Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anwendungshinweise und Interpretationen zum Schema (AIS)

AIS B6, Version 2.0

Datum:	01.03.2024
Status:	Verbindlich
Thema:	Anforderungen an einen TOE
Herausgeber:	Zertifizierungsstelle des BSI
Verteiler:	Anerkannte BSZ-Prüfstellen (ITSEFs)[1] BSI-intern Webseite des BSI

[1]Alle Evaluatoren in den vom BSI für Prüfungen im Rahmen der BSZ anerkannten Prüfstellen.

Änderungshistorie

Version	*Datum*	*Herausgeber*	*Beschreibung*
2.0	01.03.2024	SZ 33	Deutsche Erstausgabe

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0)800 247 1000
E-Mail: bsz@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Hintergrund 4
2 Spezifische Referenzen 5
3 Anwendungshinweise und Interpretationen 6
3.1 Authentifizierung und Autorisierung 6
3.2 Protokollierung 6
3.3 Dienste 7
3.4 Unterlagen 8
3.5 Zusätzliche Anforderungen für Softwareanwendungen und Anwendungen in virtualisierten Umgebungen 8
4 Definitionen 10
5 Referenzdokumente 13

1 Hintergrund

1 Dieses Dokument definiert Anforderungen, die jeder Evaluierungsgegenstand (Englisch: Target of Evaluation, TOE) für die BSZ erfüllen muss. Die Anforderungen basieren auf internationalen Normen, insbesondere Teil 4-2 von IEC 62443 zur Cybersicherheit in industriellen Kommunikationsnetzen [62443].

2 Abschnitte der Dokumente, die die Konformität mit den einzelnen Anforderungen dieses AIS-Dokuments belegen, müssen in tabellarischer Form aufgebaut sein.

2 Spezifische Referenzen

1 [BSZ-Prod] Produktzertifizierung: Programm Beschleunigte Sicherheitszertifizierung (BSZ), BSZ-Produkte, BSI

2 [BSZ-Prüf] Anerkennung von Prüfstellen: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ), BSZ-Prüfstellen, BSI

3 [BSZ-EP] Programm [BSZ-Prüfstellen]: BSZ-Evaluierungsprozess, BSZ-EP, BSI

4 [AIS B1] Anforderungen an ST und IAR, BSI

5 [AIS B2] Anforderungen an die Evaluierung kryptographischer Mechanismen gemäß BSZ, BSI

6 [AIS B3] Anforderungen an die Benutzeranleitung, BSI

7 [AIS B4] Anforderungen an die Evaluierung gemäß BSZ, BSI

8 [AIS B5] Anleitung zur Bestimmung des Aufwands für eine BSZ-Evaluierung, BSI

9 [BSZ-ETR] BSZ – Vorlage für den Evaluierungsreport, BSI

10 [BSZ-ADA] BSZ – Agenda der Auftaktbesprechung, BSI

3 Anwendungshinweise und Interpretationen

3.1 Authentifizierung und Autorisierung

3 Der TOE muss die Nutzerin oder den Nutzer an der jeweiligen Schnittstelle identifizieren und authentifizieren, bevor sie oder er auf die Dienste zugreifen kann.
Hinweis 1: Eine anonyme Nutzung kann ggf. möglich sein, wenn ein Kompromittieren des TOE ausgeschlossen ist und kritische Konfigurationen nicht abgeändert werden können.
Hinweis 2: Im Dokument Sicherheitsvorgaben (Englisch: Security Target, ST) werden die Nutzerinnen und Nutzer des TOE den Werten zugeordnet, auf die sie Zugriff haben, und ihrer jeweiligen Zugriffsart. Es muss sichergestellt sein, dass die Nutzerinnen und Nutzer erst nach erfolgreicher Authentifizierung auf entsprechende Werte zugreifen können.

4 Der TOE muss sich selbst eindeutig identifizieren und sich selbst gegenüber der Nutzerin oder dem Nutzer authentisieren können.

5 Der TOE darf keine festcodierten Passwörter, kryptographischen Schlüssel oder andere Anmeldeinformationen enthalten, die von mehreren Produkten gemeinsam genutzt werden.

6 Der TOE sollte die Verwaltung aller vorhandenen Nutzerkonten ermöglichen.
Hinweis: Die Nutzerverwaltung kann lokale oder zentrale Dienste nutzen, z. B. LDAP.

7 Der TOE muss den Nutzerinnen und Nutzern die Möglichkeit bieten, ihre eigenen lokalen Authentifizierungsdaten (z. B. Passwörter und Nutzernamen) zu ändern und vor unbefugtem Zugriff zu schützen.

8 Der TOE prüft bei der Erstellung oder Änderung der Authentifizierungsdaten ihre ausreichende Komplexität und Sicherheit. Die erforderliche konfigurierbare Stärke sollte sich an anerkannten Sicherheitsrichtlinien orientieren.

9 Der TOE darf als Reaktion auf eine Authentifizierung keine sicherheitsrelevanten Informationen preisgeben oder Rückschlüsse auf diese zulassen.

10 Der TOE muss die Anzahl der Authentifizierungsversuche einschränken, um Brute-Force-Angriffe zu verhindern.

11 Der TOE sollte für den Zugriff auf Dateien und Dienste eine Rollenverwaltung bereitstellen. Zugriffsrechte müssen restriktiv vergeben werden; dies gilt auch für die Standardkonfiguration.
Hinweis 1: Eine Rollenverwaltung ist nur dann erforderlich, wenn im TOE-Kontext eine Funktion bereitgestellt wird.
Hinweis 2: In der Standardkonfiguration darf nur die Rolle des Administrators mit vollständigen Berechtigungen verfügbar sein.

12 Der TOE muss nach einer definierten Inaktivitätsdauer oder nach einem festgelegten Zeitraum eine erneute Authentifizierung anfordern.

3.2 Protokollierung

13 Der TOE muss mindestens die folgenden Ereignisse protokollieren:

- Fehlerhafte Authentifizierung
- Datensicherung und Wiederherstellung
- Konfigurationsänderungen

14 Für die oben genannten Ereignisse muss der TOE folgende Informationen speichern:

- Zeitstempel

- Ereignistyp
- Ergebnis der Aktion, die das Ereignis ausgelöst hat

15 Der TOE muss für Ereignisprotokolle über einen ausreichenden lokalen Speicher verfügen.
Hinweis: Die Ereignisprotokollierung ist nicht auf den lokalen Speicher beschränkt. Informationen können auch an andere Systeme übertragen werden. Allerdings muss auf dem TOE ausreichend Speicher zur Zwischenspeicherung vorhanden sein, um mögliche Ausfälle in der Verbindung zu einer zentralen Instanz zu kompensieren.

16 Der TOE muss einen sicheren Zustand aufrechterhalten, wenn nicht ausreichend Speicherplatz verfügbar ist.

17 Der TOE darf nur autorisierten Nutzerinnen und Nutzern den Zugriff auf die Protokolldateien gestatten.
Hinweis: Gilt nur für die lokale Speicherung. Bei externer Speicherung muss im Handbuch eine Beschreibung zur Einrichtung der externen Speicherung enthalten.

3.3 Dienste

18 Der TOE muss robust auf falsche oder fehlerhafte Daten seiner Dienste reagieren. Der TOE darf zu keiner Zeit einen undefinierten Zustand erreichen.

19 Der TOE muss die Integrität, Authentizität und Vertraulichkeit der übermittelten Daten entsprechend dem Schutzbedarf schützen.
Hinweis 1: Welche übertragenen Daten schutzwürdig sind, hängt von den Sicherheitsfunktionen ab.
Hinweis 2: In Fällen, in denen die resultierenden Daten nicht vertraulich sind, können Schutzmaßnahmen ausschließlich auf die Integrität ausgerichtet sein.

20 Um eine fehlerhafte Verarbeitung zu vermeiden, muss der TOE die Ein- und Ausgabe vor der Verarbeitung validieren.
Hinweis: Die Ein- und Ausgabedaten des TOE selbst oder externer Schnittstellen müssen auf Syntax, Länge und Inhalt überprüft werden.

21 Der TOE muss mit Fehlern in angemessener Weise umgehen.

22 Der TOE darf keine kritischen Informationen in Fehlermeldungen preisgeben.
Hinweis: Fehlermeldungen dürfen keine für potenzielle Angreifer relevanten Informationen enthalten. Protokolldateien dürfen keine Authentifizierungsdaten enthalten.

23 Der TOE muss das Zurücksetzen auf die Werkseinstellungen ermöglichen. Für diesen Zweck muss der TOE eine Funktion zur sicheren und zuverlässigen Löschung aller nutzerspezifischen Daten zur Verfügung stellen.
Hinweis 1: Auch diese Funktion kann sicherheitskritisch sein und sollte entsprechend gesichert werden.
Hinweis 2: Bitte geben Sie eine kurze technische Beschreibung der Methode zum Löschen von Daten an.

24 Der TOE sollte in der Standardkonfiguration kryptographische Operationen gemäß den Anforderungen des Dokuments [AIS B2] unterstützen.

25 Der TOE muss die Sicherung und Wiederherstellung der aktuellen Konfiguration ermöglichen.

26 In der Standardkonfiguration sollten im TOE nur Dienste aktiviert sein, die zur Ausführung grundlegender Funktionen erforderlich sind. Nutzerinnen und Nutzer müssen die Möglichkeit haben, nicht benötigte Dienste zu deaktivieren. Nicht benötigte Dienste müssen eine Möglichkeit zur Deaktivierung durch die Nutzerin oder den Nutzer bieten.
Hinweis 1: In der Standardkonfiguration sollten möglichst wenige Dienste aktiv sein, um die Angriffsfläche gemäß dem Prinzip „Security-by-Design“ zu minimieren.
Hinweis 2: Die Grundfunktionalität wird durch die in der TOE-Zertifizierung enthaltenen Funktionen

definiert.
Hinweis 3: Die Standardkonfiguration sollte nur Funktionen bereitstellen, die für den Hauptzweck unerlässlich sind. Zusatzfunktionen sind beispielsweise Komfortfunktionen, die nur bedingt benötigt werden.

27 Auf dem TOE dürfen nur Dienste und Software vorhanden sein, die zur Bereitstellung der Funktionen des TOE erforderlich sind. Entwicklungsinformationen müssen entfernt werden.

28 Der TOE muss nach der Installation die Möglichkeit für Updates bieten.

29 Der TOE muss vor der Installation die Authentizität und Integrität der Update-Dateien bestätigen.
Hinweis: Sicherheitsupdates dienen der Beseitigung von Mängeln und Fehlern, die für den sicheren Betrieb des TOE von kritischer Bedeutung sind.

30 Der Zugang zu drahtlosen Netzwerken muss gesichert sein. Sofern dies unterstützt wird, sollte der TOE den Zugriff auf drahtlose Netzwerke mithilfe der Zugangskontrolle des Systems integrieren.

3.4 Unterlagen

31 Die Antragstellerin muss Anleitungsunterlagen vorlegen, in denen die sichere Nutzung des TOE beschrieben wird. Dies umfasst die Installation und Konfiguration, den Betrieb und die Außerbetriebnahme des TOE.
Darüber hinaus müssen der Verwendungszweck und die Betriebsumgebung beschrieben werden.
Hinweis: Diese Dokumentationsunterlagen beschränken sich nicht auf das Handbuch zur sicheren Benutzung und umfassen die gesamte Benutzerdokumentation für das Produkt.

32 Die Antragstellerin muss die folgenden in der Standardkonfiguration vorhandenen Funktionen dokumentieren:

- TOE-Schnittstellen
- Nutzerinnen und Nutzer
- Rollen
- Dienste und zugehörige Funktionen
- Aktivierungs- und Deaktivierungsstatus für die Dienste

Hinweis: Der Status der Funktionen muss in den Dokumentationsunterlagen nicht angegeben werden. Dienstspezifische Informationen können auch über einen bestimmten Dienst im TOE bereitgestellt werden.

33 Die Antragstellerin muss Empfehlungen für den sicheren Betrieb des TOE bereitstellen.
Hinweis 1: Empfehlungen können in die Dokumentationsunterlagen aufgenommen oder über einen dafür vorgesehenen Dienst des TOE (z. B. durch Einblendung während der Konfiguration) bereitgestellt werden.
Hinweis 2: In den Dokumentationsunterlagen oder Konfigurationsempfehlungen müssen Hinweise auf mögliche Sicherheitsprobleme oder Auswirkungen enthalten sein.

3.5 Zusätzliche Anforderungen für Softwareanwendungen und Anwendungen in virtualisierten Umgebungen

34 Die Hardwarespezifikation muss alle Angaben zur Hardware enthalten, die notwendig sind, damit der TOE seine Sicherheitsfunktion in der beschriebenen Hardwareumgebung erbringen kann. Diese Angaben müssen spezifische Anforderungen an die Hardwarearchitektur, Netzwerkressourcen und System- und Speicheranforderungen enthalten, sind aber nicht darauf begrenzt. Anforderungen für das System und den Speicher müssen durch Mindest- und gegebenenfalls Maximalanforderungen für erforderliche Ressourcen ergänzt werden. Für Anwendungen in

virtualisierten Umgebungen muss die Information auch virtuelle Hardwarekomponenten und virtuell genutzte Ressourcen abdecken. Wenn die Anwendung die Verwendung spezieller Hardware in der Systemumgebung erfordert, muss die Hardware spezifiziert und die Verwendung beschrieben werden.
Hinweis: Die Informationen in der Hardwarespezifikation müssen spezifisch genug sein, damit eine repräsentative Testumgebung von der Prüfstelle für die Evaluierung der Anwendung ausgewählt werden kann.

35 Eine Kompatibilitätsbeschreibung ist zusätzlich zur Hardware-Spezifikation erforderlich, wenn der TOE auf divergenter Hardware wie unterschiedlichen Systemarchitekturen oder deutlich verschiedenen Varianten von Hardware eingesetzt werden soll. Die Kompatibilitätsbeschreibung dient als Grundlage für die Beurteilung, ob der TOE seine Sicherheit in den angegebenen Bedingungen der Systemumgebung erfüllen kann oder nicht. Die Beschreibung muss die unterschiedliche Ausführung der Hardwarekomponente beinhalten, ob sie auf unterschiedliche Schnittstellen reagiert und wie sich das Verhalten der Hardwarekomponenten unterscheidet.
Hinweis: Es wird dringend empfohlen, die für die Zertifizierung in Betracht gezogene Hardware oder virtualisierten Umgebungen auf eine Anzahl zu begrenzen, die tatsächlich innerhalb des erlaubten Evaluierungszeitraums der BSZ effektiv bewertet werden kann. Die tatsächlich zulässige Anzahl hängt unter anderem von der Anzahl, Komplexität und Vielfalt der zu berücksichtigenden Umgebungen ab.

36 Die Softwarespezifikation muss das verwendete Betriebssystem sowie zusätzliche Software angeben, die aufgrund von Abhängigkeiten für die Ausführung der Anwendung erforderlich ist. Dies muss durch minimale und gegebenenfalls maximale Versionsnummern der verwendeten Software oder des Betriebssystems ergänzt werden.
Hinweis: Die Informationen für die Software können auch mittels Veröffentlichungsdaten gestaltet werden. In diesem Fall muss angegeben werden, welche Softwareversionen den sicheren Betrieb der Anwendung gewährleisten.

37 Die angegebene Software in der Softwarespezifikation muss während der erwarteten Gültigkeitsdauer des Zertifikats mit Softwaresicherheitsupdates versehen werden.

38 Die Abhängigkeiten des TOE von der Systemumgebung in Form von Softwarepaketen, Schnittstellen, Bibliotheken, Verknüpfungen zu Datenbanken, APIs oder anderen müssen angegeben werden. Alle erforderlichen Abhängigkeiten müssen ausreichend spezifiziert sein, damit Betreiber entscheiden können, welche Anforderungen an Hardware und Software für den sicheren Betrieb des TOE zu verwenden sind.
Hinweis 1: Die verwendeten Softwarepakete können als Liste angegeben werden. Alle anderen Abhängigkeiten erfordern eine Beschreibung.
Hinweis 2: Abhängigkeiten können auch Kommunikationskanäle wie E-Mails, eingebettete Formulare oder die Benutzeroberfläche sowie Anwendungsnavigation umfassen.
Hinweis 3: Listen von Softwarepaketabhängigkeiten können mithilfe von Paketverwaltungswerkzeuge erstellt werden.

39 Der TOE muss den Abruf von Ereignisprotokollen mittels programmierter Zugriffe ermöglichen. Autorisierte menschliche Nutzerinnen und Nutzer sollten ebenfalls Lesezugriff auf Ereignisprotokolle haben. Programmierter Zugriff kann über eine API erfolgen oder indem sie an ein zentrales System gesendet werden.

40 Wenn Rauschquellen verwendet werden, z. B. Zufallszahlengeneratoren, muss dies wie im Dokument [AIS B2], Abschnitt „Rauschquellenbeschreibung“, beschrieben werden.
Hinweis: Es gibt eine BSI-Studie zur Verwendung von Zufallszahlengeneratoren in virtualisierten Umgebungen, siehe Link [RNG].

4 Definitionen

Die folgenden Definitionen sind sinngemäße Übersetzungen der englischsprachigen Definitionen aus IEC 62443 Teil 1-1 [62443-1-1]:

Angriff (Attack)
Angriff auf ein System, der von einer intelligenten Bedrohung ausgeht – d. h. eine intelligente Handlung, die ein bewusster Versuch (insbesondere im Sinne einer Methode oder Technik) ist, Sicherheitsdienste zu umgehen und die Sicherheitsrichtlinie eines Systems zu verletzen.
Hinweis: Es gibt verschiedene allgemein anerkannte Angriffsklassen:

- *Ein "aktiver Angriff" versucht, Systemressourcen zu verändern oder ihren Betrieb zu beeinträchtigen.*
- *Ein "passiver Angriff" versucht, Informationen aus dem System zu erlernen oder zu nutzen, beeinträchtigt jedoch nicht die Systemressourcen.*
- *Ein "interner Angriff" ist ein Angriff, der von einer Entität innerhalb des Sicherheitsumfangs (ein "Insider") initiiert wird – d. h. eine Entität, die berechtigt ist, auf Systemressourcen zuzugreifen, diese jedoch auf eine Weise nutzt, die von denjenigen, die die Autorisierung erteilt haben, nicht genehmigt ist.*
- *Ein "externer Angriff" wird von außerhalb des Sicherheitsumfangs von einem nicht autorisierten oder unerlaubten Benutzer des Systems (einschließlich eines Insiders, der von außerhalb des Sicherheitsperimeters angreift) initiiert. Mögliche externe Angreifer reichen von Amateur-Scherzbolden (amateur prankster) über organisierte Kriminelle bis zu internationalen Terroristen und feindseligen Regierungen.*

Authentifizieren (authenticate)
Überprüfung der Identität einer Benutzerin oder eines Benutzers, eines Benutzergeräts oder einer anderen Entität, oder der Integrität von gespeicherten, übertragenen oder anderweitig einer unbefugten Änderung ausgesetzten Daten in einem Informationssystem oder Feststellung der Gültigkeit einer Übertragung.

Authentifizierung (authentication)
Sicherheitsmaßnahme, die entwickelt wurde, um die Echtheit einer Übertragung, einer Nachricht oder des Absenders festzustellen, oder ein Mittel zur Überprüfung der Autorisierung einer Person, bestimmte Kategorien von Informationen zu erhalten.

Autorisierung (authorization)
Recht oder Berechtigung, das einer Systementität gewährt wird, um auf eine Systemressource zuzugreifen.

Benutzer (user)
Person, Organisationsentität oder automatisierter Prozess (Dienst), der auf ein System zugreift, ob er dazu autorisiert ist oder nicht.

Cybersicherheit (cybersecurity)
Erforderliche Maßnahmen, um die unbefugte Nutzung, die Dienstverweigerung, die Änderung, die Offenlegung, den Ertragsverlust oder die Zerstörung kritischer Systeme oder Informationsschätze zu verhindern.

Datenintegrität (data integrity)
Eigenschaft, dass Daten nicht unbefugt oder versehentlich verändert, zerstört oder verloren gegangen sind.

Datenschutz (data confidentiality)
Eigenschaft, dass Informationen keiner unbefugten Systementität zur Verfügung gestellt oder offengelegt werden, einschließlich unbefugter Personen, Entitäten oder Prozesse.

Dienst (service)
Bietet verschiedene Funktionen über eine Schnittstelle. Dies kann zum Beispiel ein Webserver mit entsprechender Webanwendung zur Konfiguration sein.

Dienstverweigerung (denial of service)
Verhinderung oder Unterbrechung des autorisierten Zugriffs auf eine Systemressource oder Verzögerung von Systemoperationen und -funktionen.

Digitale Signatur (digital signature)
Ergebnis einer kryptografischen Transformation von Daten, das bei ordnungsgemäßer Implementierung die Dienste der Ursprungsauthentifizierung, der Datenintegrität und der Nichtabstreitbarkeit des Unterzeichners bietet.

Integrität (integrity)
Qualität eines Systems, die die logische Korrektheit und Zuverlässigkeit des Betriebssystems, die logische Vollständigkeit der Hardware und Software, die die Schutzmechanismen implementieren, und die Konsistenz der Datenstrukturen und des Auftretens der gespeicherten Daten widerspiegelt.

Kryptografischer Algorithmus/Operation (cryptographic algorithm/operation)
Algorithmus, der auf der Wissenschaft der Kryptografie basiert, einschließlich Verschlüsselungsalgorithmen, kryptografischer Hash-Algorithmen, digitaler Signaturalgorithmen und Schlüsselvereinbarungsalgorithmen.

Kryptografischer Schlüssel (cryptographic key)
Eingabeparameter, der die Transformation beeinflusst, die von einem kryptografischen Algorithmus durchgeführt wird.

Schnittstelle (interface)
Physischer oder logischer Ein- oder Ausgangspunkt, der Zugang zum Modul für logische Informationsflüsse ermöglicht.

Sicherheit (security)
a. Getroffene Maßnahmen zum Schutz eines Systems.
b. Zustand eines Systems, der sich aus der Einrichtung und Aufrechterhaltung von Maßnahmen zum Schutz des Systems ergibt.
c. Zustand von Systemressourcen, die frei von unbefugtem Zugriff und von unbefugter oder unbeabsichtigter Änderung, Zerstörung oder Verlust sind.
d. Fähigkeit eines auf Computern basierenden Systems, ausreichendes Vertrauen zu bieten, dass nicht autorisierte Personen und Systeme weder die Software und ihre Daten verändern noch auf die Systemfunktionen zugreifen können und dass dies den autorisierten Personen und Systemen nicht verweigert wird.
e. Verhinderung des illegalen oder unerwünschten Eindringens oder der Beeinträchtigung des ordnungsgemäßen und beabsichtigten Betriebs eines Produkts.

Hinweis: Maßnahmen können sich auf physische Sicherheit (Kontrolle des physischen Zugangs zu Rechenanlagen) oder logische Sicherheit (Fähigkeit, sich bei einem bestimmten System und einer Anwendung anzumelden) beziehen.

Sicherheitsdienst (security service)
Mechanismen, die zur Vertraulichkeit, Datenintegrität, Authentifizierung oder Nichtabstreitbarkeit von Informationen verwendet werden.

Sicherheitsfunktionalität (security function)
Funktion einer Zone oder einer Verbindung, die unbefugte elektronische Eingriffe verhindert, die sich auf die normale Funktion von Geräten und Systemen innerhalb der Zone oder des Leitungssystems auswirken oder beeinflussen können.

Sicherheitsleistung / Sicherheitsumfang (security perimeter)
Grenze (logisch oder physisch) des Bereichs, auf den eine Sicherheitsrichtlinie oder Sicherheitsarchitektur anwendbar ist, d. h. die Grenze des Raums, in dem Sicherheitsdienste Systemressourcen schützen.

Sicherheitsrichtlinie (securtiy policy)
Satz von Regeln, die angeben oder regeln, wie ein System oder eine Organisation Sicherheitsdienste zum Schutz ihrer Vermögenswerte (Assets) bereitstellt.

Standardkonfiguration (default configuration)
Werkseinstellung des TOE. Alle Einstellungen sind auf vom Entwickler definierte Werte gesetzt und es gibt keine benutzerspezifischen Einstellungen. Nicht zu verwechseln mit der sicheren Konfiguration nach der Installation des TOE gemäß der Secure User Guidance [AIS B3].

System (system)
Miteinander interagierende, in Beziehung stehende oder voneinander abhängige Elemente, die ein komplexes Ganzes bilden.

Vertraulichkeit (confidentiality)
Gewährleistung, dass Informationen nicht an unbefugte Personen, Prozesse oder Geräte weitergegeben werden.

Wert (Asset)
Physisches oder logisches Objekt, das im Besitz einer Organisation ist oder unter der Verwahrungspflicht einer Organisation steht und entweder einen wahrgenommenen oder tatsächlichen Wert für die Organisation hat.

Zuverlässigkeit (reliability)
Fähigkeit eines Systems, unter festgelegten Bedingungen für einen bestimmten Zeitraum eine erforderliche Funktion auszuführen.

5 Referenzdokumente

1 [62443] IEC 62443 Industrial communication networks – Network and system security Part 4-2 Technical security requirements for IACS components Edition1.0 2019-02