IEC 62443-3-3:2013 System security requirements for industrial automation

Seven foundational requirements, 51 system requirements

100 requirements. This standard can be certified against by an accredited body. As of 07/2026.

IEC 62443-3-3 can be certified against, and what gets certified is a system, not an organisation and not a person. The routes are ISASecure SSA and the IECEE CB Scheme. Anyone wanting to certify the organisation needs 62443-2-1 or 2-4, anyone meaning the component needs 62443-4-2. This list holds the 51 system requirements and the 49 requirement enhancements. Which of them apply depends on the security level you aim for: 38 from SL 1, 60 from SL 2, 90 from SL 3, all 100 at SL 4. No enhancement already applies at SL 1. This list is a working aid for self-assessment, not a proof.

Company	Date	Prepared by

5 FR 1: Who or what is asking for access, and is it really who it claims to be 24

SR 1.1 Human users are identified and their identity is verified before they gain access, at every point where they can operate or configure the automation system. This includes operator panels at the machine, engineering access and network services.

What proves it: Inventory of all logon points in the system, that is HMI, control room, PLC programming access, switch, VPN and remote maintenance client, each with the authentication mechanism used there. Add a configuration extract or a screenshot of the logon screen for each device class. A small operation starts with one table per device, columns: device, interface, authentication present yes or no, justification if no. Required from SL 1 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.1 RE 1 Every human user works under an individual identifier assigned to that person alone. Shared and shift accounts are disabled, remaining exceptions are justified case by case and backed by additional measures.

What proves it: Account export per system mapping identifier to person, exception list with justification and compensating measure, for example a camera or an attendance log at the operator station. This line is a requirement enhancement and therefore never mandatory at SL 1, it is required from SL 2 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.1 RE 2 Anyone logging on from an untrusted network, for example from the internet or through a remote maintenance connection, proves their identity using at least two independent factors.

What proves it: Configuration of the remote access with the second factor enabled, an example logon record showing both factors, and the issue list of tokens or app registrations. A small operation uses the second factor of the existing VPN gateway or an authenticator app, which costs nothing beyond setup time. Requirement enhancement, required from SL 3 onwards, not at SL 1.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.1 RE 3 The proof by two independent factors applies not only to access from outside, but to every logon by a human user, including logons inside the network that is classified as trusted.

What proves it: Policy extract of the central authentication service showing that the second factor is enforced without any network exemption, plus sample logon records from the control room and the operator panel. Requirement enhancement, required only from SL 4 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.2 Not only humans, but also software processes and devices authenticate to the system before they are allowed to exchange data or use services. This includes couplings between controllers, data links to higher level systems and diagnostic tools.

What proves it: List of machine to machine connections with source, destination, protocol and the credential used in each case, for example certificate, service account or pre shared key. Add a configuration extract of one coupling that makes the authentication visible. Required from SL 2 onwards, not required at SL 1.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.2 RE 1 **Every software process and every device presents its own unique identifier. Shared service accounts or a single key used system wide across many devices are not permitted.** Document

What proves it: Mapping of device to identifier or certificate serial number showing that no identifier appears twice. Requirement enhancement, required from SL 3 onwards and therefore not part of SL 1.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.3 **Accounts are managed across their entire life cycle: creation, change of privileges, disabling on departure and removal are governed by rules and supported by the systems involved. This covers user accounts, service accounts and emergency accounts.** Document

What proves it: Account register with type, owner, purpose and status, plus evidence for joiners and leavers, for example a signed handover or a ticket showing the disabling with its date. A recurring account review is advisable, and in a small operation an annual reconciliation of the account list against the personnel list is sufficient. Required from SL 1 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.3 RE 1 **Account management is unified across all components of the system, so that disabling an account in one place does not remain ineffective on individual devices.**

What proves it: Evidence of the central directory integration, for example directory service or RADIUS, with a list of the connected components and an explicit list of the devices that cannot be connected together with their alternative procedure. Test record of a disabling that takes effect on all connected systems. Requirement enhancement, required from SL 3 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.4 **Identifiers are issued according to fixed rules, assigned unambiguously to a person, a device or a role, retired when no longer used and never reissued to a different holder later on.**

What proves it: Naming rule for identifiers, for example surname plus initial or plant code plus number, plus the history of retired identifiers showing that they are not reused. A small operation keeps a single running list with issue date and retirement date. Required from SL 1 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.5 **Authenticators such as passwords, keys, certificates and tokens are issued in an orderly manner, changed when disclosure is suspected and revoked when needed. Default accounts and factory passwords as delivered are changed before commissioning.**

What proves it: Issue list of tokens and certificates with recipient and date, evidence of changes and revocations, plus a commissioning checklist per device with the item factory password changed, signed off. Required from SL 1 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.5 RE 1 **The credentials of software processes are not stored as a readable file on the storage medium, but in hardware backed storage that prevents the secret part from being read out.**

What proves it: Type evidence of the security component used, for example TPM, secure element or HSM, with a configuration extract proving that the key is stored inside the component. A purchase record or data sheet is sufficient as type evidence. Requirement enhancement, required from SL 3 onwards, not required at SL 1 and SL 2.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.6 **Wireless access to the system, for example WLAN, radio remote controls or Bluetooth diagnostics, is usable only after identification and authentication of both user and device, and is managed deliberately.**

What proves it: Inventory of all wireless links with purpose, range and encryption method, configuration extract of the access point and the list of approved end devices. A small operation additionally documents which wireless interfaces on devices have been deliberately switched off. Required from SL 1 onwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 1.6 RE 1 **Every wireless access must be attributable to one specific user or one specific device, a shared network key for all participants is not sufficient.**

What proves it: Evidence of a method with individual credentials, for example enterprise WLAN authentication against a directory or per device certificates, plus a connection log showing the individual identifier. Requirement enhancement, required from SL 2 onwards and therefore not at SL 1.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 1.7 **Wherever passwords are used, their minimum strength can be configured, for example minimum length and required character types, and the configured values take effect for all accounts concerned.**

What proves it: Configuration extract of the password policy per system with the values actually set, for example length >= 10 characters and at least three character types, plus a list of the systems that cannot technically support this setting together with their compensating measure. Required from SL 1 onwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 1.7 RE 1 **For human users, additional rules govern password generation and lifetime: reuse of earlier passwords is prevented and validity is limited in time.**

What proves it: Configuration extract showing the password history, for example reuse of the last five passwords blocked, and the configured maximum validity. Requirement enhancement, required from SL 3 onwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 1.7 RE 2 **The limit on password lifetime applies not only to people, but to all accounts, including service, maintenance and device accounts.**

What proves it: Rotation plan for technical accounts with the last and the next change date per account, plus evidence of the changes, for example a change record or a ticket. Requirement enhancement, required only from SL 4 onwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 1.8 **Where certificates are used, they come from an orderly certificate management with defined rules for request, issuance, validity period, renewal and revocation.** Document

What proves it: Certificate policy or a short written rule stating responsibility, validity periods and the revocation path, plus an inventory of the issued certificates with their expiry dates. A small operation keeps a table with certificate, device, expiry date and reminder date, which prevents silent plant downtime caused by expired certificates. Required from SL 2 onwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 1.9 **When key pairs are used for authentication, the system validates the certificate completely: chain of trust, validity period, revocation status and proof that the counterpart actually holds the private key. The link between certificate and account is unambiguous.**

What proves it: Configuration extract with revocation checking enabled, for example CRL or OCSP, test record of a rejected logon with an expired or revoked certificate, plus the mapping table of certificate to account. Required from SL 3 onwards, not required at SL 1 and SL 2.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 1.9 RE 1 Private keys reside exclusively in hardware backed storage from which they cannot be read out, and they are also used inside that storage.

What proves it: Data sheet or certification evidence of the security component used and a configuration extract showing that the key is generated inside the component, so that the private key never leaves it. Requirement enhancement, required only from SL 4 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.10 During logon the system reveals no information that could be exploited. Passwords entered are obscured and error messages do not disclose whether the identifier or the password was wrong.

What proves it: Screenshot of the logon screen with masked input and a screenshot of the error message after a failed attempt. For devices that cannot do this technically, for example older operator panels, add a short note on the compensating measure, for example restricted physical access to the installation location. Required from SL 1 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.11 The number of consecutive failed logon attempts is limited and the response to it is configurable, for example a temporary lockout. The chosen response does not impede safety related operation of the plant.

What proves it: Configuration extract with the threshold, for example lockout after <= 5 failed attempts, and the lockout duration, plus a short assessment of why the lockout does not block emergency operation or a safe shutdown of the plant. At operator stations with a safety function, a timed lockout is preferable to a permanent account lock. Required from SL 1 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.12 A use notification can be displayed before logon, pointing to the rules for using and monitoring the system. Text and display are configurable by the asset owner.

What proves it: Screenshot of the displayed notice text and the approved wording with the date of approval. Small operations agree the wording briefly with the employee representation or with management, one paragraph is enough. Required from SL 1 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.13 Access from untrusted networks, for example remote maintenance by suppliers, is restricted to defined paths, is monitored and can be interrupted at any time.

What proves it: Inventory of the remote access paths with purpose, remote party, contact person and the path used, plus connection logs and evidence of the ability to disconnect, for example a key switch, a firewall rule or a remote maintenance router that can be switched off. Required from SL 1 onwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 1.13 RE 1 Each individual session from an untrusted network is explicitly approved by a responsible person before the connection is established, a permanently open connection is not sufficient.

What proves it: Approval records per remote maintenance session with time, reason, approving person and duration, technically for example via a key switch at the access router or via an approval portal. In a small operation a remote maintenance logbook at the control cabinet, signed off by the maintenance technician for each session, is sufficient. Requirement enhancement, required from SL 2 onwards and therefore never at SL 1.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6 FR 2: Use Control (Privileges, Sessions, Audit Records) 24

SR 2.1 **The system technically enforces the privileges that have been granted: every logged-on person, every device and every software process receives exactly the access assigned to it, and any attempt that goes beyond this is rejected.**

What proves it: A privilege concept mapping accounts to permissions, plus a screenshot or configuration extract per control system, HMI and engineering station showing the active privileges. In addition, a test record in which a low-privilege account attempts a blocked action and is rejected. Required from SL 1. A small operation manages with two or three roles, for example operate, maintain, engineer, and documents them on a single page.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.1 RE 1 **Privilege enforcement applies not only to human operators but equally to software processes and devices that access the system on their own.**

What proves it: A list of technical and service accounts, for example OPC UA clients, historian connections, backup services, each with its assigned privilege set. An extract from the privilege management showing that these accounts do not run with administrator rights. Requirement enhancement, required from SL 2, not at SL 1.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.1 RE 2 **Privileges are not granted to individuals one by one but through roles, and the mapping from role to permitted actions is recorded in a traceable way.** Document

What proves it: A role and privilege matrix as a table: rows are the roles, columns the actions such as change setpoint, download program, acknowledge alarm, create account. Plus the list mapping person to role. Requirement enhancement, required from SL 2. A maintained spreadsheet carrying a change date is fully sufficient as evidence.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.1 RE 3 **For narrowly defined exceptional cases an authorized supervisor can lift a privilege restriction for a limited period, and every such override is recorded in the audit trail.**

What proves it: A procedure description for the exception approval stating who may grant it and how long it remains valid, plus audit records of overrides already granted, taken from the system log. Requirement enhancement, required from SL 3.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.1 RE 4 **Particularly critical interventions require approval by two independent authorized persons before the action is carried out.**

What proves it: A list of the actions subject to dual approval, for example changing safety parameters or downloading a new control program, together with configuration evidence and audit records naming both approvers. Requirement enhancement, required only from SL 4.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.2 **The use of wireless connections in the automation network is tied to an explicit authorization, and only approved participants may exchange data or intervene over the air.**

What proves it: An inventory of all wireless links, for example WLAN access points, Bluetooth pairings, cellular routers, each with its purpose and its approved participants. Plus the access control configuration at the access point. Required from SL 1. Anyone who operates no wireless link in the process network states exactly that in writing and supports it with a configuration view showing wireless disabled.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.2 RE 1 Unauthorized wireless devices in the vicinity of the automation network are detected and reported.

What proves it: A record from wireless monitoring or a recurring wireless scan with date, result list and a note on every unknown device. The reporting path to the responsible function is named. Requirement enhancement, required from SL 2, not at SL 1. A small operation can run a quarterly scan with a notebook and file the result as a record.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 2.3 The use of portable and mobile devices on the system, for example service notebooks, USB storage or tablets, is governed by rules and technically limited to explicitly approved devices.

What proves it: The rule set for device use, a list of approved service devices with their identifiers, and evidence of the technical restriction, for example USB ports on HMI and engineering station disabled or limited to specific devices. Required from SL 1. A small operation works with two labelled service sticks that are only written to at a single transfer station.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 2.3 RE 1 Before connection, the security state of a portable or mobile device is checked, and devices that do not meet the requirements are prevented from gaining access.

What proves it: The check criteria for the device state, for example current malware protection and patch level, plus check records per service device and evidence of the technical enforcement, for example through a transfer station or a network access control. Requirement enhancement, required from SL 3.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 2.4 For mobile code executed on the system, for example scripts in operator interfaces or active content in reports, it is defined which types are permitted, and types that are not permitted are prevented from executing.

Document

What proves it: A definition of which mobile code is allowed on which systems, plus configuration evidence of the restriction, for example script execution in the HMI browser disabled, macros in evaluation files blocked. Required from SL 1. A one-page definition covering the three or four cases that actually exist is sufficient.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 2.4 RE 1 Before mobile code is executed, it is verified that it comes from the expected source and has not been altered.

What proves it: Configuration evidence of the signature verification or checksum control, plus a test record in which manipulated or unsigned code is rejected. Requirement enhancement, required from SL 3.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 2.5 A session is locked after a defined period without operator action and is released again only after renewed authentication, without losing the display of safety relevant process information.

What proves it: A configuration extract with the configured lock time per workstation, plus a justification for workstations in permanently manned control rooms where the lock is deliberately set differently. Required from SL 1. Visual evidence: a screenshot of the lock screen with the alarm line still visible.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 2.6 Remote sessions are terminated after a defined period without activity or on demand of the operator, so that no open remote connection remains unattended.

What proves it: The remote access configuration with its inactivity time limit, audit records of terminated remote sessions, and a description of how the operator can immediately disconnect an ongoing remote maintenance session, for example through a key switch or a per session release. Required from SL 2, not at SL 1.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 2.7 **The number of concurrent sessions per account or role is limited, and login attempts beyond that limit are rejected.**

What proves it: A configuration extract with the defined upper limit per role, for example <= 1 concurrent session for engineering accounts, plus a test record of the rejected second login attempt. Required from SL 3.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.8 **Security relevant events are recorded, and every entry names at least the time, the source, the triggering account, the type of event and the outcome.** Document

What proves it: A definition of the event types to be recorded, for example login, failed login, privilege change, program change, configuration change, plus a genuine excerpt of the audit log showing the named fields. Required from SL 1. A small operation collects the logs from control system, HMI and firewall in one folder with a fixed retention period.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.8 RE 1 **The audit records of the individual components are brought together at a central point and form a single, system wide record that can be evaluated as a whole.**

What proves it: An architecture sketch of the log collection showing all connected sources, plus an evaluation that places events from at least two components on one timeline. Requirement enhancement, required from SL 3.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.9 **Sufficient storage is provided for the audit records so that events are retained over the defined retention period and are not overwritten unintentionally.**

What proves it: A calculation or estimate of the storage need from daily log volume times retention period, plus the configured storage size and the archiving rule. Required from SL 1. In practice a daily copy to a separate storage location with a documented retention period is enough.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.9 RE 1 **When a defined fill level threshold of the audit storage is reached, a warning is issued to the responsible function before the storage capacity is fully used up.**

What proves it: A configuration extract of the threshold, for example a warning from >= 80 percent utilization, plus an example of the triggered notification and the recipient list. Requirement enhancement, required from SL 3.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.10 **If the audit logging fails or the audit storage runs full, the system reacts in a previously defined manner and the responsible function is informed, without endangering the safe operation of the plant.**

What proves it: The defined reaction per failure case, for example overwrite older entries and raise a notification instead of stopping the plant, with a justification from the process point of view. Evidence through a triggered test notification and the corresponding audit entry. Required from SL 1.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.11 **Every audit record carries a timestamp from a named time source, so that events from different components can be placed in order relative to one another.**

What proves it: A statement of the time source used per component and a log excerpt with a visible timestamp including the time zone. Required from SL 2, not at SL 1.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 2.11 RE 1 **The clocks of all participating components are synchronized against a common time source so that the deviation stays within a defined limit.**

What proves it: The time synchronization configuration, for example NTP server and synchronization interval, plus a check record with the measured deviation per component against the defined limit, for example <= 1 second. Requirement enhancement, required from SL 3.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 2.11 RE 2 **The time source itself is protected against manipulation, and an implausible or altered time reference is detected and reported.**

What proves it: A description of how the time source is protected, for example authenticated time synchronization, restriction to an internal source, monitoring for time jumps, plus notifications or audit records of a detected deviation. Requirement enhancement, required only from SL 4.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 2.12 **For defined critical actions it can be established beyond doubt afterwards who triggered them, so that the acting person cannot credibly deny having done so.** Document

What proves it: A list of the actions this evidence applies to, for example recipe change, batch release, change of limit values, plus the corresponding records with a unique person identifier and evidence that group accounts are excluded for these actions. Required from SL 3.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 2.12 RE 1 **The undeniable attribution of the acting person applies not only to selected critical actions but to all users and all actions they trigger.**

What proves it: Evidence that every account is tied to a single person and that no shared logins remain, plus a log excerpt of arbitrary actions in which a unique person identifier appears throughout. Requirement enhancement, required only from SL 4.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

7 FR 3: System integrity, protecting data, software and sessions against unauthorised modification 19

SR 3.1 **The control system detects when information has been altered while in transit over a communication channel, and it does so for control data, configuration data and management traffic alike. The protection also covers connections that leave the system or cross untrusted network segments.**

What proves it: A network and protocol overview stating which channel uses which integrity mechanism (checksum, message authentication code, signed telegrams), a configuration extract of the fieldbus or OPC UA security settings, and a test record showing that a tampered telegram was demonstrably rejected. A small operation captures this in a table per connection with the columns source, destination, protocol and integrity mechanism, and evidences effectiveness once with a traffic capture. Required from SL 1 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.1 RE 1 **Integrity protection in transit relies on cryptographic mechanisms, so that a deliberate manipulation by an attacker using their own means cannot pass undetected. A simple checksum against transmission errors is not sufficient here.**

What proves it: A list of the cryptographic mechanisms and key lengths in use per channel, a reference to the underlying key management, and configuration extracts (for example TLS cipher suites, OPC UA SecurityPolicy, IPsec profiles). Small operations rely on the secure default profiles of their controllers and file a screenshot of the active setting. Requirement enhancement, required from SL 3 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.2 **Protection mechanisms against malicious code are in place that prevent unwanted program code from executing on system components and that report any detection. The mechanisms are chosen so that they do not disturb the intended operation of the plant, and they are kept current.**

What proves it: An overview per component of which mechanism applies (anti-virus, application whitelisting, hardened operating system without execution rights), evidence that signatures or whitelists are updated, and alerts from the protection system. Where anti-virus is not feasible, for instance on a controller, the compensating measure is recorded with its rationale. Small operations do well with whitelisting on the operator PC and a written rule for USB media. Required from SL 1 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.2 RE 1 **Protection against malicious code additionally takes effect at the entry and exit points of the plant, where data enters or leaves, and not only on the end devices themselves.**

What proves it: A list of all entry and exit points (remote maintenance access, data transfer gateway, removable media, handover to the office network, email path for program versions) with the scanning mechanism effective at each, plus records of the handovers that were checked. Small operations set up a single handover PC with virus scanning as a gateway and fix this in a work instruction. Requirement enhancement, required from SL 2 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.2 RE 2 **The protection mechanisms against malicious code are managed from a central point, updates are distributed centrally, and detections are collected in one place for evaluation.**

What proves it: The configuration of the central management console, a report on the update status of all connected components, and an evaluation of reported detections over a period of time. Requirement enhancement, required from SL 3 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.3 **The security functions of the system are verified at planned intervals and after changes to confirm that they actually work. The tests are scheduled so that they do not endanger plant operation, and the results are recorded.** Document

What proves it: A test plan stating the object under test, the interval and the time window, together with the test records showing date, tester, expected behaviour and observed behaviour. Useful individual tests are: a login with a disabled account fails, the anti-virus reacts to a test file, remote maintenance access is unreachable without release. Small operations attach the testing to the maintenance shutdown that is planned anyway and work through a fixed checklist. Required from SL 1 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.3 RE 1 **Verification of the security functions runs with automated means, so that it is repeatable without manual effort and delivers a consistent result.**

What proves it: The scripts or test tools together with their schedule, their output files, and a comparison of several runs showing that deviations are detected. Requirement enhancement, required from SL 3 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.3 RE 2 **Verification of the security functions is also possible during normal operation, without having to stop the plant or place it into a special state.**

What proves it: A description of the test procedure with evidence that it has no adverse effect on the process, for example an analysis of the impact on cycle times and network load, plus test records taken from productive operation. Requirement enhancement, required from SL 4 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.4 **Unauthorised changes to software, firmware and information at rest are detected. This applies equally to control programs, parameter sets, recipes and configuration files.**

What proves it: An inventory of the versions worth protecting with stored check values or signatures, the results of the integrity comparisons, and the documented reconciliation with the version held in version control. Small operations store the released program version together with its checksum in a write-protected location and compare on suspicion or after maintenance. Required from SL 1 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.4 RE 1 **If a violation of the integrity of software or information is detected, the system reports this automatically to a responsible point, without anyone having to actively look for it.**

What proves it: The configuration of the notification paths (alarm in the control room, email, message to the monitoring system), a recipient list with deputy arrangements, and at least one test alarm with a documented response time. Requirement enhancement, required from SL 3 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.5 **Inputs that the system accepts from process data, interfaces or user interfaces are checked for permitted syntax, permitted value range and permitted length before they are processed. Invalid inputs do not lead to uncontrolled behaviour.**

What proves it: A specification of the limits and formats per input, extracts from the validation logic in the controller or application, and test cases with deliberately invalid inputs (a value that is too large, a wrong data type, an overlong character string) together with the documented behaviour of the system. Small operations record the plausibility limits per measuring point in a table and verify them during commissioning. Required from SL 1 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.6 **For the event of a fault it is defined which state the outputs to the plant assume, and the system assumes exactly that state. The defined state is aligned with the functional safety of the plant.**

What proves it: A definition per output or output group (hold value, defined substitute value, safe shutdown state) with a rationale from the risk assessment, a configuration extract of the controller, and evidence from a failure test, for example a cable break or loss of communication, showing the expected behaviour. Required from SL 1 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.7 **The system handles error conditions in such a way that operation remains under control and no information is disclosed that would help an attacker. Error messages shown to operators stay brief, while the technical details go only into the internal records.**

What proves it: An overview of the error classes with the system behaviour foreseen for each, examples of the displayed messages compared with the corresponding internal log entries, and test evidence that no file paths, account names, database output or version details appear on the operator interface. Required from SL 1 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.8 **Active sessions are protected against hijacking and against the injection of foreign messages. A session ends after logout or after a defined period without activity, and afterwards it cannot be reused.**

What proves it: The configuration of session management with the configured limits for idle time and maximum duration, evidence of the mechanism protecting against message replay, and a test record in which a captured session no longer works after logout. Required from SL 2 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 3.8 RE 1 **Session identifiers lose their validity when the session ends and are not accepted again by the system, not even when they are presented again from outside.**

What proves it: A configuration extract of session management covering invalidation, plus a test record in which a previously valid identifier is sent again after logout and is rejected by the system. Requirement enhancement, required from SL 3 upwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 3.8 RE 2 **For every new session a dedicated, single use identifier is generated. Identifiers are not reused across sessions, users or devices.**

What proves it: A description of the generation procedure and evidence from the log or a traffic capture that several consecutive logins receive different identifiers. Requirement enhancement, required from SL 3 upwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 3.8 RE 3 **Session identifiers are generated with recognised random mechanisms, so that they can neither be guessed nor derived from preceding identifiers.**

What proves it: A statement of the random number generator used and its entropy source, a supplier declaration or test report on it, and a statistical evaluation of a sample of generated identifiers. Requirement enhancement, required from SL 4 upwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 3.9 **The security related records and the tools used to evaluate them are protected against unauthorised access, modification and deletion. The circle of people allowed to change or remove records is kept narrow and is named.** Document

What proves it: An authorisation concept for the log data with named assignment, the configuration of forwarding to a separate logging system, retention periods, and test evidence that an ordinary operator cannot delete entries. Small operations forward the logs to a separate device to which the plant operators have no write access. Required from SL 2 upwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 3.9 RE 1 **The security related records are additionally stored on a medium that rules out subsequent overwriting, so that an entry once written can no longer be altered, not even with administrative rights.** Document

What proves it: A description of the storage used (write once medium, tamper resistant archive, continuously extended signature chain), evidence of an unsuccessful attempt to change an entry, and the rule for how the media are retained and retrieved. Requirement enhancement, required from SL 3 upwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

8 FR 4: Data Confidentiality 6

SR 4.1 **The automation system protects confidential information against unauthorised disclosure, both while it is in transit and while it is at rest. It is defined which data counts as confidential, for example recipes, parameter sets, credentials, configuration files or diagnostic data with a personal reference.** Document

What proves it: A list of the data types worth protecting, stating where they are held and how they are transmitted, plus the specific protective measure for each entry, for example an encrypted connection, an encrypted storage medium or a restricted share. A small operation manages with a single-page table: data type, where it sits, who may see it, what protects it. Required from SL 1 upwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

SR 4.1 RE 1 **For information that travels across untrusted networks or is stored outside the protected environment, confidentiality is enforced by technical means rather than merely promised in an organisational rule.**

What proves it: A configuration extract of the transport encryption or storage encryption in use, for example the VPN profile for remote maintenance, the TLS settings of the control system interface, or the encryption of the backup media. A dated screenshot of the active setting is enough as evidence. Required from SL 2 upwards, not from SL 1, because this is a requirement enhancement.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 4.1 RE 2 **Confidentiality is also enforced at the boundaries between zones, so that information does not become visible in the clear when it crosses from one zone into another.**

What proves it: A zone and conduit plan marking which crossings are encrypted, together with the configuration of the boundary component such as a gateway, firewall or data diode. A traffic capture or a test record showing that no plaintext data appears at the boundary. Required from SL 4 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 4.2 **It is defined how confidential information is reliably removed when devices are decommissioned, change owner, go out for repair or are reused, so that no readable residual data is left behind.** Document

What proves it: A written decommissioning procedure with the sanitisation method per device type, plus erasure records giving the device identification, the date and the person who carried it out. A small operation records this as one line per device in a shared list and files the certificates of external disposal contractors alongside it. Required from SL 2 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 4.2 RE 1 **Shared storage areas are purged before they are reallocated to another user or process, so that content belonging to the previous user cannot be read out.**

What proves it: A vendor statement or configuration record covering the purging of reused memory and buffer areas, supplemented by a test record from acceptance testing or maintenance. Where a component cannot do this, the documented compensating measure serves as evidence, for example not sharing the device across different roles. Required from SL 3 upwards, not from SL 1, because this is a requirement enhancement.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 4.3 **Wherever cryptography is used, the algorithms, key lengths and key handling follow recognised good practice, and it is defined how keys are generated, distributed, stored, rotated and revoked.** Document

What proves it: An overview of the mechanisms used per system, giving algorithm, key length and validity period, plus the key management rules and records of key rotations and certificate renewals. Public recommendations serve as the yardstick, for example the technical guidelines of the German BSI. A small operation keeps a certificate list with expiry dates and a reminder >= 30 days before expiry. Required from SL 1 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

9 FR 5: Restricted Data Flow, Zones and Conduits 11

SR 5.1 **The control system can be partitioned into separate zones, and traffic between those zones passes only through defined conduits. The partitioning follows a rationale that can be explained, for example by protection need, ownership or the function of the plant sections involved.** Document

What proves it: Network diagram showing the zones and the conduits between them, a zone list with the rationale for each boundary, and the configuration of the separating components such as VLAN definitions or firewall interfaces. A small operation gets by with a single page sketch showing office, machine network and remote access as three boxes with the links between them, plus a screenshot of the switch VLAN configuration.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 5.1 RE 1 **Zone separation is implemented physically, that is through dedicated network components and dedicated cabling, and does not rest on logical configuration inside shared devices alone. Section 9.1 in this list, required from SL 2 upwards. Requirement enhancements of this standard are never mandatory as early as SL 1.**

What proves it: Inventory of network components stating which switch or router serves which zone, photos or cabinet layout of the separated distributions, cable labelling. Small operations evidence this with two separate, clearly labelled switches instead of one shared device and a photo of the control cabinet in the plant documentation.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 5.1 RE 2 **The automation network can be operated independently of networks outside automation. If office IT or an external link fails, control and monitoring of the plant keep running. Required from SL 3 upwards.**

What proves it: Dependency list of the services used inside the automation network such as time server, name resolution, directory service or licence server, stating where each one is hosted, together with a test record of a disconnection trial in which the link to office IT was pulled. A small operation notes the outcome of such a trial in the maintenance log: uplink pulled, plant kept running, only the office reports were missing.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 5.1 RE 3 **Zones carrying particularly critical functions, for example safety or protection functions, are separated from the remaining zones both logically and physically. Required from SL 4 upwards.**

What proves it: Marking of the critical zones in the zone diagram with the rationale for the classification, evidence of dedicated network components and dedicated cabling for those zones, configuration of the conduits with evidence that no shared path exists.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 5.2 **At the zone boundaries, traffic is controlled, monitored and either permitted or denied according to defined rules. There is no path between two zones that bypasses this control point.**

What proves it: Exported rule set of the firewall or boundary device, logs of denied and permitted connections, evidence that no side paths exist, for example through a check for additional network cards, modems or cellular routers in plant computers. A small operation evidences this with the rule export of its single firewall and a short walkthrough note confirming that no unplanned router sits in any control cabinet.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 5.2 RE 1 **The rule set at the zone boundary works on the principle that everything is denied unless it has been explicitly permitted. Every permit rule is individually justified and tied to a purpose. Required from SL 2 upwards.**

What proves it: Rule set with a visible final rule that drops the remainder, and a permit list stating source, destination, service, purpose and responsible person for each rule. Small operations keep this list as a five column table alongside the firewall export and review it once a year for rules nobody needs any more.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 5.2 RE 2 **The automation network can be deliberately cut off from all external connections and kept running in island mode. The action can be triggered without having to stop the plant. Required from SL 3 upwards.**

What proves it: Description of the isolation procedure stating who may trigger it and how, evidence of the technical implementation such as an emergency rule set or a labelled isolating switch, plus the record of a drill in which the isolation was actually exercised. A small operation runs the drill once a year during maintenance and notes date, duration and anything unusual.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 5.2 RE 3 **If the device at the zone boundary fails or loses its rules, it denies traffic instead of passing it. A failure must not leave an open connection behind. Required from SL 4 upwards.**

What proves it: Supplier statement or configuration evidence on how the component behaves on fault and on restart, test record of a deliberately induced failure with the observed result, alignment with the plant risk assessment, because a boundary that denies traffic can itself have consequences depending on the process.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 5.3 **General person to person communication services such as email, messaging or video calls can be prevented on automation devices and inside automation networks. The scope of the block is defined and justified.**

What proves it: Definition of which services are not permitted in the automation network, plus the technical implementation: blocked ports and destinations in the rule set, removed or blocked applications on operator stations, evidence from the device software inventory. A small operation handles this with an application block on the HMI station and a rule that outbound mail and web traffic from the machine network is denied.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 5.3 RE 1 **Such person to person communication services are prevented across the whole automation network, not merely restricted in part or limited to individual devices. Required from SL 2 upwards.**

What proves it: Evidence that the block applies to every device in the zone, for example through a review of the installed software on each computer in the zone and a connection test from an arbitrary plant computer. Small operations evidence this with a device list in which every row is ticked off with the check date, and a screenshot of the failed connection attempt.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 5.4 **Application data and application functions are partitioned so that processes with different protection needs or different privileges cannot reach the same areas. The separation is designed into the system architecture and is not left to the accident of installation.**

What proves it: Overview of the applications stating which data and services they use and which accounts sit behind them, configuration of separate instances, databases, directories or virtual machines, and a privilege list per area. A small operation solves this with separate user accounts and separate data folders for engineering and operation, plus a note on which application accesses which folder.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

10 FR 6: Timely Response to Events 3

SR 6.1 **The audit records collected in the system can be read and evaluated by the persons and roles authorised for that purpose without disturbing the running operation of the plant, and access to those records is itself restricted to authorised users.**

What proves it: A role and permission matrix showing who may view log data, plus a screenshot or export of a log view that was actually retrieved, carrying a timestamp. Add a short note on the route used for retrieval, for example the controller operator interface, a log server or a file export. Small operations get by with a one-page overview per plant: where the log sits, who has read access, how it is fetched. A test retrieval once a year, recorded in the maintenance log, shows the route works. Applies from SL 1 upwards for all security levels.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 6.1 RE 1 **The audit records can be retrieved through a machine interface so that analysis tools can process them further without manual re-typing, and the data is provided in a documented, commonly used format.**

What proves it: A description of the interface in use together with the format, for example syslog, OPC UA Alarms and Conditions, a REST query or a CSV export, plus a sample record and the configuration of the receiving system. Evidence can be an extract from the SIEM or log collector configuration together with proof of incoming records. Without a SIEM, a log collector on a simple server that pulls the logs overnight by script and stores them is enough; the script itself plus a directory listing of the collected files is the evidence. As an enhancement this is only required from SL 3 upwards, not from SL 1.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 6.2 **Security-relevant activity in the system is monitored continuously, the monitoring detects attempted attacks and misuse and reports them promptly to a named point of contact, and the tools, reporting routes and responsibilities used for this are defined.**

What proves it: An overview of the monitoring tools per zone, for example a network sensor, antivirus alerts, firewall alarms or integrity checking, stating who receives the alert and within what time frame a response is expected. Alarm configurations, a list of alerts raised in recent months and the handling notes for them serve as evidence. Small operations do not need a round-the-clock control room: a shared mailbox or ticket inbox that bundles the alerts of the existing systems, plus a fixed rule that a named person reviews it on every working day, is sufficient and is evidenced through the mailbox history. Required from SL 2 upwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

11 FR 7: Resource Availability 13

SR 7.1 **Under overload or deliberate flooding attacks the system stays in a defined operating state, the essential control functions keep running, and the failure of an individual service does not drag the plant down with it.**

What proves it: Configuration of the protective mechanisms (rate limiting, connection limits, broadcast storm control on the switches), vendor statements on behaviour under load, plus a record of a load test or of a real overload event with observation of the control function. Required from SL 1 onwards. A small operation covers this with screenshots of the switch and firewall settings and a short note on which function kept running during a test of the most important cell.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 7.1 RE 1 **The communication load that individual components can inject into the network is capped, so that a faulty or compromised component cannot flood the network segment.**

What proves it: Per-port bandwidth and multicast limits on the network components, evidence of the cap for each connection, plus a measurement of the actual baseline load per device. Required from SL 2 onwards, not from SL 1. Without managed switches this line cannot be evidenced, and that is then the open point.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 7.1 RE 2 **An overload situation inside the system under consideration does not spill over into adjacent systems or networks; the outward impact is technically contained.**

What proves it: Segmentation and filtering rules at the boundaries, evidence that outbound traffic is capped, plus a test record showing that a load generated in the cell network did not degrade the office or neighbouring network. Required from SL 3 onwards.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 7.2 **The use of processing time, memory, storage space and network bandwidth is bounded such that a single process or service cannot consume the resources needed for control.**

What proves it: Configuration of the resource limits (quotas, process priorities, memory limits), evaluation of utilisation monitoring over a representative period, plus the thresholds at which a warning is raised. Required from SL 1 onwards. Small operations use the built-in means of the operating system and simple monitoring with a disk space and CPU alert by e-mail.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 7.3 **Backups exist for the system configurations, application data and program versions; they can be produced without interrupting running operations and are protected against unauthorised access and modification.** Document

What proves it: Backup concept covering scope, frequency and retention period, backup logs of the most recent runs, plus evidence of access protection for the backup media (separate storage, encryption, dedicated permissions). Required from SL 1 onwards. A small operation backs up PLC projects and HMI versions to an encrypted medium that is physically disconnected after the backup, and records date and version in a simple list.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

SR 7.3 RE 1 **The usability of the backups has been verified; it is evidenced that a working state can actually be restored from them.**

What proves it: Record of a restore trial with date, backup version tested, target system and result, at least for the critical components. Required from SL 2 onwards, not from SL 1. Small operations check one PLC program and one HMI image on a spare device once a year on a sample basis and record the result in two sentences.

Open In progress Met Not applicable

Evidence / justification

SR 7.3 RE 2 **The backup runs automatically on a defined schedule; a failed run is detected and reported.**

What proves it: Schedule of the backup job, execution logs without gaps, plus evidence of the failure notification for a run that did not succeed (alarm, ticket, mail). Required from SL 3 onwards.

Open In progress Met Not applicable

Evidence / justification

SR 7.4 **After a disturbance, failure or attack the system can be returned to a known, secure state; the recovery has been rehearsed and the responsibilities are named.** Document

What proves it: Restart plan for each critical component with sequence, media required, contacts and target time, together with the record of the most recent recovery exercise. Required from SL 1 onwards. A small operation gets by with a one-page restart card per line, kept in the control cabinet and checked whenever a spare part is replaced.

Open In progress Met Not applicable

Evidence / justification

SR 7.5 **If the regular power supply fails, the system moves into a defined state: either the supply is maintained by a backup source or an orderly shutdown takes place without loss of the secure state.**

What proves it: Sizing and maintenance evidence for the uninterruptible power supply or the emergency generator, test record of the most recent battery or load test, plus a description of the behaviour on switchover and on return of mains power. Required from SL 1 onwards. Small operations test the UPS under load once a year and record test date, bridging time and battery age.

Open In progress Met Not applicable

Evidence / justification

SR 7.6 **The network and security settings of the system are fixed to an approved target state, deviations from that target state are detectable, and the current state can be retrieved at any time.** Document

What proves it: Approved target configuration per device class (hardening specification), current configuration states of the devices, plus the result of a target versus actual comparison with a list of deviations and the reason for each. Required from SL 1 onwards. A small operation stores the configuration exports under version control and compares them before and after every change.

Open In progress Met Not applicable

Evidence / justification

SR 7.6 RE 1 **The current state of the security settings can be output in machine-readable form so that it can be checked automatically against the target state.**

What proves it: Sample output in a machine-readable format (configuration export, structured file, interface query) and the script or tool that performs the comparison against the target state, together with the result report of one run. Required from SL 3 onwards.

Open In progress Met Not applicable

Evidence / justification

SR 7.7 **The system is restricted to the functions needed for operation; services, ports, protocols and interfaces that are not required are disabled or removed.**

What proves it: List of active services and open ports per component with a justification of the need, evidence that the remaining ones are disabled (configuration, port scan result), plus a rule for USB and maintenance interfaces. Required from SL 1 onwards. Small operations run a simple port scan per segment and justify every open item in one line.

Open In progress Met Not applicable

Evidence / justification

SR 7.8 **A current inventory of all system components with manufacturer, type, firmware or software version and network address is available and is kept up to date when changes occur.** Document

What proves it: Component inventory with its revision date and owner, evidence of upkeep via the change history, plus a comparison against a network discovery to find devices that are not recorded. Required from SL 2 onwards, not from SL 1. A small operation keeps the inventory as a table and updates it as a firm rule whenever a device is replaced and whenever firmware is updated.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification