DIN EN ISO/IEC 15408-1

ICS 35.030 Einsprüche bis 2020-02-06

Entwurf

Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit – Teil 1: Einführung und allgemeines Modell (ISO/IEC 15408-1:2009); Englische Fassung prEN ISO/IEC 15408-1:2019

Information technology –
Security techniques –
Evaluation criteria for IT security –
Part 1: Introduction and general model (ISO/IEC 15408-1:2009);
English version prEN ISO/IEC 15408-1:2019

Technologies de l'information –
Techniques de sécurité –
Critères d'évaluation pour la sécurité TI –
Partie 1: Introduction et modèle général (ISO/IEC 15408-1:2009);
Version anglaise prEN ISO/IEC 15408-1:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-12-06 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 94 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

Nationales Vorwort

Der Text von ISO/IEC 15408-1:2009 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 15408-1:2019 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Gremium ist der Arbeitskreis NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Dieses Dokument enthält unter Berücksichtigung des Präsidialbeschlusses 1/2004 nur die englische Originalfassung der ISO/IEC-Norm.

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

Nationaler Anhang NA
(informativ)

Begriffe

Die Benummerung der folgenden Begriffe und Abkürzungen sind identisch mit der Benummerung in der englischen Fassung.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ANMERKUNG Dieser Abschnitt enthält nur diejenigen Begriffe, die innerhalb von ISO/IEC 15408 in spezieller Weise verwendet werden. Manche Kombinationen von in ISO/IEC 15408 verwendeten allgemeinen Begriffen sind daher nicht in diesem Abschnitt enthalten, werden aber der Klarheit wegen in dem Zusammenhang erläutert, in dem sie verwendet werden.

3.1 In ISO/IEC 15408 verwendete Begriffe

3.1.1
nachteilige Aktionen
Aktionen, die von einem Bedrohungsagenten gegen ein Schutzobjekt durchgeführt werden

3.1.2
Schutzobjekte
Entitäten, von denen anzunehmen ist, dass sie für den Eigentümer des TOE einen Wert darstellen

3.1.3
Zuordnung
Spezifikation eines bezeichneten Parameters in einer Komponente (von ISO/IEC 15408) oder einer Anforderung

3.1.4
Sicherheit
Vertrauensgrundlage, dass ein TOE die SFRs einhält

3.1.5
Angriffspotential
Maß für den erforderlichen Aufwand bei einem Angriff auf ein TOE, ausgedrückt in Form von Fachkenntnis, Ressourcen und Motivation des Angreifers

3.1.6
Erweiterung
Hinzufügen von einer oder mehreren Anforderung(en) zu einem Paket

3.1.7
Authentisierungsdaten
Informationen, die zur Überprüfung der angegebenen Identität eines Benutzers verwendet werden

3.1.8
autorisierter Benutzer
TOE-Benutzer, der in Übereinstimmung mit den SFRs eine Funktion durchführen darf

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.1.9
Klasse
eine Reihe von ISO/IEC 15408-Familien mit einem gemeinsamen Fokus

3.1.10
kohärent
logisch geordnet und mit einer erkennbaren Bedeutung

ANMERKUNG Im Zusammenhang mit Dokumentation bezieht sich dies sowohl auf den eigentlichen Text als auch auf die Struktur des Dokuments hinsichtlich der Verständlichkeit für die Zielgruppe.

3.1.11
vollständig
Eigenschaft, die angibt, dass alle erforderlichen Teile einer Entität bereitgestellt wurden

ANMERKUNG In Bezug auf Dokumentation bedeutet dies, dass alle relevanten Informationen in der Dokumentation in einer solchen Detailliertheit beschrieben sind, dass auf der entsprechenden Abstraktionsebene keine weitere Erklärung erforderlich ist.

3.1.12
Komponente
kleinster selektierbarer Elementesatz, auf dem Anforderungen basieren können

3.1.13
zusammengesetztes Sicherheitspaket
CAP
(en: Composed Assurance Package)
Sicherheitspaket, bestehend aus Anforderungen, die auf ISO/IEC 15408-3 beruhen (vorwiegend auf der ACO-Klasse) und die einen Punkt der in ISO/IEC 15408 definierten zusammengesetzten Sicherheitsskala repräsentieren

3.1.14
bestätigen
erklären, dass etwas detailliert und mit einer unabhängig bestimmten Angemessenheit geprüft wurde

ANMERKUNG Die erforderliche Stringenz hängt von der Art der betrachteten Einheit ab. Dieser Begriff wird nur für Evaluatorenaktionen verwendet.

3.1.15
Konnektivität
Eigenschaft des TOE, die eine Interaktion mit IT-Entitäten außerhalb des TOE ermöglicht

ANMERKUNG Dies schließt den Datenaustausch über verdrahtete oder drahtlose Verbindungen, über beliebige Entfernungen und in allen Umgebungen und Konfigurationen ein.

3.1.16
widerspruchsfrei
Beziehung zwischen zwei oder mehreren Entitäten, bei der keine offensichtlichen Widersprüche zwischen diesen Entitäten auftreten

3.1.17
abwehren, Verb
einem Angriff entgegenwirken, wobei die Auswirkung einer bestimmten Bedrohung abgemildert, aber nicht notwendigerweise ausgemerzt wird

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.1.18
nachweisliche Konformität
Beziehung zwischen einem ST und einem PP, wobei das ST eine Lösung bereitstellt, welche das generische Sicherheitsproblem im PP löst

ANMERKUNG Das PP und das ST können völlig unterschiedliche Aussagen enthalten, die verschiedene Entitäten behandeln, verschiedene Konzepte verwenden usw. Die nachweisliche Konformität eignet sich auch für TOE-Typen, für die bereits mehrere ähnliche PPs existieren, so dass der ST-Autor auch die Konformität mit diesen PPs beanspruchen kann, um so Arbeit zu ersparen.

3.1.19
nachweisen
eine Schlussfolgerung liefern, die durch eine weniger strenge Analyse als einen „Beweis“ erlangt wurde

3.1.20
Abhängigkeit
Verhältnis zwischen Komponenten, bei dem gilt, dass wenn eine auf der abhängigen Komponente basierende Anforderung in einem PP, ST oder Paket enthalten ist, normalerweise auch eine Anforderung im PP, ST oder Paket enthalten sein muss, die auf der Komponente basiert, von der die Abhängigkeit besteht

3.1.21
beschreiben
spezifische Einzelheiten zu einer Entität bereitstellen

3.1.22
bestimmen
eine bestimmte Schlussfolgerung auf Basis einer unabhängigen Analyse bestätigen mit dem Ziel, eine bestimmte Schlussfolgerung zu erreichen

ANMERKUNG Die Verwendung dieses Begriffs setzt eine wirklich unabhängige Analyse voraus, in der Regel ohne dass eine vorhergehende Analyse durchgeführt wurde. Vergleiche die Begriffen „bestätigen“ oder „verifizieren“, welche voraussetzen, dass bereits eine Analyse durchgeführt wurde, welche überprüft werden muss.

3.1.23
Entwicklungsumgebung
Umgebung, in der das TOE entwickelt wird

3.1.24
Element
nicht unterteilbare Beschreibung einer Sicherheitsanforderung

3.1.25
sicherstellen
eine starke kausale Abhängigkeit zwischen einer Aktion und deren Auswirkungen garantieren

ANMERKUNG Wenn diesem Begriff das Wort „helfen“ vorangestellt ist, weist dies darauf hin, dass die Auswirkung aufgrund nur dieser Aktion nicht sicher garantiert ist.

3.1.26
Evaluierung
Bewertung eines PP, eines ST oder eines TOE auf Grundlage definierter Kriterien

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.1.27
Evaluierungssicherheitsniveau
EAL
(en: Evaluation Assurance Level)
Reihe von aus ISO/IEC 15408-3 entnommenen Sicherheitsanforderungen, die einem Punkt der in ISO/IEC 15408 definierten Sicherheitsskala entsprechen, welche ein Sicherheitspaket bilden

3.1.28
Evaluierungsinstanz
Institution, die für von Institutionen innerhalb einer bestimmten Gemeinschaft durchgeführte Evaluierungen die Anforderungen festlegt und die Qualität überwacht und die mittels eines Evaluierungsprogramms ISO/IEC 15408 für die jeweilige Gemeinschaft implementiert

3.1.29
Evaluierungsprogramm
administratives und regulatorisches Rahmenwerk, auf dessen Basis ISO/IEC 15408 innerhalb einer bestimmten Gemeinschaft durch eine Evaluierungsinstanz umgesetzt wird

3.1.30
erschöpfend
Merkmal eines methodischen Konzepts zur Durchführung einer Analyse oder Aktivität in Übereinstimmung mit einem eindeutigen Plan

ANMERKUNG Dieser Begriff wird in ISO/IEC 15408 bezüglich der Durchführung einer Analyse oder einer anderen Aktivität verwendet. Er ist mit „systematisch“ verwandt, ist aber erheblich stärker, da er nicht nur angibt, dass zur Durchführung der Analyse oder Aktivität eine methodischer Ansatz nach einem eindeutigen Plan befolgt wurde, sondern auch, dass der befolgte Plan ausreicht, um sicherzustellen, dass alle möglichen Verfahrensweisen durchgeführt wurden.

3.1.31
erklären
ein Argument für die Begründung einer gewählten Vorgehensweise liefern

ANMERKUNG Dieser Begriff unterscheidet sich von den Begriffen „beschreiben“ und „demonstrieren“. Er soll die Frage nach dem „Warum“ beantworten, ohne Argumente dafür zu liefern, dass die gewählte Vorgehensweise notwendigerweise optimal war.

3.1.32
Erweiterung
Hinzufügen von funktionellen Anforderungen, die nicht in ISO/IEC 15408-2 enthalten sind, zu einem ST oder PP und/oder Hinzufügen von Sicherheitsanforderungen, die nicht in ISO/IEC 15408-3 enthalten sind

3.1.33
externe Entität
menschliche oder IT-Entität, die möglicherweise von außerhalb der TOE-Grenze mit dem TOE interagiert

ANMERKUNG Eine externe Entität kann auch als Benutzer bezeichnet werden.

3.1.34
Familie
Satz von Komponenten, die eine ähnliche Zielsetzung haben, sich aber in Schwerpunkt oder Stringenz unterscheiden

3.1.35
formell
ausgedrückt in einer Sprache mit begrenzter Syntax und definierter Semantik, basierend auf anerkannten mathematischen Konzepten

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.1.36
Leitliniendokumentation
Dokumentation, die die Auslieferung, die Bereitstellung, den Betrieb, das Management und/oder die Verwendung des TOE beschreibt

3.1.37
Identität
Repräsentation, mit der Entitäten im Zusammenhang mit dem TOE eindeutig identifiziert werden (z. B. Benutzer, Prozesse oder Festplatten)

ANMERKUNG Ein Beispiel für eine solche Repräsentation ist eine Zeichenkette. Bei einem menschlichen Benutzer kann die Repräsentation der vollständige oder abgekürzte Name oder ein (nach wie vor eindeutiges) Pseudonym sein.

3.1.38
informell
in der natürlichen Sprache ausgedrückt

3.1.39
Inter-TSF-Übertragungen
Datenkommunikation zwischen dem TOE und den Sicherheitsfunktionen anderer vertrauenswürdiger IT-Produkte

3.1.40
interner Kommunikationskanal
Kommunikationskanal zwischen getrennten Teilen des TOE

3.1.41
interne TOE-Übertragung
Datenkommunikation zwischen getrennten Teilen des TOE

3.1.42
in sich widerspruchsfrei
es bestehen keine offensichtlichen Widersprüche zwischen irgendwelchen Aspekten einer Entität

ANMERKUNG In Bezug auf Dokumentation bedeutet dies, dass keine Aussagen in der Dokumentation enthalten sein können, die als widersprüchlich zueinander interpretiert werden können.

3.1.43
Iteration
Verwendung der gleichen Komponente, um zwei oder mehr unterschiedliche Anforderungen auszudrücken

3.1.44
Begründung
Analyse, die zu einer Schlussfolgerung führt

ANMERKUNG „Begründung“ ist stringenter als ein Nachweis. Dieser Begriff erfordert erhebliche Stringenz, indem jeder Schritt eines logischen Arguments sehr sorgfältig und gründlich erläutert wird.

3.1.45
Objekt
passive Entität im TOE, die Informationen enthält oder empfängt und an der Subjekte Operationen durchführen

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.1.46
Operation
<an einer Komponente von ISO/IEC 15408> Modifikation oder Wiederholung einer Komponente

ANMERKUNG Zulässige Operationen an Komponenten sind Zuordnung, Iteration, Präzisierung und Auswahl.

3.1.47
Operation
<an einem Objekt> spezifische Aktion, die durch ein Subjekt an einem Objekt durchgeführt wird

3.1.48
Betriebsumgebung
Umgebung, in der das TOE betrieben wird

3.1.49
organisatorische Sicherheitspolitik
OSP
(en: Organisational Security Policy)
Satz von Sicherheitsregeln, -verfahren oder -leitlinien für eine Organisation

ANMERKUNG Eine Politik kann sich auf eine spezifische Betriebsumgebung beziehen.

3.1.50
Paket
benannter Satz von Anforderungen bezüglich der Sicherheitsfunktionalität oder -garantie

ANMERKUNG Ein Beispiel für ein Paket ist „EAL 3“.

3.1.51
Schutzprofilevaluierung
Bewertung eines PP auf Grundlage definierter Kriterien

3.1.52
Schutzprofil
PP
(en: Protection Profile)
implementierungsunabhängige Beschreibung der Sicherheitsanforderungen für einen TOE-Typ

3.1.53
beweisen
Übereinstimmung im mathematischen Sinn durch formelle Analyse aufzeigen

ANMERKUNG Der Begriff ist in jeder Beziehung vollständig stringent. Im Allgemeinen wird „beweisen“ verwendet, wenn die Übereinstimmung zwischen zwei TSF-Darstellungen auf einem hohen Stringenzniveau dargestellt werden soll.

3.1.54
Präzisierung
Hinzufügen von Details zu einer Komponente

3.1.55
Rolle
vordefinierter Regelsatz, der die zulässigen Interaktionen zwischen einem Benutzer und dem TOE festlegt

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.1.56
Geheimnis
Informationen, die nur autorisierten Benutzern und/oder dem TSF bekannt sein dürfen, um ein spezifisches SFP durchzusetzen

3.1.57
sicherer Zustand
Zustand, in dem die TSF-Daten konsistent sind und das TSF die ordnungsgemäße Durchsetzung der SFRs fortlaufend wahrnimmt

3.1.58
Sicherheitsattribut
Eigenschaft von Subjekten, Benutzern (einschließlich externen IT-Produkten), Objekten, Informationen, Sitzungen und/oder Ressourcen, die verwendet wird, um die SFRs zu definieren, und deren Werte zur Durchsetzung der SFRs verwendet werden

3.1.59
Sicherheitsfunktionspolitik
SFP
(en: Security Function Policy)
Regelsatz, der ein bestimmtes Sicherheitsverhalten beschreibt, das vom TSF durchgesetzt wird und sich als ein Satz von SFRs beschreiben lässt

3.1.60
Sicherheitszielsetzung
(en: Security Objective)
Absichtserklärung, identifizierte Bedrohungen abzuwehren und/oder identifizierte organisatorische Sicherheitspolitiken und/oder -annahmen zu erfüllen

3.1.61
Sicherheitsproblem
Aussage, die formell die Natur und den Geltungsbereich der Sicherheit definiert, welche das TOE adressieren soll

ANMERKUNG Diese Aussage besteht aus folgenden Teilen:

— den Bedrohungen, die durch das TOE und seine Betriebsumgebung abgewehrt werden sollen,

— den OSPs, die durch das TOE und seine Betriebsumgebung durchgesetzt werden, und

— den Annahmen, die für die Betriebsumgebung des TOE bestehen.

3.1.62
Sicherheitsanforderung
in einer standardisierten Sprache ausgedrückte Anforderung, die zur Erreichung der Sicherheitsziele für ein TOE beitragen soll

3.1.63
Sicherheitsvorgabe
ST
(en: Security Target)
implementierungsabhängige Beschreibung der Sicherheitsanforderungen für ein spezifisches, identifiziertes TOE

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.1.64
Auswahl
Spezifikation eines oder mehrerer Element(e) aus einer Liste innerhalb einer Komponente

3.1.65
halbformell
ausgedrückt in einer Sprache mit begrenzter Syntax und definierter Semantik

3.1.66
spezifizieren
auf stringente und präzise Weise spezifische Einzelheiten zu einer Entität bereitstellen

3.1.67
strikte Konformität
hierarchische Beziehung zwischen einem ST und einem PP, wobei alle Anforderungen im PP auch im ST vorhanden sind

ANMERKUNG Diese Beziehung kann grob definiert werden als: „das ST muss alle Aussagen enthalten, die im PP vorhanden sind, darf aber weitere enthalten“. Es wird erwartet, dass strikte Konformität für stringente Anforderungen eingesetzt wird, die in konsistenter Weise erfüllt werden müssen.

3.1.68
ST-Evaluierung
Bewertung eines ST auf Grundlage definierter Kriterien

3.1.69
Subjekt
aktive Entität im TOE, die Operationen an Objekten durchführt

3.1.70
Evaluierungsgegenstand
TOE
(en: Target of Evaluation)
Satz von Software, Firmware und/oder Hardware, möglicherweise mit beigefügten Leitlinien

3.1.71
Bedrohungsagent
Entität, die auf Schutzobjekte nachteilig einwirken kann

3.1.72
TOE-Evaluierung
Bewertung eines TOE auf Grundlage definierter Kriterien

3.1.73
TOE-Ressource
alles, was innerhalb des TOE nutzbar oder verwertbar ist

3.1.74
TOE-Sicherheitsfunktionalität
(en: TOE Security Functionality)
kombinierte Funktionalität der gesamten Hardware, Software und Firmware eines TOE, welche die korrekte Durchsetzung der SFRs sicherstellen muss

3.1.75
verfolgen, Verb
Durchführen einer informellen Korrespondenzanalyse zwischen zwei Entitäten mit nur minimaler Stringenz

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.1.76
Übertragungen außerhalb des TOE
TSF-vermittelte Kommunikation von Daten an Entitäten, die nicht der Kontrolle des TSF unterliegen

3.1.77
Übersetzung
beschreibt den Prozess der Beschreibung von Sicherheitsanforderungen in einer standardisierten Sprache

ANMERKUNG Die Verwendung des Begriffs „Übersetzung“ ist in diesem Zusammenhang nicht wörtlich zu nehmen; es wird nicht impliziert, dass jedes in standardisierter Sprache ausgedrückte SFR wieder in die Sicherheitszielsetzungen zurückübersetzt werden kann.

3.1.78
vertrauenswürdiger Kanal
ein Weg, über den ein TSF und ein anderes vertrauenswürdiges IT-Produkt mit dem notwendigen Vertrauensgrad kommunizieren können

3.1.79
vertrauenswürdiges IT-Produkt
IT-Produkt (nicht das TOE), dessen funktionelle Sicherheitsanforderungen administrativ mit dem TOE koordiniert sind und von dem angenommen wird, dass es die funktionellen Sicherheitsanforderungen korrekt implementiert

ANMERKUNG Ein Beispiel für ein vertrauenswürdiges IT-Produkt wäre ein Produkt, das getrennt evaluiert wurde.

3.1.80
vertrauenswürdiger Pfad
Weg, über den ein Anwender und ein TSF mit dem notwendigen Vertrauensgrad kommunizieren können

3.1.81
TSF-Daten
Daten für den Betrieb des TOE, welche für die Durchsetzung des SFR benötigt werden

3.1.82
TSF-Schnittstelle
(en: TSF Interface)
Weg, über den externe Entitäten (oder Subjekte im TOE, die nicht Teil des TSF sind) Daten an das TSF übermitteln, Daten vom TSF empfangen und Dienste des TSF aufrufen

3.1.83
Benutzerdaten
Daten für den Benutzer, die nicht den Betrieb des TSF beeinflussen

3.1.84
verifizieren
streng, detailliert und mit einer unabhängig bestimmten Angemessenheit prüfen

ANMERKUNG Siehe auch „bestätigen“. Dieser Begriff hat eine strengere Bedeutung. Der Begriff „verifizieren“ wird im Zusammenhang mit Evaluatorenaktionen verwendet, wenn eine unabhängige Anstrengung durch den Evaluator erforderlich ist.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.2 Begriffe in Zusammenhang mit der ADV-Klasse

ANMERKUNG Die folgenden Begriffe werden in den Anforderungen an die interne Software-Struktur verwendet. Einige sind entnommen aus IEEE Standard 610.12-1990, *Standard glossary of software engineering terminology, Institute of Electrical and Electronics Engineers*.

3.2.1
Administrator
Entität, die bezüglich aller durch das TSF implementierten Politiken einen Vertrauensgrad besitzt

ANMERKUNG Nicht alle PPs und STs nehmen für Administratoren den gleichen Vertrauensgrad an. Üblicherweise wird angenommen, dass Administratoren jederzeit die im ST des TOE definierten Politiken einhalten. Manche dieser Politiken können mit der Funktionalität des TOE in Zusammenhang stehen, andere mit der Betriebsumgebung.

3.2.2
Aufrufbaum
identifiziert die Module in einem System in Form eines Diagramms, das aufzeigt, welche Module sich gegenseitig aufrufen

ANMERKUNG Basierend auf IEEE Standard 610.12-1990.

3.2.3
Kohäsion
Modulstärke
Art und Grad, wie die von einem Software-Modul durchgeführten Aufgaben miteinander in Zusammenhang stehen

[IEEE Standard 610.12-1990]

ANMERKUNG Zu den Kohäsionsarten gehören die zufällige, die kommunikative, die funktionelle, die logische, die sequentielle und die zeitliche Kohäsion. Diese Kohäsionsarten werden beim entsprechenden Begriffseintrag beschrieben.

3.2.4
zufällige Kohäsion
Modul, das unzusammenhängende oder nur bedingt zusammenhängende Aktivitäten ausführt

[IEEE Standard 610.12-1990]

ANMERKUNG Siehe auch Kohäsion (3.2.3).

3.2.5
kommunikative Kohäsion
Modul, das Funktionen enthält, die Ausgaben für andere Funktionen innerhalb des Moduls produzieren oder Ausgaben anderer Funktionen innerhalb des Moduls nutzen

[IEEE Standard 610.12-1990]

ANMERKUNG 1 Siehe auch Kohäsion (3.2.3).

ANMERKUNG 2 Ein Beispiel für ein kommunikativ kohäsives Modul ist ein Zugriffsüberprüfungsmodul, das obligatorische, diskrete und Funktionsprüfungen enthält.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.2.6
Komplexität
Maßwert dafür, wie schwierig Software zu verstehen und daher zu analysieren, testen und warten ist

[IEEE Standard 610.12-1990]

ANMERKUNG Die Reduzierung der Komplexität ist das oberste Ziel beim Einsatz von modularer Aufteilung, Schichtung und Minimierung. Die Kontrolle von Kopplung und Kohäsion trägt erheblich zur Erreichung dieses Ziels bei.

Im Bereich des Software-Engineering wurde erheblicher Aufwand in den Versuch investiert, Metriken zur Messung der Komplexität von Quellcode zu entwickeln. Die meisten dieser Metriken nutzen einfach zu berechnende Eigenschaften des Quellcodes, wie beispielsweise die Anzahl von Operatoren und Operanden, die Komplexität des Kontrollflussgraphen (zyklomatische Komplexität), die Anzahl der Quellcode-Zeilen, das Verhältnis zwischen Kommentaren und ausführbarem Code und ähnliche Maßwerte. Kodierungsstandards haben sich als wertvolles Instrument zur Erzeugung von Code erwiesen, der einfacher zu verstehen ist.

Die Familie der TSF-Interna (ADV_INT) erfordert eine Komplexitätsanalyse aller Komponenten. Es wird erwartet, dass der Entwickler Nachweise für die Behauptung liefert, dass die Komplexität ausreichend reduziert wurde. Diese Nachweise können beispielsweise die Programmierstandards des Entwicklers enthalten sowie eine Angabe, dass alle Module den Standards entsprechen (oder dass es einige Ausnahmen gibt, die durch Software-Engineering-Argumente begründet sind). Sie könnten die Ergebnisse von Werkzeugen enthalten, die zur Messung mancher Eigenschaften des Quellcodes eingesetzt wurden, oder andere Nachweise, die der Entwickler für angemessen hält.

3.2.7
Kopplung
Art und Grad der gegenseitigen Abhängigkeit von Software-Modulen

[IEEE Standard 610.12-1990]

ANMERKUNG Zu den Kopplungsarten gehören die Aufrufkopplung, die Bereichskopplung und die Inhaltskopplung. Diese sind nachstehend beschrieben.

3.2.8
Aufrufkopplung
Beziehung zwischen zwei Modulen, die strikt nur über ihre dokumentierten Funktionsaufrufe kommunizieren

ANMERKUNG Beispiele für die Aufrufkopplung sind die Daten-, Datenstruktur- und Kontrollkopplung.

3.2.9
Aufrufkopplung
<Datenkopplung> Beziehung zwischen zwei Modulen, die strikt nur durch die Verwendung von Aufrufparametern kommunizieren, die einzelnen Datenelementen entsprechen

ANMERKUNG Siehe auch Aufrufkopplung (3.2.8).

3.2.10
Aufrufkopplung
<Datenstrukturkopplung> Beziehung zwischen zwei Modulen, die durch die Verwendung von Aufrufparametern kommunizieren, die mehrere Felder umfassen oder die sinnvolle interne Strukturen haben

ANMERKUNG Siehe auch Aufrufkopplung (3.2.8).

3.2.11
Aufrufkopplung
<Kontrollkopplung> Beziehung zwischen zwei Modulen, wobei ein Modul Informationen weitergibt, welche die interne Logik des anderen Moduls beeinflussen sollen

ANMERKUNG Siehe auch Aufrufkopplung (3.2.8).

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.2.12
Bereichskopplung
Beziehung zwischen zwei Modulen, die sich einen gemeinsamen Datenbereich oder eine andere gemeinsame Systemressource teilen

ANMERKUNG Globale Variablen zeigen an, dass die Module, die diese globalen Variablen verwenden, über eine Bereichskopplung verfügen. Die Bereichskopplung mittels globaler Variablen ist allgemein zulässig, aber nur in einem begrenzten Ausmaß.

Beispielsweise sind Variablen, die in einem globalen Bereich platziert sind, aber nur von einem einzigen Modul verwendet werden, unpassend platziert und sollten entfernt werden. Weitere Faktoren, die bei der Bewertung der Eignung globaler Variablen berücksichtigt werden müssen, sind:

Die Anzahl der Module, die eine globale Variable modifizieren: Im Allgemeinen sollte nur ein einziges Modul die Kontrolle des Inhalts einer globalen Variablen wahrnehmen, aber es kann Situationen geben, in denen ein zweites Modul diese Aufgabe ebenfalls wahrnimmt; in solchen Fällen muss eine ausreichende Begründung geliefert werden. Es ist nicht annehmbar, dass diese Aufgabe von mehr als zwei Modulen wahrgenommen wird. (Bei der Durchführung dieser Bewertung sollte sorgfältig bestimmt werden, welches Modul tatsächlich für den Inhalt der Variablen verantwortlich ist. Wenn die Variable beispielsweise nur von einer Routine modifiziert wird, aber diese Routine einfach nur die vom aufrufenden Modul angeforderte Modifikation durchführt, dann ist das aufrufende Modul verantwortlich, und es könnten mehrere solcher Module vorhanden sein). Wenn zwei Module für den Inhalt einer globalen Variablen zuständig sind, sollte des Weiteren als Teil der Komplexitätsbewertung klar definiert sein, wie die Modifikationen zwischen den Modulen koordiniert werden.

Die Anzahl der Module, die eine globale Variable referenzieren: Auch wenn es keinen allgemeinen Grenzwert für die Anzahl der Module gibt, die eine globale Variable referenzieren., sollte in Fällen, in denen viele Module eine solche Referenzierung durchführen, die Gültigkeit und Notwendigkeit untersucht werden.

3.2.13
Inhaltskopplung
Beziehung zwischen zwei Modulen, wobei ein Modul die Interna des anderen Moduls direkt referenziert

ANMERKUNG Beispiele sind die Modifizierung des Codes oder die Referenzierung von internen Labels des anderen Moduls. Daraus ergibt sich, dass ein Teil oder der gesamte Inhalt eines Moduls effektiv im anderen Modul enthalten ist. Die Inhaltskopplung kann als die Verwendung nicht offengelegter Modulschnittstellen betrachtet werden, im Gegensatz zur Aufrufkopplung, bei der nur offengelegte Modulschnittstellen verwendet werden.

3.2.14
Domänentrennung
Eigenschaft von Sicherheitsarchitekturen, wobei das TSF getrennte Sicherheitsdomänen für jeden Benutzer und für das TSF definiert und sicherstellt, dass kein Benutzerprozess den Inhalt der Sicherheitsdomäne eines anderen Benutzers oder des TSF beeinflussen kann

3.2.15
funktionelle Kohäsion
funktionelle Eigenschaft eines Moduls, das nur Aktivitäten für eine einzige Aufgabe durchführt

[IEEE Standard 610.12-1990]

ANMERKUNG Ein funktionell kohäsives Modul wandelt eine einzige Eingabeart in eine einzige Ausgabeart um, wie beispielsweise ein Stack-Manager oder ein Warteschlangen-Manager. Siehe auch Kohäsion (3.2.3).

3.2.16
Interaktion
allgemeine, auf Kommunikation basierende Aktivität zwischen Entitäten

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.2.17
Schnittstelle
Mittel zur Interaktion mit einer Komponente oder einem Modul

3.2.18
Schichtung
Entwurfstechnik, bei der getrennte Modulgruppen (die Schichten) hierarchisch so organisiert sind, dass sie getrennte Zuständigkeiten besitzen, wobei eine Schicht nur die Dienste der in der Hierarchie darunterliegenden Schichten nutzt und die eigenen Dienste nur den darüberliegenden Schichten zur Verfügung stellt

ANMERKUNG Bei einer strengen Schichtung gilt zusätzlich, dass jede Schicht nur die Dienste der unmittelbar darunterliegenden Schicht nutzen kann und ihre Dienste nur für die unmittelbar darüberliegende Schicht zur Verfügung stellt.

3.2.19
logische Kohäsion
prozedurale Kohäsion
Merkmale eines Moduls, das ähnliche Aktivitäten an verschiedenen Datenstrukturen durchführt

ANMERKUNG Ein Modul weist eine logische Kohäsion auf, wenn seine Funktionen verwandte, aber unterschiedliche Operationen an verschiedenen Eingaben durchführen. Siehe auch „Kohäsion“.

3.2.20
modulare Aufteilung
Prozess der Aufteilung eines Systems in Komponenten, um den Entwurf, die Entwicklung und die Evaluierung zu vereinfachen

[IEEE Standard 610.12-1990]

3.2.21
Unumgänglichkeit
<des TSF> Eigenschaft einer Sicherheitsarchitektur, wobei alle Aktionen in Zusammenhang mit dem SFR vom TSF vermittelt werden

3.2.22
Sicherheitsdomänen
Umgebungen, die vom TSF für die Nutzung durch nicht vertrauenswürdige Entitäten derart bereitgestellt werden, dass diese Umgebungen isoliert und voreinander geschützt sind

3.2.23
sequentielle Kohäsion
Modul, das Funktionen enthält, deren Ausgaben als Eingaben für die jeweils folgenden Funktionen innerhalb des Moduls genutzt werden

[IEEE Standard 610.12-1990]

ANMERKUNG Ein Beispiel für ein sequentiell-kohäsives Modul ist ein Modul, das Funktionen zum Schreiben von Audit-Datensätzen und zur laufenden Zählung einer spezifischen Art von akkumulierten Audit-Verletzungen enthält.

3.2.24
Software-Engineering
Einsatz eines systematischen, disziplinierten und quantifizierbaren Verfahrens zur Entwicklung und Wartung von Software; kurz die Anwendung von Ingenieurwissenschaften auf Software

[IEEE Standard 610.12-1990]

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

ANMERKUNG Wie bei allen ingenieurwissenschaftlichen Praktiken ist bei der Anwendung der Engineering-Prinzipien ein gewisses Urteilsvermögen nötig. Entscheidungen werden durch eine Vielzahl von Faktoren beeinflusst, nicht nur durch die Anwendung von Maßnahmen zur modularen Aufteilung, Schichtung und Minimierung. So kann ein Entwickler beispielsweise ein System entwerfen, bei dem er zukünftige Applikationen berücksichtigt, die anfänglich nicht implementiert werden. Der Entwickler kann daher Logik einbinden, um diese zukünftigen Applikationen zu handhaben, ohne sie vollständig zu implementieren; des Weiteren kann der Entwickler Aufrufe von bisher nicht implementierten Modulen einschließen, so dass unvollständige Aufrufe (en: Call Stubs) entstehen. Bei der Beurteilung. ob solche Abweichungen von gut strukturierten Programmen durch den Entwickler gerechtfertigt sind, muss Urteilsvermögen und eine gute Software-Engineering-Disziplin zur Anwendung kommen.

3.2.25
zeitliche Kohäsion
Merkmal eines Moduls, das Funktionen enthält, die ungefähr gleichzeitig ausgeführt werden müssen

ANMERKUNG 1 Basierend auf [IEEE Standard 610.12-1990].

ANMERKUNG 2 Beispiele für zeitlich kohäsive Module sind Module für die Initialisierung, Wiederherstellung und Abschaltung.

3.2.26
TSF-Selbstschutz
Eigenschaft einer Sicherheitsarchitektur, wobei das TSF nicht von TSF-fremdem Code oder fremden Entitäten beschädigt werden kann

3.3 Begriffe in Zusammenhang mit der AGD-Klasse

3.3.1
Installation
von einem menschlichen Benutzer durchgeführtes Verfahren zur Einbindung des TOE in seine Betriebsumgebung und dessen Inbetriebnahme

ANMERKUNG Diese Operation wird normalerweise nur einmal nach Erhalt und Abnahme des TOE durchgeführt. Es wird erwartet, dass das TOE soweit konfiguriert wird, dass die Konfiguration entsprechend dem ST zulässig ist. Wenn ähnliche Prozesse durch den Entwickler durchgeführt werden müssen, dann werden sie im Rahmen der ALC: Produktlebenszyklusunterstützung als „Generierung“ bezeichnet. Falls das TOE eine Erstinbetriebnahme erfordert, die nicht regelmäßig wiederholt werden muss, dann würde dieser Prozess als Installation eingestuft.

3.3.2
Betrieb
Nutzungszeitraum des TOE, einschließlich „übliche Nutzung“, Administration und Wartung des TOE nach Auslieferung und Bereitstellung

3.3.3
Bereitstellung
Aktivität in der Lebenszyklusphase eines Produkts, die die Kundenabnahme des ausgelieferten TOE und dessen Installation umfasst, worunter Aktivitäten wie das Hochfahren, die Initialisierung, die Erstinbetriebnahme und die Vorbereitung des TOE bis zu einem betriebsbereiten Zustand fallen können

3.4 Begriffe in Zusammenhang mit der ALC-Klasse

3.4.1
Abnahmekriterien
während der Durchführung der Abnahmeverfahren anzuwendende Kriterien (z. B. erfolgreiche Dokumentationsprüfung oder, im Fall von Software, Firmware oder Hardware, erfolgreiche Funktionsprüfung)

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.4.2
Abnahmeverfahren
Verfahren, die durchgeführt werden, um neu erstellte oder geänderte Konfigurationselemente als Teil des TOE zu akzeptieren oder in den nächsten Lebenszyklusschritt zu überführen

ANMERKUNG Diese Verfahren identifizieren die Rollen oder Einzelpersonen, die für die Abnahme verantwortlich sind, sowie die anzuwendenden Kriterien, die für die Entscheidung über die Abnahme herangezogen werden.

Es gibt mehrere Arten von Abnahmesituationen; manche können sich überschneiden:

a) erstmalige Übernahme eines Elements in das Konfigurationsmanagementsystem, insbesondere Einbindung von Software-, Firmware- und Hardware-Komponenten anderer Hersteller in das TOE („Integration“);

b) Überführung von Konfigurationselementen in die nächste Lebenszyklusphase in allen Entwurfsphasen des TOE (z. B. Modul, Teilsystem, Qualitätskontrolle des fertiggestellten TOE);

c) im Anschluss an Transporte von Konfigurationselementen (z. B. Teilen des TOE oder vorläufigen Produkten) zwischen verschiedenen Entwicklungsstandorten;

d) im Anschluss an die Auslieferung des TOE an den Verbraucher.

3.4.3
Konfigurationsmanagement
CM
(en: Configuration Management)
Fachgebiet, in dem technische und administrative Anleitung und Überwachung eingesetzt werden, um die funktionellen und physikalischen Merkmale eines Konfigurationselements zu identifizieren und zu dokumentieren, Änderungen dieser Merkmale zu kontrollieren, die Umsetzung von Änderungen sowie den Implementierungsstatus aufzuzeichnen und zu berichten und die Einhaltung der festgelegten Anforderungen zu überprüfen

ANMERKUNG Basierend auf IEEE Standard 610.12.

3.4.4
CM-Dokumentation
vollständige CM-Dokumentation, umfasst die CM-Ausgaben, die CM-Liste (Konfigurationsliste), die CM-Systemdatensätze, die CM-Planung und die CM-Nutzung

3.4.5
Konfigurationsmanagementnachweis
alle Nachweise, die verwendet werden können, um Vertrauen in den ordnungsgemäßen Betrieb des CM-Systems herzustellen

ANMERKUNG Zum Beispiel CM-Ausgaben, vom Entwickler gelieferte Begründungen, Beobachtungen, Experimente oder Interviews, die während einer Standortbegehung vom Evaluator durchgeführt wurden.

3.4.6
Konfigurationselement
Objekt, das während der TOE-Entwicklung vom CM-System gesteuert wird

ANMERKUNG Es kann sich dabei entweder um Teile des TOE oder um Objekte handeln, die mit der Entwicklung des TOE in Zusammenhang stehen, wie beispielsweise Beurteilungsdokumente oder Entwicklungswerkzeuge. CM-Elemente können, zusammen mit ihrer Version, entweder direkt im CM-System gespeichert sein (zum Beispiel Dateien) oder referenziert werden (zum Beispiel Hardware-Bauteile).

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.4.7
Konfigurationsliste
Ausgabedokument des Konfigurationsmanagements, das alle Konfigurationselemente für ein spezifisches Produkt zusammen mit der genauen Version aller Konfigurationsmanagementelemente auflistet, die für eine bestimmte Version des Gesamtprodukts relevant sind

ANMERKUNG Diese Liste ermöglicht die Unterscheidung der Elemente, die zur evaluierten Version des Produkts gehören, von anderen Versionen dieser Elemente, die zu anderen Produktversionen gehören. Die finale Konfigurationsmanagementliste ist ein spezifisches Dokument für eine spezifische Version des spezifischen Produkts. (Bei der Liste kann es sich natürlich um ein elektronisches Dokument innerhalb eines Konfigurationsmanagement-Werkzeugs handeln. In diesem Fall kann sie als spezifischer Einblick in das System oder einen Teil des Systems angesehen werden und nicht als eine Ausgabe des Systems. Allerdings wird die Konfigurationsliste im praktischen Einsatz während einer Evaluierung vermutlich als Teil der Evaluierungsdokumentation bereitgestellt werden.) Die Konfigurationsliste definiert die Elemente, die unter die Konfigurationsmanagementanforderungen von ALC_CMC fallen.

3.4.8
Konfigurationsmanagementausgabe
Ergebnisse in Bezug auf das Konfigurationsmanagement, die vom Konfigurationsmanagementsystem erstellt oder durchgesetzt werden

ANMERKUNG Diese mit dem Konfigurationsmanagement in Zusammenhang stehenden Ergebnisse können die Form von Dokumenten haben (zum Beispiel ausgefüllte Papierformulare, Konfigurationsmanagement-Systemdatensätze, Protokolldaten, Ausdrucke und elektronische Ausgabedaten) oder von Aktionen (zum Beispiel manuelle Maßnahmen zur Erfüllung von Konfigurationsmanagementanweisungen). Beispiele für solche Konfigurationsmanagementausgaben sind Konfigurationslisten, Konfigurationsmanagementpläne und/oder das Verhalten während des Produktlebenszyklus.

3.4.9
Konfigurationsmanagementplan
Beschreibung, wie das Konfigurationsmanagementsystem für das TOE eingesetzt wird

ANMERKUNG Das Ziel bei der Erstellung eines Konfigurationsmanagementplans ist es, Mitarbeitern deutlich zu machen, welche Aufgaben zu erfüllen sind. Aus Sicht des gesamten Konfigurationsmanagementsystems kann dieser als Ausgabedokument betrachtet werden (da er möglicherweise als Teil der Anwendung des Konfigurationsmanagement-systems erstellt wird). Aus Sicht des konkreten Projekts handelt es sich um ein Anwendungsdokument, da er von den Mitgliedern des Projektteams verwendet wird, um die Schritte zu verstehen, die während des Projekts durchgeführt werden müssen. Der Konfigurationsmanagementplan beschreibt die Anwendung des Systems für das spezifische Produkt; das gleiche System kann in einem anderen Umfang für andere Produkte eingesetzt werden. Dies bedeutet, dass der Konfigurationsmanagementplan die Ausgaben des während der TOE-Entwicklung eingesetzten Konfigurations-managementsystems eines Unternehmens definiert und beschreibt.

3.4.10
Konfigurationsmanagementsystem
Satz von Verfahren und Werkzeugen (einschließlich deren Dokumentation), der von einem Entwickler zur Entwicklung und Wartung der Konfigurationen seiner Produkte während deren Lebenszyklus verwendet wird

ANMERKUNG Konfigurationsmanagementsysteme können über unterschiedliche Stringenz- und Funktionsgrade verfügen. Auf den höheren Stufen können Konfigurationsmanagementsysteme automatisiert sein und über Mängelbehebung, Änderungskontrolle und andere Nachverfolgungsmechanismen verfügen.

3.4.11
Konfigurationsmanagementsystem-Datensätze
Ausgaben, die während des Betriebs des Konfigurationsmanagementsystems erstellt werden und wichtige Konfigurationsmanagementaktivitäten dokumentieren

ANMERKUNG Beispiele für Konfigurationsmanagementsystem-Datensätze sind Kontrollformulare für Änderungen der Konfigurationsmanagementelemente oder Zugriffsgenehmigungsformulare für Konfigurationsmanagement-elemente.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.4.12
Konfigurationsmanagementwerkzeuge
manuell geführte oder automatisierte Werkzeuge, die ein Konfigurationsmanagementsystem realisieren oder unterstützen

ANMERKUNG Beispielsweise Werkzeuge für die Versionsverwaltung der TOE-Teile.

3.4.13
Konfigurationsmanagement-Nutzungsdokumentation
Teil des Konfigurationsmanagementsystems, der beschreibt, wie das Konfigurationsmanagementsystem definiert und angewendet wird, beispielsweise mithilfe von Handbüchern, Vorschriften und/oder der Dokumentation von Werkzeugen und Verfahren

3.4.14
Auslieferung
Übergabe des fertiggestellten TOE von der Produktionsumgebung in die Hände des Kunden

ANMERKUNG Diese Produktlebenszyklusphase kann die Verpackung und Lagerung am Entwicklungsstandort beinhalten, aber umfasst nicht den Transport des nicht fertiggestellten TOE oder von dessen Teilen zwischen verschiedenen Entwicklern oder Entwicklungsstandorten.

3.4.15
Entwickler
für die Entwicklung des TOE zuständige Organisation

3.4.16
Entwicklung
Produktlebenszyklusphase, welche die Erzeugung der Implementierungsrepräsentation des TOE betrifft

ANMERKUNG Im Rahmen der Unterstützungsanforderungen während des ALC: Produktlebenszyklus sind Entwicklung und verwandte Begriffe (Entwickler, entwickeln) im allgemeineren Sinn zu verstehen und umfassen die Entwicklung und die Erstellung.

3.4.17
Entwicklungswerkzeuge
Werkzeuge (einschließlich Testsoftware, falls zutreffend), welche die Entwicklung und Erstellung des TOE unterstützen

ANMERKUNG Beispielsweise sind bei einem Software-TOE die Entwicklungswerkzeuge in der Regel Programmiersprachen, Compiler, Linker und Generierungswerkzeuge.

3.4.18
Implementierungsrepräsentation
am wenigsten abstrakte Darstellung des TSF, genauer die Darstellung, die ohne weitere Designverfeinerung zur Erstellung des TSF selbst verwendet wird

ANMERKUNG Beispiele für Teile von Implementierungsrepräsentationen sind Quellcode, der anschließend kompiliert wird, oder Hardware-Zeichnungen, die zum Aufbau der eigentlichen Hardware verwendet werden.

3.4.19
Lebenszyklus
Abfolge von Daseinsstufen eines Objekts (zum Beispiel eines Produkts oder eines Systems) über die Zeit

3.4.20
Lebenszyklusdefinition
Definition des Lebenszyklusmodells

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.4.21
Lebenszyklusmodell
Beschreibung der für die Lebenszyklusverwaltung eines bestimmten Objekts verwendeten Stufen und deren Beziehungen untereinander und ihrer Abfolge sowie ein Überblick ihrer Merkmale

ANMERKUNG Siehe auch Bild 1.

3.4.22
Erstellung
die Erstellungs-Lebenszyklusphase folgt der Entwicklungsphase und besteht aus der Umsetzung der Implementierungsrepräsentation in die Implementierung des TOE, d. h. in einen Zustand, der für die Auslieferung an den Kunden geeignet ist

ANMERKUNG Diese Phase kann die Herstellung, Integration, Generierung, interne Transporte, Lagerung und die Kennzeichnung des TOE umfassen.

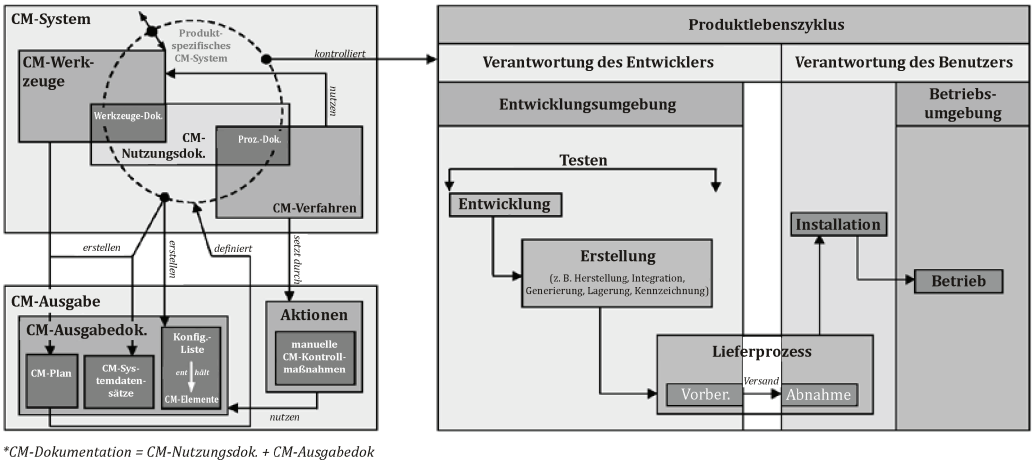


Bild 1 — Terminologie im CM und Produktlebenszyklus

3.5 Begriffe in Zusammenhang mit der AVA-Klasse

3.5.1
verdeckter Kanal
erzwungener, unrechtmäßiger Signalkanal, mit dem der Benutzer heimlich die Mehrstufentrennungspolitik und die Anforderungen an die Nichtbeobachtbarkeit des TOE umgehen kann

3.5.2
aufgedeckte mögliche Vulnerabilitäten
mögliche Schwachstellen im TOE, die vom Evaluator bei der Durchführung der Evaluierungsaktivitäten identifiziert wurden und die für Verletzungen von SFRs genutzt werden könnten

3.5.3
ausnutzbare Vulnerabilität
Schwachstelle im TOE, die für Verletzungen von SFRs in der Betriebsumgebung des TOE genutzt werden kann

3.5.4
Überwachungsangriffe
generische Angriffsmethodenkategorie, die passive Analysetechniken einschließt, welche auf die Offenlegung sensitiver interner Daten des TOE abzielen, wobei das TOE entsprechend der Leitliniendokumentation betrieben wird

AVA Documents Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

3.5.5
mögliche Vulnerabilität
vermutete, aber nicht bestätigte Schwachstelle

ANMERKUNG Der Verdacht ergibt sich aufgrund eines angenommenen Angriffspfads zur Verletzung der SFRs.

3.5.6
Restvulnerabilität
Schwachstelle, die nicht in der Betriebsumgebung des TOE ausgenutzt werden kann, die aber für Verletzungen der SFRs durch einen Angreifer genutzt werden könnte, der ein höheres Angriffspotential hat, als es für die Betriebsumgebung des TOE angenommen wird

3.5.7
Vulnerabilität
Schwachstelle im TOE, die für Verletzungen von SFRs in manchen Umgebungen ausgenutzt werden kann

3.6 Begriffe in Zusammenhang mit der ACO-Klasse

3.6.1
Basiskomponente
Entität in einem zusammengesetzten TOE, die selbst einer Evaluierung unterzogen wurde und die Dienste und Ressourcen für eine abhängige Komponente bereitstellt

3.6.2
kompatibel (Komponenten)
Eigenschaft einer Komponente, um die von einer anderen Komponente geforderten Dienste über die entsprechenden Schnittstellen der beiden Komponenten in einer konsistenten Betriebsumgebung bereitzustellen

3.6.3
Komponenten-TOE
erfolgreich bewertetes TOE, das Teil eines anderen zusammengesetzten TOE ist

3.6.4
zusammengesetztes TOE
TOE, das nur aus zwei oder mehreren Komponenten besteht, die erfolgreich evaluiert wurden

3.6.5
abhängige Komponente
Entität in einem zusammengesetzten TOE, die selbst einer Evaluierung unterzogen wird und die auf die Bereitstellung von Diensten durch eine Basiskomponente angewiesen ist

3.6.6
funktionelle Schnittstelle
externe Schnittstelle, die dem Benutzer den Zugriff auf die Funktionalität des TOE ermöglicht und die nicht direkt an der Durchsetzung der funktionellen Sicherheitsanforderungen beteiligt ist

ANMERKUNG In einem zusammengesetzten TOE sind dies die von der Basiskomponente bereitgestellten Schnittstellen, die von der abhängigen Komponente benötigt werden, um den Betrieb des zusammengesetzten TOE zu unterstützen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

4 Symbole und Abkürzungen

Die folgenden Abkürzungen werden in einem oder mehreren Teilen von ISO/IEC 15408 verwendet:

API Programmierschnittstelle (en: Application Programming Interface)

CAP Zusammengesetztes Sicherheitspaket (en: Composed Assurance Package)

CM Konfigurationsmanagement (en: Configuration Management)

DAC Diskrete Zugriffskontrolle (en: Discretionary Access Control)

EAL Evaluierungssicherheitsstufe (en: Evaluation Assurance Level)

GHz Gigahertz

GUI Grafische Benutzungsschnittstelle (en: Graphical User Interface)

IC Integrierte Schaltung (en: Integrated Circuit)

IOCTL Eingabe-Ausgabe-Steuerung (en: Input Output Control)

IP Internet-Protokoll (en: Internet Protocol)

IT Informationstechnik (en: Information Technology)

MB Megabyte

OS Betriebssystem (en: Operating System)

OSP Organisatorische Sicherheitspolitik (en: Organisational Security Policy)

PC Personal Computer

PCI Peripheral Component Interconnect

PKI Public-Key-Infrastruktur (en: Public Key Infrastructure)

PP Schutzprofil (en: Protection Profile)

RAM Direktzugriffsspeicher (en: Random Access Memory)

RPC Remote Procedure Call

SAR Sicherheitsgarantieanforderung (en: Security Assurance Requirement)

SFR Funktionelle Sicherheitsanforderung (en: Security Functional Requirement)

SFP Sicherheitsfunktionspolitik (en: Security Function Policy)

SPD Sicherheitsproblemdefinition (en: Security Problem Definition)

ST Sicherheitsvorgabe (en: Security Target)

TCP Transmission Control Protocol

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

TOE	Evaluierungsgegenstand (en: Target of Evaluation)
TSF	TOE-Sicherheitsfunktionalität (en: TOE Security Functionality)
TSFI	TSF-Schnittstelle (en: TSF Interface)
VPN	Virtual Private Network

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

Nationaler Anhang NB
(informativ)

Literaturhinweise

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagement-systeme — Anforderungen*

DIN EN ISO/IEC 27002, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheits-maßnahmen*

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

Contents

Page

Foreword v
Introduction vi
2 Normative references 1
3 Terms and definitions 1
3.1 Terms and definitions common in ISO/IEC 15408 2
3.2 Terms and definitions related to the ADV class 9
3.3 Terms and definitions related to the AGD class 13
3.4 Terms and definitions related to the ALC class 13
3.5 Terms and definitions related to the AVA class 17
3.6 Terms and definitions related to the ACO class 17
4 Abbreviated terms 18
5 Overview 19
5.1 General 19
5.2 The TOE 19
5.3 Target audience of ISO/IEC 15408 20
5.4 The different parts of ISO/IEC 15408 21
5.5 Evaluation context 22
6 General model 22
6.1 Introduction to the general model 22
6.2 Assets and countermeasures 23
6.3 Evaluation 27
7 Tailoring Security Requirements 27
7.1 Operations 27
7.2 Dependencies between components 30
7.3 Extended components 30
8 Protection Profiles and Packages 31
8.1 Introduction 31
8.2 Packages 31
8.3 Protection Profiles 31
8.4 Using PPs and packages 34
8.5 Using Multiple Protection Profiles 34
9 Evaluation results 34
9.1 Introduction 34
9.2 Results of a PP evaluation 35
9.3 Results of an ST/TOE evaluation 35
9.4 Conformance claim 35

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2020-01

9.5 Use of ST/TOE evaluation results 36
Annex A (informative) Specification of Security Targets 38
Annex B (informative) Specification of Protection Profiles 54
Annex C (informative) Guidance for Operations 59
Annex D (informative) PP conformance 62
Bibliography 64

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15408-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*. The identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organisations as Common Criteria for Information Technology Security Evaluation. The common XML source for both publications can be found at http://www.commoncriteriaportal.org/cc/

This third edition cancels and replaces the second edition (ISO/IEC 15408-1:2005), which has been technically revised.

ISO/IEC 15408 consists of the following parts, under the general title *Information technology — Security techniques — Evaluation criteria for IT security*:

— *Part 1: Introduction and general model*

— *Part 2: Security functional components*

— *Part 3: Security assurance components*

This corrected version of ISO/IEC 15408-1:2009 incorporates miscellaneous editorial corrections related to the following:

— terminology: correction for the terms "security problem" and "security domains";

— clause 8.3: explanation of strict conformance, removal of former Figure 4.

AVA Documents
Document Sharing Hub

Introduction

ISO/IEC 15408 permits comparability between the results of independent security evaluations. ISO/IEC 15408 does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

ISO/IEC 15408 is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

ISO/IEC 15408 is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using ISO/IEC 15408 in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, may result in meaningless evaluation results.

Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties and methods to determine that an evaluation will provide meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs.

ISO/IEC 15408 addresses protection of assets from unauthorised disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. ISO/IEC 15408 may also be applicable to aspects of IT security outside of these three. ISO/IEC 15408 is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. Apart from IT security, ISO/IEC 15408 may be applied in other areas of IT, but makes no claim of applicability in these areas.

Certain topics, because they involve specialised techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of ISO/IEC 15408. Some of these are identified below.

a) ISO/IEC 15408 does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognised that significant security can often be achieved through or supported by administrative measures such as organisational, personnel, physical, and procedural controls.

b) The evaluation of some technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area.

c) ISO/IEC 15408 does not address the evaluation methodology under which the criteria should be applied. This methodology is given in ISO/IEC 18045.

d) ISO/IEC 15408 does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that ISO/IEC 15408 will be used for evaluation purposes in the context of such a framework.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01

e) The procedures for use of evaluation results in accreditation are outside the scope of ISO/IEC 15408. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors should make separate provisions for those aspects.

f) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in ISO/IEC 15408. Should independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which ISO/IEC 15408 is applied must make provision for such assessments.

ISO terminology, such as "can", "informative", "may", "normative", "shall" and "should" used throughout the document are defined in the ISO/IEC Directives, Part 2. Note that the term "should" has an additional meaning applicable when using this standard. See the note below. The following definition is given for the use of “should” in ISO/IEC 15408.

should

within normative text, “should” indicates “that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.” (ISO/IEC Directives, Part 2).

NOTE ISO/IEC 15408 interprets “not necessarily required” to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2020-01