Support for Essential Functions

Disclaimer

Maintenance

After release, this document immediately enters the maintenance phase. Maintenance includes error corrections and general improvement of the document. Please send your change requests to the following email address: cybersecurity.review@ertms.be

This document lists the requirements of the technical security specifications which either support essential functions or have an adverse effect on essential functions. In case of adverse effects, mitigations are documented.

Outline Number	Description	Support for essential function Assessment
SP-SEC-Comp-5.3.5-1	If the Secure Component has physical I/O controlling an automation process, the Secure Component shall provide the capability to set all physical outputs to a predetermined state if normal operation cannot be maintained. Note: The predetermined state is normally the safe state of the component and normally invoked in fault situations and realized by the safety system.8	Requirement supports essential functions (avoiding adverse effects).
SP-SEC-Comp-5.4.3-2	The Secure Component shall support separate re-authentication per physical network interface using NAC.	Requirement supports essential functions (avoiding availability impact for network connectivity).
SP-SEC-Comp-5.4.4-1	The Secure Component shall limit use of system resources by security functions to protect against resource exhaustion. Note: This can be tested by monitoring system resources as CPU utilization, volatile memory, persistence memory and network utilization during normal and stress situations over an extended period of time. The test should show that resource utilization stays in the specified limits.	Requirement supports essential functions (avoiding system resource exhaustion).
SP-SEC-Comp-5.4.4-2	After a Denial of Service (DoS) event (e.g. saturation / high load of the network interface), the Secure Component shall operate normally. Note: recommended test time for network saturation is at least one minute, recommended time to check for normal operation after network saturation is 30 seconds. This supports maintaining essential functions in a degraded mode as the result of a DoS event, together with SPPRAMSS-2630 and SPPRAMSS-9633	Requirement supports essential functions (avoiding adverse effects after DoS).
SP-SEC-Comp-5.4.4-3	The Secure Component shall provide the capability to only allow a configurable maximum number of concurrent sessions per interface for any given user (human, or technical user).	Requirement supports essential functions (avoiding system resource exhaustion).

Outline Number	Description	Support for essential function Assessment
SP-SEC-Comp-5.5.2-5	The Secure Component shall automatically request the renewal of its certificates a configurable number of days in advance to the certificate's expiration date. Note: after rekeying a certificate, it is recommended to not revoke the old certificate to keep CRLs manageable.	Requirement supports essential functions (avoiding availability impact on communication).
SP-SEC-Comp-5.5.2-7	If the renewed certificate(s) corresponds to a two-channel safety-related connection (e.g. SCI), the Secure Component shall re-establish communications only one active channel at a time. Note: If in a two-channel safety communication, one channel is not active (e.g. in maintenance, not connected), a diagnostic event should be generated and the re-establishment should happen when the other channel becomes active again.	Requirement supports essential functions (avoiding availability impact on communication).
SP-SEC-Comp-5.5.2-12	If an CRL update contains certificate which is used in current communications, the Secure Component shall terminate the communications using the revoked certificate.	Requirement has adverse effect on availability (makes communication impossible). Mitigation: SP-SEC-PGRM-10.1-7 The railway shall define and implement a process to revoke a certificate in a in a predetermined time. provides a process to avoid adverse impact of expired or revoked certificates
SP-SEC-Comp-5.6.1-1	The Secure Component shall support the update of software and configuration via the interface (I-STD-MAINTENANCE (SMI) Note 1: when updating non-safety related software, typically also the process allowlist has to be updated. Note 2: this supports together with the backup and restore functionality (chapter 5.6.3) the recovery and reconstitution to a known secure state after a disruption or failure.	Requirement has adverse effect on availability (makes device unavailable to perform essential functions during update period). Mitigation: SP-SEC-PGRM-9-1.25 The railway shall follow IEC 62443-2-1 DATA 1.3 for updating the secure component... requiring policies and procedures for updating safety system only when configuration mode is enabled. Also the I-STD-MAINTENANCE specification supports this procedure.

Outline Number	Description	Support for essential function Assessment
SP-SEC-Comp-5.7.1-7	If the storage capacity is exceeded, the Secure Component shall overwrite the oldest log entry first.	Requirement supports essential functions (avoiding system resource exhaustion).
SP-SEC-Comp-7.2-1	If the Secure Component provides a human-machine interface, the Secure Component shall support human user authentication using the central authentication service via SSI-UAS.	Requirement has adverse effect on availability (access restriction to human-machine interface). Mitigation: SP-SEC-PGRM-11-5 The railway shall define a process, including frequency, for regular check of all access rights concerning their need and validity this ensures that access rights are changed in a controlled fashion avoiding impact on essential functions SP-SEC-PGRM-13-4: The railway shall align the overall system RAM (Reliability, Availability, Maintainability) target with the security availability concept. SP-SEC-PGRM-13.1-4: The railway shall have a resource availability and redundancy management based on ISO 27002 8.14 this ensures high availability of the SSI-UAS
SP-SEC-Comp-7.2-2	If the Secure Component provides a human-machine interface, the Secure Component shall enforce the permissions received from the IAM service via SSI-IAM for the corresponding communication session.	Requirement has adverse effect on availability (access restriction to human-machine interface). Mitigation: SP-SEC-PGRM-11-5 The railway shall define a process, including frequency, for regular check of all access rights concerning their need and validity this ensures that access rights are changed in a controlled fashion avoiding impact on essential functions

Outline Number	Description	Support for essential function Assessment
SP-SEC-Comp-7.2-4	If the Secure Component provides a human-machine interfaces, the Secure Component shall lock or terminate sessions after a time period of inactivity depending on configuration.	Requirement has adverse effect on availability (access restriction to human-machine interface). Mitigation: see SP-SEC-Comp-7.2-7
SP-SEC-Comp-7.2-5	If the Secure Component provides a human-machine interfaces, the Secure Component shall enable the human user to lock or terminate sessions manually.	Requirement has adverse effect on availability (access restriction to human-machine interface). Mitigation: see SP-SEC-Comp-7.2-7
SP-SEC-Comp-7.2-6	If the Secure Component provides a human-machine interfaces, the Secure Component shall unlock the locked human-user sessions only after re-authentication of the human user. See also SPPRAMSS-6670 for supervisor override in case of HMI controlling essential services.	Requirement has adverse effect on availability (access restriction to human-machine interface). Mitigation: see SP-SEC-Comp-7.2-7
SP-SEC-Comp-7.2-7	If a Secure Component implements a human-machine interface which is needed to control an essential service, the Secure Component shall support a supervisor manual override for a configurable time or sequence of events.	Requirement supports essential functions (provide access to a locked user interface).
SP-SEC-COMM-3.2-3	If DNS resolution was used to resolve the IP address for the corresponding connection, the TLS endpoint shall abort the connection if the expected DNS FQDN does not match the dNSName in the Subject Alternative Name of the communication partners certificate.	Requirement has adverse effect on availability (no communication possible for a component if DNS is misconfigured). Mitigation: SP-SEC-PrgmReq-6-11: The railway shall establish security responsibilities training This ensures that only trained personell is operating sensitive configuration (as DNS configuration).

Outline Number	Description	Support for essential function Assessment
SP-SEC-COMM-3.2-4	If DNS resolution was not used to resolve the IP address for the corresponding connection, the TLS endpoint shall abort the connection if the expected IP address does not match the iPAddress in the Subject Alternative Name of the communication partners certificate.	Requirement has adverse effect on availability (no communication possible for a component if IP addresses are misconfigured). Mitigation: SP-SEC-PrgmReq-6-11: The railway shall establish security responsibilities training This ensures that only trained personell is operating sensitive configuration (as IP address configuration).
SP-SEC-COMM-3.2-5	If an URI is used to uniquely identify the communication partners application, the TLS endpoint shall abort the connection if the expected URI does not match the URI in the Subject Alternative Name of the communication partners certificate.	Requirement has adverse effect on availability (no communication possible for a component if URIs are misconfigured). Mitigation: SP-SEC-PrgmReq-6-11: The railway shall establish security responsibilities training This ensures that only trained personell is operating sensitive configuration (as URI configuration).
SP-SEC-COMM-3.2-6	If an strongly typed Common Name which is not part of the Subject Alternative Name is used to indentify the communication partner, the TLS endpoint shall abort the connection if the expected Common Name does not match the Common Name of the communication partners certificate. Note: This procedure is used for EULYNX SCI connections.	Requirement has adverse effect on availability (no communication possible for a component if identifiers are misconfigured). Mitigation: SP-SEC-PrgmReq-6-11: The railway shall establish security responsibilities training This ensures that only trained personell is operating sensitive configuration (as identifiers configuration).

Outline Number	Description	Support for essential function Assessment
SP-SEC-COMM-3.2-8	If the status of a certificate is revoked or no valid certificate revocation information is available, the TLS endpoint shall abort the connection setup.	Requirement has adverse effect on availability (makes communication impossible). Mitigation: SP-SEC-PGRM-10.1-7 The railway shall define and implement a process to revoke a certificate in a predetermined time. provides a process to avoid adverse impact of expired or revoked certificates
SP-SEC-COMM-3.2-10	If the re-validation of a certificate fails, the TLS endpoint shall terminate the TLS connection.	Requirement has adverse effect on availability (makes communication impossible). Mitigation: SP-SEC-PGRM-10.1-7 The railway shall define and implement a process to revoke a certificate in a predetermined time. provides a process to avoid adverse impact of expired or revoked certificates
SP-SEC-SERV-6.2.2-6	If more than one network interface is used for safety communication, dedicated OSCCs shall be used for each network interface. Note: this ensures that if the communication certificate of one network interface is renewed, the connection over the other network interface maintains its independency.	Requirement supports essential functions (avoiding availability impact on communication).

Outline Number	Description	Support for essential function Assessment
SP-SEC-SERV-8-10	If the Secure Component's serial number does not exist in the Asset Inventory, the Network Authentication Server shall reply with a RADIUS EAP failure to the RADIUS authenticator.	Requirement has adverse effect on availability (no communication possible for a component without network access). Mitigation: SP-SEC-PGRM-11-5 The railway shall define a process, including frequency, for regular check of all access rights concerning their need and validity This ensures that access rights for network access control are maintained in a controlled fashion avoiding impact on essential functions. Mitigation: SP-SEC-PrgmReq-6-11: The railway shall establish security responsibilities training This ensures that only trained personell is operating the shared cybersecurity services.
SP-SEC-SERV-12.5-1	The SSI-MNT interface shall provide the maintenance method Security:FactoryReset() to purge persistent data to reset the component to factory state. Note 1: this method can be used as part of a decommissioning process SP-SEC-PGM 10.2 Decommissioning Note 2: this method does not purge the factory key material (e.g. the MDC together with its root certificates will stay on the devices. Note 3: this provides the user with the ability to erase data which requires confidentiality from persistent memory.	Requirement has adverse effect on availability (likely no operation possible with a factory reseted component). Mitigation: SP-SEC-PGRM-11-5 The railway shall define a process, including frequency, for regular check of all access rights concerning their need and validity This ensures that access rights for factory reset are maintained in a controlled fashion avoiding impact on essential functions. Mitigation: SP-SEC-PrgmReq-6-11: The railway shall establish security responsibilities training This ensures that only trained personell is operating the shared cybersecurity services.

Outline Number	Description	Support for essential function Assessment
26 items found  (type:srq AND (outlineNumber:SP-SEC-* AND NOT status:deleted AND supportsEssentialFunc.KEY:yes)) AND project.id:SPPRAMS		