password strength based on minimum length and variety of character types not possible
- ☐ usage of hardcoded, default, unchangeable and weak passwords

2.1.8 SR 1.8

(not applicable in SL1)

2.1.9 SR 1.9

(not applicable in SL1)

2.1.10 SR 1.10 Authenticator Feedback

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

Implementation The default configuration in the system is to obscure password entry-related feedback. The system does not provide any hint in case of an authentication failure.

Not Accepted:

- ☐ displaying password, wireless key, SSH token in input field instead of asterisks

SR 1.11 Unsuccessful Login Attempts

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.

Implementation All Centralized RBACs amd managend Windows operating system are configured to limit the number of invalid access attempts with the Account lockout threshold policy setting.

Network and embedded devices delay further login attemps after a number of invalid account attempts.

Not Accepted:

- ☐ no logging, warning and shield function againt unsucessful login attempts
- ☐ accounts used for essential functions could be locked out, even temporarily. An essential function is a function or capability that is required to maintain health, safety, the environment and availability for the equipment under control.

2.1.11 SR 1.12 System Use Notification

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.

Implementation All managend Windows operating systems have the capability to enforce a use notification with the LegalNoticeCaption function. In the case of remote access to the system, human user authentication is centrally performed

Not Accepted:

- ☐ system use notification can not be customized/enabled

SR 1.13 Access via Untrusted Networks

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

Implementation System access via untrusted networks (remote access, office network etc) is controlled and monitored by firewalls that support communication restrictions to the needed protocols, IP addresses and support logging and monitoring functions.

Not Accepted:

- ☐ access system from untrusted network (office network, remote access) cannot be monitored, denied, controlled or logged by an industrial firewall with strict ruleset

2.2 FR 2 Use Control

2.2.1 SR 2.1 Authorization Enforcement

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.

Implementation Role-based access control is supported in the system for all user accounts and for all user accesses to the system. This includes capabilities to assign appropriate rights to users administering the user accounts for the system. Appropriate roles for the system, including operators, engineers, viewers can be configured.

Not Accepted:

- ☐ interfaces without authorization mechanism with system and safety relevant access (e.g. HMI, web interface, console) - not viewer access
- ☐ authorization mechanism is not forced by the least privilege principle
- ☐ authorization functions affect safety instrumented functions

2.2.2 SR 2.2 Wireless Use Control

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.

Implementation In order to reduce the risk, the secure production Cell avoids wireless communication.

If wireless communination in production cell is functional necessary to ability to identify and authenticate all users engage in wireless communication must be fulfilled.

Not Accepted:

- ☐ unmanaged and unsecured wireless LANs are used for routine jobs

2.2.3 SR 2.3 Use Control for Portable and Mobile Devices

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.

Implementation The system design only allows engineering access from engineering station in the production cell or secured via firewall rules from trusted and untrusted networks. The usage of any mobile devices like USB adapers should be avoided.

In additon hardening controls like disabling unused Ethernet and USB Ports and physical protection like door locks etc shoult be targeted.

Not Accepted:

- ☐ usage of removable and mobile media is not strictly reduced
- ☐ no locks for exposed server room, racks

2.2.4 SR 2.4 Mobile Code

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.

Implementation In general, mobile code exchange from outside the system is not needed and not allowed. System-wide hardening limits the attack surface that would allow malware to enter the system. Examples are the secure zone concept including firewalls at the zone borders, and deactivation of USB and network ports. Deinstallation of unneeded software and secure configuration of application software reduces the risk of malware introduction through mobile code (for example in PDF files, Javascript).

For Windows-based systems malware protection (classical antivirus or application whitelisting) is in place.

Not Accepted:

- ☐ usage of removable and mobile media is not strictly reduced and need for routine jobs
- ☐ no locks for server room, racks
- ☐ Internet access of control devices is not restricted

2.2.5 SR 2.5 Session Lock

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.

Implementation Session time-out is supported by network, embedded and host-based devices.

Not Accepted:

- ☐ no configurable session lock (manual, time period of inactivity, disable session lock)
- ☐ accounts used for essential functions could be locked out, even temporarily. An essential function is a function or capability that is required to maintain health, safety, the environment and availability for the equipment under control.
- ☐ identification and authentication affect safety instrumented functions

2.2.6 SR 2.6

(not applied in SL1)

2.2.7 SR 2.7

(not applied in SL1)

2.2.8 SR 2.8 Auditable Events

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.

To ensure that security logs are kept for a specified number of days and to provide them for further analysis, security logging server acts as central destination and collects the security logs via the syslog

or eventlog protocol. This server can be connected to a superordinate SIEM system without interfering with the substation component configuration.

Implementation Security-related events are logged across the whole system. All components support security logging like Syslog or Eventlog. Security-logging server act as central destination and collects the security logs.

Not Accepted:

- ☐ relevant security-related events are not logged
- ☐ security-related events are not forwardable to central logging server
- ☐ audit records not include the following information: timestamp, source, category, type, event ID, event result
- ☐ incorrectly timestamped audit records affect essential functions

2.2.9 SR 2.9 Audit Storage Capacity

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.

Implementation All Windows-based systems support the Windows eventlog. The maximum log capacity can be configured via the Windows GPO (group policy objects). A percentage threshold can be configured for the security event log at which the system will generate a warning.

The storage capacity on the syslog server is limited by the disc space only. The logging server has the capability to send a message to a SIEM if a threshold (disk space) is reached. The logging server has the capability to automatically delete old log entries after sending those to a SIEM. If the maximum size for the log is reaching, the runing applications are note aeffect and keep running. The control system prevents the loss of information with several measures depending on the dedicated component.

Not Accepted:

- ☐ failure of audit functionality when a threshold is reached or the storage capacity is exceeded

2.2.10 SR 2.10 Response to Audit Processing Failures.

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.

Implementation Audit and logging events are not able to influe the main function fo the process. The system prevents the loss of information with several measures depending on the dedicated component. The security log information will be sent to a syslog/eventlog server in near-real-time manner. Failures between the syslog/event server and SIEM are recognized and lead to a log entry.

Not Accepted:

- ☐ loss of essential services or functions during an audit processing failure
- ☐ no warning/status about audit processing failure

2.2.11 SR 2.11 Timestamps

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

Implementation Timestamps for audit record generation will be provided by the logging devices.

Not Accepted:

- ☐ no ability to generate timestamps for audit records (see SR 2.8) - timestamps include date and time
- ☐ no correct or synced time on systems avoidable with general usage of ntp time services
- ☐ incorrectly timestamped audit records affect essential functions

2.2.12 SR 2.12

(not applied in SL1)

2.3 FR 3 System Integrity

2.3.1 SR 3.1 Communication Integrity

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

Implementation The secure production cell is based on secure zones and tight firewall configuration for access to secure zones. The equipment withstands the harsh environmental conditions in production area. This avoids violation of communication integrity due to electromagnetic impact.

The communication from secure production cell to another secure production cell, service cell operations application or remote access via VPN must secured with minimum Transport Layer Security Standard (–> SR 4.3) recommended protocols (e.g. BSI TR-02102), see 4.3

Not Accepted:

- ☐ usage of non-standardized cryptographic protocol
- ☐ usage of unsecure and legacy protocols

2.3.2 SR 3.2 Malicious Code Protection

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.

Implementation For Windows-based systems, antivirus (Microsoft Defender) and application whitelisting solutions (Microsoft Defender Applicaton Control) are released to protect against malware. Updates for antivirus signatures can be deployed via WSUS or WSUS offline (Windows Server Update Services).

Not Accecpted:

- ☐ no controls like antivirus and application whitelisting for standard host-based systems with standard applications (eg. HMI)
- ☐ outdated antivirus definition on running system
- ☐ usage of non hardenend shares, generic domain users, outdated legacy file share protocols
- ☐ installation of not signed software from unsecure sources
- ☐ permament connection to internet (mail, browser)

2.3.3 SR 3.3 Security Functionality Verification

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.

Implementation Verification of correct implementation of security functions to address the security requirements is performed according to security tests.

Not Accecpted:

- ☐ no possibility to test and monitor security functionality, e.g. no log message, no notification

2.3.4 SR 3.4 Software and Information Integrity

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

Implementation The integrity checks are based on digitally signed software and component capabilities. Microsoft and application software updates are protected by digital signatures. Firmware updates for are digitally signed.

Not Accecpted:

- ☐ usage of a outdated software and operation system
- ☐ no usage of version-control for programmable controller code

2.3.5 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.

Implementation As a standard capability regarding to safety and functional requirements, the secure production cell components perform verification of process-related input values, for example regarding allowed ranges.

Not Accecpted:

- ☐ out-of-range values for a defined field type
- ☐ invalid characters in data fields
- ☐ missing or incomplete data and buffer overflow

2.3.6 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.

Implementation In case of abnormal communication, the protection in control devices will continue to provide protection and the system providing core function without communication

Not Accecpted:

- ☐ in case of abnormal communication, the protection in control devices will not continue to provide protection

2.3.7 SR 3.7

(not applied in SL1)

2.3.8 SR 3.8

(not applied in SL1)

2.3.9 SR 3.9

(not applied in SL1)

2.4 FR 4 Data Confidenitality

2.4.1 SR 4.1 Information Confidentiality

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.

Implementation Confidentiality of sensitive data like user authorization and certificate information is ensured in the system by applying appropriate access protection mechanisms.

System shall support communicaiton with encrypted protocols and robust check sums/hashing to the confidentiality and integrity of information at rest or in transit. –> SR 4.2

The usage of legacy or unsecure protocols like smbv1, snmpv1, ftp etc for communication secure production to operations applications must be avoided.

Windows-based systems use the Windows build-in data protection architecture.

This requirement can only fulfilled if also SR2.3, SR 2.4 is considered and additonal hardening controls like disabling unused Ethernet and USB Ports and physical protection like door locks etc should be applied.

Not Accecpted:

- ☐ usage of legacy or unsure protocols like smbv1, snmpv1, ftp etc for communication secure production cell to operations applications
- ☐ sensitive data eg GDPR is stored on system in cleartext and accessable for everybody without any authorisation
- ☐ (wireless) no use of any encryption

2.4.2 SR 4.2

(not applied in SL1)

2.4.3 SR 4.3 Use of Cryptography

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.

Implementation The production cell use standardized cryptographic mechanisms, including X.509 certificates, SSL/TLS, IPsec etc. Common best practices regarding crypto algorithms and key lengths are constantly monitored from diverse international sources (for example NIST, BSI) and adopted in the components. use of recommended protocols (e.g. BSI TR02102)

Follow protocols are accepted for usage without any compensation controls, if minimum standard for Transport Layer Security TLS 1.2 is fulfilled.

- OPC UA/TLS
- SSH
- MQTTS
- FTPS
- SMBv3
- RDP
- HTTPS

Network and embedded devices should support secured version of - NTP - SYSLOGs - RADIUS or use compensation controls like vpn.

Not Accecpted:

- ☐ usage of legacy or unsure protocols like smbv1, snmpv1, ftp etc for communication secure production cell to operations applications
- ☐ use of non-standardized cryptographic protocol
- ☐ (wireless) no use of any encryption
- ☐ use of weak and outdated cryptographic protocol

2.5 FR 5 Ristricted Data Flow

2.5.1 SR 5.1 Network Segmentation

Requirement 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.

Implementation The production cell is shielded with an industrial firewalls with a firewall configuration follow the least priviledge/hardening principle.

The architecture of the secure production cell separates real-time communication for automation eg. Profinet from industrial ethernet communication. One production can consist of one inudstriual ethernet network with 0,1 or more connected real-time communication networks.

The mixture of Profinet and Industrial Ethernet must be avoided, the networks must be separated. The gateway from industrial ethernet to profinet is typically the controller. So a direct communication to a profinet device without using the controller is not possible.

Not Accecpted:

- ☐ production cell is not shielded with am industrial firewalls with a firewall configuration follow the least priviledge/hardening principle
- ☐ Profinet and Industrial Ethernet networks are not separated

2.5.2 SR 5.2 Zone Boundary Protection

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.

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).

Implementation The network segmentation is accomplished by separating the networks using industrial firewalls. The firewalls control all inbound and outbound communication with a firewall configuration follow the least priviledge/hardening principle. The default recommended firewall configuration only allows the required communication and protocols.

All blocked and relevant allow traffic will be logged for further analysis.

Not Accecpted:

- ☐ demonstrate insufficient boundary protection
- ☐ no defined zones or conduits
- ☐ no firewall ruleset following deny by default, allow by exception
- ☐ essential functions are not maintained if zone boundary protection goes into fail-close and/or island mode

2.5.3 SR 5.3 General Purpose Person-to-Person Communication Restrictions

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.

Implementation Secure zone boundaries are protected by firewalls. The default recommended firewall configuration only allows the required communication and protocols. All other communication like unnecessary protocols carrying person-to-person communication is denied.

Not Accecpted:

- ☐ demonstrate insufficient boundary protection with nonexistend, insufficient traffic inspection

2.5.4 SR 5.4 Application Partitioning

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.

Implementation Partitioning of different functions, applications, or data are supported. Critical automation and protection functions are located in the secure production cell. Service functionality (for example engineering) is located in a service cell instead of placing it directly in production cell.

Not Accepted:

- ☐ centralized applications and data
- ☐ develope system is separated from runtime

2.6 FR 6 Timely Response To Events

2.6.1 SR 6.1 Audit Log Accessibility

Requirement The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

Implementation All components of system should provide security audit log capabilities. The audit logs can be accessed by authorized users eg. via ssh or https.

Not Accepted:

- ☐ audit logs are accessible to unauthorized users
- ☐ no capability for authorized humans or no tools to access audit logs

2.6.2 SR 6.2

(not applied in SL1)

2.7 FR 7 Resource Availability

2.7.1 SR 7.1 Denial of Service Protection

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

Implementation DoS protection is realized with the defense-in depth approach. Industrial firewalls protect the system and prevent direct communication with the production cell from untrusted networks.

Not Accepted:

- ☐ production cell is not protected by an industrial firewall against denial of service (DoS)
- ☐ denial of service (DoS) or denial of service (DoS) protection itself affect safety instrumented functions

2.7.2 SR 7.2 Resource Management

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

Implementation Critical automation and protection functions and management functionality (for example engineering) are located inside the secure production cell. The secure system is designed to continue independent basic operation without relying on external network services.

The industrial firewall limits the use of ressources by securtiy funtions to protect against resource exhaustion.

With the automatic cell offline mode the system operates in case of it outages and disruption.

Not Accepted:

- ☐ no automatic cell offline mode available.

2.7.3 SR 7.3 System Backup

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.

Implementation The system has the capability to backup and restore critical files like configuration and real time data that are needed to restore the system. The latest firmware and configuration are backed up via the engineering tool and are available on the engineering station.

Not Accepted:

- ☐ no / insufficient backup capabilities
- ☐ insufficient description of configuration

2.7.4 SR 7.4 System Recovery and Reconstitution

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

Implementation Disaster recovery capabilities and strategies based on the backup and restore capabilities stated for SR 7.3. The capabilities include backup and recovery of software, configuration and operational data. This includes also the secure configuration like implemented hardening, updates and patches.

Not Accepted:

- ☐ no capability to recover and reconstitute to a known secure state after disruption or failure
- ☐ security-critical patches are not reinstalled or security-related configuration settings are not reestablished with recovery
- ☐ system documentation and operating procedures is not available

2.7.5 SR 7.5 Emergency Power

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.

Implementation For the system in scope, the capability is provided as due to loss of power supply no degradation of security will occur. Loss of power supply will result in temporary unavailability from remote, not in allowing any-to-any communication.

Not Accepted:

- ☐ loss of power occur loss of security functions

2.7.6 SR 7.6 Network and Security Configuration Settings

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.

Implementation The system can be configured according to the recommended system security and hardening guidelines.

Not Accepted:

- ☐ the system can not be configured according to the recommended system security and hardening guidelines

2.7.7 SR 7.7 Least Functionality

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

Implementation Capability to set configuration options to a secure state (hardening) are provided by the system.

Not Accepted:

- ☐ no capability to restrict the use of unnecessary functions, ports, protocols, unneeded software and/or services
- ☐ functions beyond a baseline configuration can not be deactivated

2.7.8 SR 7.8

(not applied in SL1)

3 Literature

/1/ IEC 62443-3-3: System Security Requirements and Security Levels

/2/ IEC 62443-2-4: Security Program Requirements for IACS Service Providers

/3/ Siemens Secure Subsation Declartion of Security Conformance IEC 62443-3-3 V1.00 - 2020