6 Anhang C (normativ) - Akzeptanzkriterien

6.1 Vorbemerkung

Die Anforderungen werden nachfolgend im ursprünglichen englischen Text angegeben, da geplant ist das vorliegende Prüfschema zukünftig zu übersetzen und international einzubringen, siehe Kapitel 3.2 "Zertifizierung".

Die Akzeptanzkriterien sind primär als "accept" positiv formuliert. In manchen Fällen ist ein expliziter Ausschluss einer Umsetzung zur besseren Hervorhebung allerdings sinnvoll, diese Kriterien sind unterhalb von "not accept" aufgeführt.

6.2 FR-1: Identification and Authentication Control

ID	Requirement	SL-1	SL-2	SL-3
CR 1.1	Human user identification and authentication	Accept: - authentication of human users on all interfaces with human access	Accept: - unique authentication for every human user on all interfaces, for example with username and password	Accept: - capability to employ multifactor authentication for all human user access to the component
CR 1.2	Software process and device identification and authentication	no requirements	Accept: - the component identifies itself and authenticates to any other component using passwords, tokens or location (physical or logical) - authentication mechanism is capable to prevent attacks like man-in-the-middle or message spoofing	Accept: - uniquely identify and authenticate itself to any other component Not accept: - unencrypted authentication and identification - no recommended encryption (e.g. BSI TR-02102)

CR 1.3	Account management	Not relevant if only one fixed administrative account is implemented on the component. Accept: - capability to integrate into a higher level account management system - account management capability (only by authorized users, including adding, activating, modifying, disabling and removing accounts) - the core functionality of the component is not affected by an availability problem of the higher-level system Not accept: - no capability to enable/disable accounts	no additional requirements	no additional requirements
CR 1.4	Identifier management	Not relevant if only one fixed administrative account is implemented on the component. Accept: - capability to integrate into a system that supports management of identifiers - provide the capability to support the management of identifiers by user, group, role or control system interface	no additional requirements	no additional requirements

CR 1.5	Authenticator management	Accept: - support of (initial) authenticator content (tokens, symmetric keys, private keys, biometrics, passwords, key cards) - enforced change of default authenticators after installation or recognition of unchanged default authenticator (combined with warning message) - periodic change of authenticators - protection of unauthorized disclosure or modification of authenticators (when stored, used, transmitted) Not accept: - transmission of cleartext passwords	no additional requirements	Accept: - authenticators are protected via hardware mechanisms (e.g. Password protected memory, OTP memory, hardware data integrity checks, and device security boot mechanism) Not accept: - no hardware protection mechanism
CR 1.6	Wireless access management	Network Component Requirement Accept: - capability to identify and authenticate all users (human, software processes and devices) engaged in wireless communication	Accept: - capability to uniquely identify and authenticate all users (human, software processes and devices) engaged in wireless communication	no additional requirements

CR 1.7	Strength of password-based authentication	Accept: - enforce configurable password strength based on minimum length and variety of character types - configurable password strength according to internationally recognized and proven password guidelines, e.g. NIST SP800-63-2, BSI TR-02102 - external authentication	no additional requirements	Accept: - prevent any human user account from reusing a password for a configurable number of generations - enforce password minimum and maximum lifetime restrictions for human users - external authentication Not accept: - no configurable options for reusing passwords, i.e. password reuse cannot be prevented - no minimum and maximum lifetime restrictions for human user passwords
CR 1.8	Public key infrastructure certificates	no requirements	Relevant if PKI or public keys are in use. Accept: - interaction and operation within the scope of the PKI according to 62443-3-3 SR 1.8 ("operate a PKI according to commonly accepted best practices (see IETF RFC 3647) or obtain a public key certificate from an existing PKI")	no additional requirements

CR 1.9	Strength of public key authentication	no requirements	Relevant if PKI or public keys are in use. Accept: - provide directly or integrate into a system that provides, the capability to: - validating signature of a given certificate - validate certificate chain - in case of self-signed certificates, leaf certificates should be deployed to all hosts that communicate with the subject to which the certificate is issued - validate certification revocations status - establish user (software, human or device) control of the corresponding private key - map authenticated identity to a user by checking either the subject name, common name or distinguished name against the destination - algorithms and keys comply with CR 4.3	Accept: - protect the relevant private keys via hardware mechanisms (e.g. smart cards) Not accept: - no additional protection mechanisms
CR 1.10	Authenticator feedback	Accept: - sensitive data concerning the authentication process is obscured Not accept: - feedback not distinguish between wrong password or wrong username - no timing differences for error and no error response - displaying password, wireless key, SSH token in input field instead of asterisks - usage of WEP	no additional requirements	no additional requirements

CR 1.11	Unsuccessful login attempts	Accept: - capability to enforce, for each user type (human, software, device), a configurable limit of consecutive invalid access attempts performed in a configurable time period - capability to deny access for a specified period of time or until unlocked, when limit reached	no additional requirements	no additional requirements
CR 1.12	System use notification	Accept: - capability to display a system use notification message before authenticating to the local user interface - capability as an authorized user to configure the message	no additional requirements	no additional requirements
CR 1.13	Access via untrusted networks	Network Component Requirement Accept: - monitor and control all methods of access to the network device via untrusted networks (dial-up, office network, remote access) Not accept: - access to the network device cannot be monitored / controlled - untrusted network is missing in monitoring or cannot be	no additional requirements	Accept: - deny access requests via untrusted networks unless approved by an assigned role - for each connection a device-internal or external physical key is used to authorize the connection
CR 1.14	Strength of symmetric key-based authentication	no requirements	Relevant if symmetric key authentication (e.g. pre-shared-secrets) is used. Accept: - validate shared secret to establish the mutual trust - authentication is valid as long as shared secret remains a secret, i.e. secrets are stored securely - restrict access to the shared secret	Accept: - control system provides the capability to protect the relevant shared keys via hardware mechanisms

			- ensure that the algorithms and keys used comply with CR 4.3 (Use of cryptography)	

6.3 FR-2: Use Control

ID	**Requirement**	**SL-1**	**SL-2**	**SL-3**
CR 2.1	Authorization enforcement	Accept: - authorization mechanism is enforced on all interfaces which can accessed by human users based on their responsibilities, as dictated by the least privilege principle Not accept: - interface without authorization mechanism (e.g. HMI, web interface, console)	Accept: - authorization mechanism on all interfaces which are exposed, independent of user type (additionally technical users) - management of roles and permissions (definition and modification, only by privileged role) - management of users mapped to roles Not accept: - interface without authorization mechanism (e.g. HMI, web interface, console) - user with access to HMI can log in via console or SSH	Accept: - capability to configure a time or sequence of events during supervisor override without closing the current session Not accept: - no possibility to configure supervisor override
CR 2.2	Wireless use control	Accept: - capability to deny critical action via wireless connection (i.e. only use wired) - monitor devices	no additional requirements	no additional requirements
CR 2.3	Use control for portable and mobile devices	no requirements	no additional requirements	no additional requirements

CR 2.4	Mobile code	Only relevant if components allows to execute mobile code. Accept: - capability to enforce a security policy for the usage of mobile code - control execution of mobile code - define which users are allowed to transfer mobile code to/from device	Accept: - provides the capability to verify the integrity of the mobile code before execution is allowed Not accept: - execution is allowed without verifying the integrity of the mobile code	no additional requirements
		Embedded Component Requirements - only upload to device - perform integrity checks on the code prior to code execution - perform authenticity checks to verify origin prior to code execution		
CR 2.5	Session lock	Accept: - for HMI (local or via network): - Session Lock after configurable time period of inactivity - option to explicitly disable Session Lock (e.g. in control room scenarios) - manual session lock - access to session only possible using authentication procedures - comply with session locks requested by the underlying infrastructure (operating system, control system)	no additional requirements	no additional requirements
CR 2.6	Remote session termination	no requirements	Remote session is interpreted as logical network session. Accept: - remote session terminated by user who initiated session (minimum requirement) - remote session manually terminated by a local authority/user	no additional requirements

			- remote session terminated after configurable inactive period of time	
CR 2.7	Concurrent session control	no requirements	No requirements	Accept: - ability to limit the number of session per interface for any user Not accept: - Sessions cannot be limited per interface - Sessions cannot be limited per user
CR 2.8	Auditable events	Accept: - audit records for following security relevant cases are generated: access control, request errors, control system events, backup and restore events, configuration changes, audit log events - audit records include at least the following information: timestamp, source, category, type, event ID, event result	no additional requirements	no additional requirements
CR 2.9	Audit storage capacity	Accept: - capability to allocate audit record storage Not accept: - failure of audit functionality when a threshold is reached or the storage capacity is exceeded	no additional requirements	Accept: - a warning message informs when a configurable threshold is reached Not accept: - no warning is produced if the used storage capacity reaches the threshold - the hreshold not configurable
CR 2.10	Response to audit processing failures	Accept: - no loss of essential services or functions during an audit processing failure - optional support of	no additional requirements	no additional requirements

		appropriate actions in response to an audit processing failure - e.g. alerting personnel could be an appropriate action		
CR 2.11	Timestamps	Accept: - ability to generate timestamps for audit records (see CR 2.8) - timestamps include date and time	Accept: - synchronized timestamps - e.g. external source like NTP server	no additional requirements
CR 2.12	Non-repudiation	Relevant if HMI is used. Accept: - possibility to determine which human user took a particular action - logging user id in audit trail	no additional requirements	no additional requirements
CR 2.13	Use of physical diagnostic and test interfaces	No requirements	Exempt are software applications In case factory diagnostic and test interfaces use network communication, the interfaces are to be subjected to all of the requirements of this standard. Accept: - prevent unauthorized use of the physical factory diagnostic and test interfaces, e.g. JTAG - disabled diagnostic and test interface based on removed external connectors Not accept: - any diagnostic and test interface without authorization	Accept: - provides active monitoring of the device's diagnostic and test interfaces - generate log entry when attempts to access these interfaces are detected Not accept: - disabled diagnostic and test interface based on removed external connectors

Tabelle 7

6.4 FR-3: System Integrity

ID	Requirement	SL-1	SL-2	SL-3
CR 3.1	Communication integrity	Accept: - capability to protect integrity of transmitted information - use of CRC (protection against casual or coincidental manipulation) - use of standardized cryptographic protocol - use of recommended protocols (e.g. BSI TR-02102), see CR4.3	Accept: - capability to authenticate information during communication Not accept: - use of error detection codes, weak hashing or weak signature functions - authentication of information is not possible - fallback to not recommended protocols	no additional requirements
CR 3.2	Protection from malicious code	Software Application Component Accept: - list at least one compatible security component which implements the protection functionality (user documentation requirement)	no additional requirements	no additional requirements
		Embedded Component Accept: - capability to protect from installation and execution of unauthorized software - environment is allowed to provide malicious code protection mechanism, has to be required by component intended -use description (user documentation requirement) - allowed detection techniques: binary integrity, attributes monitoring, hashing, signature techniques - allowed prevention techniques (e.g. removable media control, sandbox techniques, specific computing platforms mechanisms (e.g. restricted firmware	no additional requirements	no additional requirements

		update), No Execute (NX) bit, data execution prevention (DEP), address space layout randomization (ASLR), stack corruption detection. mandatory access controls) Not accept: - reference to IACS capabilities which are not implemented by the component itself		
		Host Component Accept: - need to support the use of malicious code protection (design documentation requirement)	Accept: - able to automatically report version of the malicious code protection which is actually in use	no additional requirements
		Network Component Accept: - provided by the network device directly - allowed to use compensating control	no additional requirements	no additional requirements
CR 3.3	Security functionality verification	Accept: - definition of (manual) verification procedures for verifying the security functionality - guidance on how to test security functionality (documentation requirement) - documented side effects if these verification procedures are running during normal operation Not accept: - no possibility to test security functionality, e.g. no log message, no notification	no additional requirements	no additional requirements

CR 3.4	Software and information integrity	Accept: - integrity check of data at rest (e.g. software, configuration) - capability to be integrated into a system that can perform or support integrity checks Not accept: - no recording of results of checks	Accept: - authenticity check of data at rest (e.g. software, configuration)	Accept: - unauthorized change is reported to a configurable entity upon discovery of the attempt
CR 3.5	Input validation Note: Not-accept-criteria give guidance which insufficient input validation methods are most relevant for the SL levels to plan test cases with reasonable effort.	Accept: - every input, that directly impacts the action of the application or device is validated for syntax and content Not accept: - out-of-range values for a defined field type - invalid characters in data fields - missing or incomplete data and buffer overflow	Not accept: - SQL injection attacks - cross-site scripting - commonly known malformed packets	Not accept: - malformed packets as commonly generated by protocol fuzzers
CR 3.6	Deterministic output	Applicable if device directly controls a process. Accept: - the deterministic output needs to be documented (documentation requirement) - in case of failsafe, allowed to demonstrate by described process	no additional requirements	no additional requirements
CR 3.7	Error handling	Accept: - error conditions are identified and handled - no unintended information is leaked - no security relevant information is visible	no additional requirements	no additional requirements

CR 3.8	Session integrity	no requirements	Accept: - use of mechanisms to protect the integrity of communication sessions - sessions are invalidated after termination - sessions are invalidated after reboot - use of unique session IDs Not accept: - session hijacking - man in the middle attack - insertion of false information into a session - replay attacks	no additional requirements
CR 3.9	Protection of audit information	no requirements	Accept: - protect audit information and audit tools (if present) Not accept: - unauthorized access, modification or deletion of audit information	no additional requirements
CR 3.10	Support for updates	Accept: - capability to be updated and upgraded once commissioned - if component supports or executes essential functions, needs for mechanism to support patching and updating without impacting the essential function	Accept: - the authenticity and integrity of any update is validated prior installation	no additional requirements
CR 3.11	Physical tamper resistance and detection	no requirements	Not relevant in case of software applications. Relevant if intended use does not offer physical protection of component according to threat modelling. Accept: - anti-tamper resistance: specialized materials to make tampering difficult; e.g.: hardened enclosures, locks, encapsulation, security screws - detection mecha-	Accept: - capability to automatically notify upon discovery of an attempt to make an unauthorized physical access

			nisms for unauthorized physical access into the device, e.g. seal	
CR 3.12	Provisioning product supplier roots of trust	no requirements	Not relevant in case of software applications. Accept: - provision of product supplier keys and roots of trust during device manufacturing - e.g. cryptographic hashes or public key used for verification Fail: - keys or root of trust can be manipulated or leaked	no additional requirements
CR 3.13	Provisioning asset owner roots of trust	no requirements	Not relevant in case of software applications. Relevant if CR 2.4 Mobile Code is selected. Accept: - capability to provision asset owner roots of trust - protection of asset owner roots of trust Not accepted: - export of root of trust (private key) - leakage of root of trust security information	no additional requirements
CR 3.14	Integrity of the boot process	Not relevant in case of software applications. Accept: - integrity verification of boot process relevant firmware, software and configuration data prior to the use	Accept: - authentication verification of boot process relevant firmware, software and configuration data prior to the use - use of product suppliers roots of trust for verification	no additional requirements

Tabelle 8

6.5 FR-4: Data Confidentiality

ID	Requirement	SL-1	SL-2	SL-3
CR 4.1	Information confidentiality	Accept: - capability to protect against unauthorized disclosure of information via **eavesdropping or casual exposure** - capability to protect the confidentiality of information at rest for which explicit read authorization is supported - protection of the confidentiality of information in transit - (wireless) use of encryption Not accept: - outdated or deprecated encryption protocols - use of cleartext protocols (e.g. FTP)	Accept: - capability to protect against unauthorized disclosure of information caused by an attacker actively searching for vulnerabilities with **low resources, generic skills and low motivation**	Accept: - capability to protect against unauthorized disclosure of information caused by an attacker actively searching for vulnerabilities with **moderate resources, IACS specific skills and moderate motivation**
CR 4.2	Information persistence	no requirements	Accept: - capability to purge component - capability to erase all information with explicit read authorization Not accept: - existence of data after component was decommissioned	Accept: - capability to protect against unauthorized and unintended information transfer via volatile shared memory resources - capability to verify that the erasure of information occurred effectively
CR 4.3	Use of cryptography	If cryptography is required by CR 1.14, CR 3.1 and CR 4.1. Accept: - use of standardized cryptographic protocol - use of recommended protocols (e.g. BSI TR-02102), see CR4.3 - used according to proven practic-	no additional requirements	no additional requirements

		es or documentation		

Tabelle 9

6.6 FR-5: Restricted Data Flow

ID	Requirement	SL-1	SL-2	SL-3
CR 5.1	Network segmentation	Network Component Requirement Accept: - support of network segmentation, e.g. multiple network cards, VLANs - network configuration with routing and router capability	no additional requirements	no additional requirements
		Non-Network Component Requirement Not Accept: - component opens or requires network connections that make a network segmentation non-feasible or hard to maintain		

CR 5.2	Zone boundary protection	Network Component Requirement Accept: - capability to monitor and control communication at zone boundaries to enforce compartmentalization defined in risk-based zones and conduits model Not accept: - demonstrate insufficient boundary protection	Accept: - capability to deny network traffic by default - allow network traffic by exception	Accept: - capability to prevent any communication through the control system boundary (island mode) - provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (fail close)
CR 5.3	General purpose person-to-person communication restrictions	Accept: - capability to prevent general purpose, person-to-person messages from being received from users/systems to the control system (email, all forms of social media, message systems) - e.g. filtering traffic with packet filters or application-level gateways Not accepted: - no/insufficient traffic inspection	no additional requirements	no additional requirements

Tabelle 10

6.7 FR-6: Timely Response To Events

ID	Requirement	SL-1	SL-2	SL-3
CR 6.1	Audit log accessibility	Accept: - capability for authorized humans or tools to access audit logs on a read only basis - web interface (audit perspective) - console tools (separate information system for audit access) Not accepted: - audit logs are accessible to unauthorized users	no additional requirements	Accept: - programmatic access to audit records by either using an application programming interface (API), or - capability to send the audit logs to a centralized system
CR 6.2	Continuous monitoring	no requirements	Accept: - capability to provide an active interface for continuous monitoring, or - capability to send continuous monitoring information to a centralized system	no additional requirements

Tabelle 11

6.8 FR-7: Resource Availability

ID	Requirement	SL-1	SL-2	SL-3
CR 7.1	Denial of service protection	Accept: - capability to operate in a degraded mode (essential functions) during a DoS event	Accept: - Manage communication load from application or device to mitigate effects of DoS events - e.g. limit network capacity of interfaces	no additional requirements