CR 7.2	Resource management	Accept: - capability to limit the use of resources by (active running) security functions to prevent resource exhaustion - e.g. software process prioritization, network traffic rate limiting	no additional requirements	no additional requirements
CR 7.3	Control system backup	Accept: - shall provide backup abilities to safeguard application/device state (user- and system-level information) - Backup Process does not affect normal operation Not accept: - no / insufficient backup abilities - normal operation is affected by control system backup	Accept: - capability to verify the reliability of backup mechanism - e.g. verify backup data mechanism, integrity of backed up information is validated prior to restoring it	no additional requirements
CR 7.4	Control system recovery and reconstitution	Accept: - capability to recovery and reconstitute to a known secure state after disruption or failure - system parameters (either default or configurable) are set to secure values - security-critical patches are reinstalled - security-related configuration settings are re-established - system documentation and operating procedures are available - components are reinstalled and configured with established set-	no additional requirements	no additional requirements

		tings - recovery uses a backup selected explicitly by an authorized person or the recovery uses an internal authentic backup source		
CR 7.5	Emergency power	no requirements	no additional requirements	no additional requirements
CR 7.6	Network and security configuration settings	Accept: - network and security configurations can be configured (as described in guidelines provided by the control system supplier) - component provides an interface to the deployed network and security configuration settings Not accept: - missing related guideline - insufficient description of configurations	no additional requirements	Accept: - capability to generate a report listing the currently deployed security settings in a machine-readable format
CR 7.7	Least functionality	Accept: - capability to restrict the use of unnecessary functions, ports, protocols and/or services (security-by-configuration) - functions beyond a baseline configuration should be able to be deactivated	no additional requirements	no additional requirements
CR 7.8	Control system component inventory	no requirements	Accept: - capability to support a control system component inventory - e.g. vendor-specific management-system or standard-based inventory systems (e.g. with SNMP support) - capable to monitor device ID and status	no additional requirements

Tabelle 12

7 Anhang D (informativ) – Methoden zur Schwachstellenbewertung

7.1 Einführung

Der Prüfschritt der Schwachstellenanalyse bedingt die Bewertung von möglichen Angriffen hinsichtlich der gewählten SL-Stufe (im Sinne Angriffsresistenz). Das zu nutzende Bewertungsmodell wird nicht im vorliegenden Prüfschema fest vorgegeben. Die Anforderungen an das Bewertungsmodell sind in Kapitel 2.6 zu finden.

Nachfolgend wird das Bewertungsmodell nach [CEM] Methodik eingeführt, dieses erfüllt alle definierten Anforderungen an ein Bewertungsmodell für die Schwachstellenanalyse.

7.2 AVA/CEM Bewertung

Als Bewertungsmodell hat sich die „Vulnerability Assessment (AVA)“ Methodik aus der Common Evaluation Methodology [CEM] oder ISO/IEC 18045 [ISO18045] bewährt. Für die Nutzung im Zusammenhang mit der IEC 62443 muss eine adaptierte Variante genutzt werden, um die definierten SL-Stufen nutzen zu können. Diese adaptierte Variante wird im Folgenden beschrieben.

Die Methode hat nicht das Ziel Schwachstellen oder Angriffe zu identifizieren. Die Methode dient nur dazu skizzierbare Angriffspfade zu bewerten.

Um die Methodik auf die IEC 62443 anwenden zu können, müssen die SL-Stufen auf die nummerischen Werte der [CEM] definiert werden. Dies erfolgt in der folgenden Tabelle:

SL-Stufe	**Schwelle für ausreichende Resistenz**	**Kommentar**
SL-1	> 0	angenommenes Angriffspotential betrifft nur nicht gezielte Angriffe; umgekehrt bedeutet dies, dass damit gefundene Schwachstellen gegen eine explizite Anforderung (CR) verstoßen müssen, um im Rahmen einer Prüfung nach SL-1 bewertet zu werden
SL-2	> 4	geringes Angriffspotential bedeutet im Wesentlichen der zeitliche Faktor ist ausschlaggebend, als Schwelle wird hier weniger als 1 Monat Angriffszeit angenommen, zusammen für Entwicklung und Durchführung, ein Monat wird mit 4 Punkten bewertet, siehe [CEM] Anhang B
SL-3	> 14	das angenommene mittlere Angriffspotential ergibt eine Mindestsumme von 14 Punkten, dies bedingt sich durch eine Angriffszeit von zwei Monaten (7 Punkte), entweder weitergehender Expertise (3 Punkte) oder Zugriff auf restriktive Daten (ebenfalls 3 Punkte) sowie spezialisiertes Equipment (4 Punkte), hiermit ergeben sich in Summe 14 Punkte, siehe [CEM] Anhang B
SL-4	-	nicht relevant für Prüfschema in dieser Version

Tabelle 5

Folgende Eigenschaften werden zur Bewertung eines kompletten Angriffs zugrunde gelegt:

- Zeitbedarf (sowohl zur Entwicklung des Angriffs sowie zur Durchführung)
- Expertise
- Wissen über die Komponente
- Möglichkeit (window of opportunity)
- Ausstattung

Die Spalte "Schwelle für ausreichende Resistenz" ist so zu lesen, dass ein skizzierbarer Angriff oberhalb dieser Schwelle liegen MUSS, damit die Komponente in entsprechender SL-Stufe als ausreichend resistent bezeichnet werden kann.

Der Einstufung jeder einzelnen Bewertungseigenschaft werden Punkte zugeordnet, welche dann aufsummiert und mit einem Zielniveau abgeglichen werden. Die Definition der Punkte und die detaillierte Beschreibung finden sich im Anhang B der [CEM].

7.3 Beispiel einer Bewertung nach AVA/CEM

Als Beispiel sei folgendes Szenario angenommen. Die betrachtete Komponenten-Schnittstelle ist SSH (Secure Shell) mit einer Passwort-Authentifizierung, weiter wird mindestens ein 4-stelliges Passwort (ohne weitere Restriktionen) gewählt, eine Beschränkung der Anmeldeversuche existiert nicht. Auf Basis des Szenarios lässt sich ein Angriff skizzieren, indem mit einem SSH-Bruteforce-Tool versucht wird das Passwort einer Benutzerkennung zu raten. Ein solches Bruteforce-Tool ist beispielsweise Hydra. In einer LAN-Umgebung sind beispielsweise 180 SSH-Anmeldeversuche pro Minute möglich, entsprechende Werte könnten im Rahmen eines Labortests ermittelt werden.

Nimmt man weiter an, dass das zu ratende Passwort tatsächlich vier Stellen hat und aus großen und kleinen Buchstaben sowie Ziffern besteht, ergeben sich 62^4 mögliche Kennwörter. Mit oben genannter Brute-Force-Rate wäre der Angriff in unter 23 Stunden durchführbar. Hinzu kommt noch ein gewisser Aufwand zum Aufbau und Durchführung des Angriffs. Im Ergebnis wird damit ein Gesamtaufwand von etwas mehr als einem Tag angesetzt.

Werden die Eckdaten des Angriffs mit Hilfe der Kennzahlen aus der [CEM] abgeschätzt, ergibt sich folgende Tabelle:

Kategorie	**Begründung**	**Wert nach [CEM]**	**Punktzahl nach [CEM]**
Zeitbedarf	mehr als 1 Tag, weniger als eine Woche	<= one week	1
Expertise	Angriffswerkzeug ist mit vielen Beispielen öffentlich dokumentiert	Layman	0
Wissen über die Komponente	SSH ist ein per RFC dokumentiertes Protokoll und ein offener Port kann über einen Netzwerk-Portscan gefunden werden	Public	0
Möglichkeit (window of opportunity)	dies hängt stark vom Verwendungszweck ab, falls keine Restriktionen definiert sind, dann sind diese unbegrenzt	Unnecessary/unlimited access	0
Ausstattung	das Tool Hydra ist öffentlich und leicht zugänglich verfügbar	Standard	0

Tabelle 6

Daraus ergibt sich eine Gesamtzahl von 1 Punkt. In diesem Beispiel wäre die Resistenz der Komponente also nicht ausreichend, um sich für SL-2 zu qualifizieren, d.h. die Schwachstellenanalyse hätte an dieser Stelle ein negatives Prüfergebnis.

8 Anhang E (informativ) – Übersicht zur Nutzung der Ergebnisse des IEC 62443-4-1 Entwicklungsprozesses

Practice 1	**Security Management**	**Nutzung im Prüfschema**
SM-1	Development Process	keine[1]
SM-2	Identification of repsonsibilities	keine
SM-3	Identification of applicability	keine
SM-4	Security expertise	keine
SM-5	Process scoping	keine
SM-6	File integrity	Prüfung Design-Dokumentation, siehe 2.3
SM-7	Development environment security	keine
SM-8	Controls for private keys	keine
SM-9	Security requirements for externally provided components	Prüfung Design-Dokumentation, siehe 2.3
SM-10	Custom development components from third-party suppliers	Prüfung Design-Dokumentation, siehe 2.3
SM-11	Assessing and addressing security-related issues	keine
SM-12	Process Verification	keine
SM-13	Continuous improvement	keine
Practice 2	**Specification of security requirements**	
SR-1	Product security context	Prüfung des Verwendungszwecks, siehe 2.2
SR-2	Threat model	Prüfung des Verwendungszwecks, siehe 2.2 Schwachstellenanalyse, siehe 2.6
SR-3	Product security requirements	Konformitätsbewertung, siehe 2.5
SR-4	Product security requirements content	Prüfung des Verwendungszwecks, siehe 2.2
SR-5	Security requirements review	Konformitätsbewertung, siehe 2.5, Rolle Tester
Practice 3	**Secure by design**	
SD-1	Secure design principles	Umgesetzte Security Eigenschaften an Schnittstellen, betrifft Prüfung De-

[1] *keine Nutzung im Prüfschema* ist so zu lesen, dass keine direkten Ergebnisse (deliverables) im Produkt oder den Design-Dokumenten ablesbar sind.

		sign-Dokumentation, siehe 2.3
SD-2	Defense in depth design	Schwachstellenanalyse, siehe 2.6
SD-3	Security design review	Umgesetzte Security Eigenschaften (Details ab SL-3 gefordert), betrifft Prüfung Design-Dokumentation, siehe 2.3
SD-4	Secure design best practices	Umgesetzte Security Eigenschaften (Details ab SL-3 gefordert), betrifft Prüfung Design-Dokumentation, siehe 2.3
Practice 4	**Secure implementation**	
SI-1	Security implementation review	keine
SI-2	Secure coding standards	keine
Practice 5	**Security verification and validation testing**	
SVV-1	Security requirements testing	Konformitätsbewertung, siehe 2.5
SVV-2	Threat mitigation testing	Schwachstellenanalyse, siehe 2.6
SVV-3	Vulnerability testing	Schwachstellenanalyse, siehe 2.6
SVV-4	Penetration testing	Schwachstellenanalyse, siehe 2.6
SVV-5	Independence of testers	Schwachstellenanalyse, siehe 2.6 Konformitätsbewertung, siehe 3.1
Practice 6	**Management of security-related-issues**	
DM-1	Receiving notifications of security-related issues	keine
DM-2	Reviewing security related issues	keine
DM-3	Assessing security-related issues	keine
DM-4	Adressing security-related issues	keine
DM-5	Disclosing in security-related issues	keine
DM-6	Periodic review of security defect management practice	keine
Practice 7	**Security update management**	
SUM-1	Security update qualification	keine
SUM-2	Security update documentation	Prüfung Dokumentation (Anwender), siehe 2.4
SUM-3	Dependent component or operating system security update documentation	Prüfung Dokumentation (Anwender), siehe 2.4
SUM-4	Security update delivery	keine
SUM-5	Timely delivery of security patches	keine

Practice 8	**Security guidelines**	
SG-1	Product defense in depth	Prüfung Dokumentation (Anwender), siehe 2.4
SG-2	Defense in depth measures expected in the environment	Prüfung Dokumentation (Anwender), siehe 2.4
SG-3	Security hardening guidelines	Prüfung Dokumentation (Anwender), siehe 2.4
SG-4	Secure disposal guidelines	Prüfung Dokumentation (Anwender), siehe 2.4
SG-5	Secure operation guidelines	Prüfung Dokumentation (Anwender), siehe 2.4
SG-6	Account management guidelines	Prüfung Dokumentation (Anwender), siehe 2.4
SG-7	Documentation review	Prüfung Dokumentation (Anwender), siehe 2.4

9 Anhang F (informativ) – Übersicht der Ergänzungen zur Norm

Zielsetzung des Prüfschemas ist es, dass langfristig keine zusätzlichen Anforderungen als in der selbst Norm definiert gefordert werden.

Da aus Sicht der Prüfung bezogen auf den aktuellen Stand der Normteile IEC 62443-4-2 und IEC 62443-4-1 noch weitere Details benötigt werden, um vergleichbare Prüfungen durchführen zu können, werden in diesem Dokument teilweise präzisierte Anforderungen definiert. Diese Ergänzungen werden an dieser Stelle aufgelistet:

- Komponentenspezifikation entsprechend Anhang A
- Akzeptanzkriterien entsprechend Anhang C
    - geänderte Akzeptenzkriterien im Vergleich zu CR des Normteils IEC 62443-4-2:
        - CR 3.5: Komplexität der referenzierten Verfahren SL-Stufen zugeordnet
        - CR 4.1: Ansteignde Mechanismenstärke der eingesetzten Verfahren aufgrund SL-Stufe (im Sinne Angriffsresistenz)
        - CR 5.1: Unterscheidung zwischen Network Component und anderen Komponententypen
- Forderung einer je SL-Stufe (im Sinne Angriffsresistenz) angemessenen Umsetzung von Anforderungen (CR), welche denen keine gestuften Anforderung (RE, Requirement Enhancements) definiert sind (beispielsweise CR 4.1), siehe Kapitel 2.3

10 Abkürzungsverzeichnis

Abkürzung	Bedeutung
CVSS	Common Vulnerability Scoring System
EDR	Embedded Device Requirement
DM	Defect management (Abkürzung aus IEC 62443-4-1)
PKI	Public Key Infrastructure
SD	Security by design (Abkürzung aus IEC 62443-4-1)
SG	Security guidelines Abkürzung aus IEC 62443-4-1)
SI	Security Implementation (Abkürzung aus IEC 62443-4-1)
SM	Security management (Abkürzung aus IEC 62443-4-1)
SR	Security requirements (Abkürzung aus IEC 62443-4-1)
SUM	Security update management (Abkürzung aus IEC 62443-4-1)
SVV	Security verification and validation testing (Abkürzung aus IEC 62443-4-1)

11 Literaturverzeichnis

[IEC62442-3-3] IEC 62443-3-3:2013

[IEC62442-4-1] IEC 62443-4-1:2018

[IEC62442-4-2] IEC 62443-4-2:2019

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, April 2017, Version 3.1, Revision 5, CCMB-2017-04-004

[Dakks] Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443, 71 SD 2 019, Revision: 1.0, 05.03.2018

[ISO18045] ISO/IEC 18045:2008, Information technology - Security techniques - Methodology for IT security evaluation, 2014-01, Edition 2

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.