

VDMA 66413



ICS 21.020; 35.240.50

Ersatz für
VDMA 66413:2012-07

**Funktionale Sicherheit –
Universelle Datenbasis für sicherheitsbezogene Kennwerte
von Komponenten oder Teilen von Steuerungen**

Functional Safety –
Universal data format for safety-related values of components
or parts of control system

Fortsetzung Seite 2 bis 43

Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA)

Inhalt

	Seite
Vorwort	4
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Definition der Geräte-Typen (DeviceType)	11
4.1 Geräte-Typ 1	12
4.2 Geräte-Typ 2	12
4.3 Geräte-Typ 3	12
4.4 Geräte-Typ 4	12
4.5 Kennwerte der Geräte-Typen	13
5 Anforderungen	14
5.1 Anforderungen der ISO 13849-1	14
5.2 Anforderungen der IEC 62061	17
6 Kennwert-Bibliothek	20
6.1 Datenstruktur	20
6.2 Angaben zum Datenbasis-Format [VDMA66413]	22
6.3 Angaben zum Gerätehersteller [Manufacturer]	23
6.4 Datenblock	25
6.4.1 Identifizierung des Gerätes [Device]	25
6.4.2 Anwendungsfall [UseCase]	27
6.4.3 Kennwerte [DeviceType1..4]	31
6.5 Sprachtexte [Language]	33
7 Sprach-Bibliothek (optional)	35
7.1 Datenstruktur	35
7.2 Angaben zum Datenbasis-Format [VDMA66413_Language]	37
7.3 Angaben zum Gerätehersteller [Manufacturer]	38
7.4 Sprachtexte [Language]	39
8 Datentypen	40
Anhang A Dateien für die Anwendung	43
A.1 XML-Schema-Datei Kennwert-Bibliothek	43
A.2 XML-Beispiel-Datei Kennwert-Bibliothek	43
A.3 XML-Schema-Datei Sprach-Bibliothek	43
A.4 XML-Beispiel-Datei Sprach-Bibliothek	43

Vorwort

Dieses Dokument beschreibt eine universelle Datenbasis als gemeinsame Grundlage für den Informationsaustausch (Kennwerte) zwischen Maschinenherstellern, Geräteherstellern, benannten Stellen und Anbietern von Berechnungstools im Bereich Funktionale Sicherheit. Wesentliche Merkmale sind:

- Definition der erforderlichen Informationen;
- eindeutige Beschreibung der Gerätedaten, unabhängig vom Hersteller;
- passend für den Maschinenbau, unabhängig von Branchen;
- unabhängig von physikalischen Schnittstellen, Berechnungstools, Übertragungsprotokollen, Datenbankformaten oder ähnlichen Faktoren.

Dieses VDMA-Einheitsblatt enthält keine sicherheitstechnischen Festlegungen.

Dieses VDMA-Einheitsblatt dient als Beitrag zur breitenwirksamen Anwendung des aktuellen technischen Entwicklungsstands auf dem Gebiet der Funktionalen Sicherheit. Es wird unter gemeinsamer Mitwirkung von Vertretern aller betroffenen Seiten weiterentwickelt und den allgemeinen Anforderungen des technischen Fortschritts ständig angepasst. Es ist daher nicht zulässig, von diesem Gemeinzwirk abweichende, proprietäre Datenformatkonzepte mit der in diesem VDMA-Einheitsblatt entwickelten universellen Datenbasis anzubieten. Vorschläge zur Verbesserung der universellen Datenbasis sind ausdrücklich erwünscht.

An der Erarbeitung dieses VDMA-Einheitsblattes waren Vertreter der Hersteller und Anwender von sicherheitsbezogenen Komponenten von Steuerungen sowie der Deutschen Gesetzlichen Unfallversicherung e.V. (DGUV, im Auftrag der Berufsgenossenschaften) beteiligt.

Die freie Verbreitung und Verwendung der im Anhang A referenzierten XML-Dateien ist ohne die Zustimmung des VDMA gestattet, nicht jedoch die Änderung, Ergänzung oder Bearbeitung.

Die im Anhang A referenzierten XML-Dateien können per E-Mail angefordert werden bei ea@vdma.org.

Änderungen

Gegenüber VDMA 66413:2012-07 wurden folgende Änderungen vorgenommen:

- a) Bild 1: Bei Geräte-Typ 4 wurde T_1 ergänzt.
- b) Abschnitt 5.2.2 – Erläuterung: „Es kann sein, dass der Gerätehersteller einen MTBF angibt ...“ MTBF geändert in MTTF.
- c) Abschnitt 5.2.3 – Erläuterung: Formel gemäß Norm korrigiert.
- d) Abschnitt 6.4.1.1 – Anmerkung 1: „... Device.PartNumber oder Device.Revision.“ geändert in „... Device.PartNumber und Device.Revision.“
- e) Tabelle 7: Für Geräte-Typ 2 die tabellarische Darstellung der Gruppierung MTTFD, LambdaD, MTTF MTBF geändert.
- f) Abschnitt 6.4.3.6: „Es wird empfohlen, mit den Kennwerten MTTF, MTBF oder B10D ...“ B10D geändert in B10.

Frühere Ausgaben

VDMA 66413:2012-07

Einleitung

Die unter der Maschinenrichtlinie 2006/42/EG harmonisierten Normen EN ISO 13849-1:2008, EN ISO 13849-2:2008 und EN 62061:2005 fordern Bewertungen und Berechnungen hinsichtlich der Wahrscheinlichkeit eines gefahrbringenden Ausfalls und systematischer Aspekte der Sicherheitsfunktionen einer Maschine (Funktionale Sicherheit).

ANMERKUNG Die Anforderungen der Prozessindustrie (IEC 61511) werden in diesem VDMA-Einheitsblatt nicht behandelt.

- Die Bewertungen und Berechnungen muss der Maschinenhersteller (als „Inverkehrbringer“) durchführen und nachweislich dokumentieren.
- Die relevanten Daten (Kennwerte) der in der Maschine eingesetzten sicherheitsbezogenen Geräte müssen und können ausschließlich die Gerätehersteller aus Sicht der Produkthaftung liefern.
- Die sicherheitstechnischen Berechnungen können mit Hilfe von Berechnungstools (Software-Programme) durchgeführt werden.

Die Anwendung der genannten Normen erfordert den Austausch der relevanten Daten zwischen allen Beteiligten: Maschinenherstellern, Geräteherstellern und Berechnungstools.

Gerätehersteller

erzeugen für ihre Geräte Kennwert-Bibliotheken im Format „Universelle Datenbasis“.

Als Gerätehersteller gilt derjenige, der Geräte und/oder Komponenten herstellt und im Sinne des freien Warenverkehrs dem Maschinenhersteller oder Verwender zur Verfügung stellt. Deshalb kann und darf nur der Gerätehersteller auch der Ersteller einer Kennwert-Bibliothek sein.

ANMERKUNG Das Bereitstellen der Kennwerte ist in Abschnitt 6 und 7 beschrieben.

Berechnungstool (-Anbieter)

stellen einen Importmechanismus für Kennwert-Bibliotheken im Datenbasis-Format bereit. Die Kennwerte werden für die Darstellung und Auswahl im Tool aufbereitet.

ANMERKUNG 1 Das Verwenden und Darstellen der Kennwerte ist in Abschnitt 6 und 7 beschrieben.

ANMERKUNG 2 Beispiele für bereits am Markt verfügbare Berechnungstools sind SISTEMA, Safety Evaluation Tool, PAScal.

Maschinenhersteller

nutzen die vom Gerätehersteller zur Verfügung gestellte Kennwert-Bibliothek (Datei), um die Kennwerte (Gerätedaten) im Berechnungstool einzulesen und zu aktualisieren.

ANMERKUNG Zum Verständnis der Kennwerte sind in Abschnitt 4 die Geräte-Typen beschrieben.

Anforderungen an die „Universelle Datenbasis“

- a) Anforderungen aus Sicht der Maschinenhersteller:
 - Für alle Berechnungstools sollen die Kennwerte aller Gerätehersteller zur Verfügung stehen.
 - Inhaltliche Transparenz der Kennwerte für Anwender.
 - Verständliche Zusatzinformationen für Anwender.
 - Kennwert-Bibliothek lesbar und editierbar mit Standard-PC Software.
 - Kennwert-Sätze vom Anwender weiter verwendbar, ohne zusätzliche Software, beispielsweise zur Archivierung oder zur Nutzung mit ERP-Systemen (Enterprise Resource Planning System).
- b) Anforderungen aus Sicht der Gerätehersteller:
 - Kennwerte nur einmal, in einer elektronischen Form bereitstellen, nutzbar in allen Berechnungstools.
 - Aufwand für das Bereitstellen der Kennwerte minimieren (zum Beispiel Export aus ERP-Systemen).
 - Für den „Importmechanismus“ der Berechnungstools sind die Anbieter der Tools verantwortlich: Die Importergebnisse und deren korrekte Weiterverarbeitung sollen nicht durch den Gerätehersteller geprüft werden müssen.
 - Die Kennwerte sollen allen Maschinenherstellern (Anwendern, Kunden) in einem einheitlichen Format, als Kennwert-Bibliothek zur Verfügung gestellt werden.
- c) Den Anforderungen der Berechnungstool-Hersteller soll das Format soweit wie möglich gerecht werden.

1 Anwendungsbereich

In diesem VDMA-Einheitsblatt werden

- Begriffe,
- Definitionen von Kennwerten und
- die einheitliche elektronische Darstellung (Datenformat)

für Komponenten oder Teile von Steuerungen im Umfeld der Funktionalen Sicherheit festgelegt. Diese Festlegung wird als Universelle Datenbasis bezeichnet.

Mit der Universellen Datenbasis soll es möglich sein, die Ausfallwahrscheinlichkeit von Sicherheitsfunktionen gemäß ISO 13849 und IEC 62061 berechnen zu können. Die Kenntnis der Normen wird vorausgesetzt.

Daraus ergeben sich neben den normativen Anforderungen an diese Universelle Datenbasis auch Anforderungen zur Beschreibung (eindeutige Auswahlkriterien) der Geräte, mit Hinblick auf eine bestmögliche Validierung.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 13849-1:2006, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

ISO 13849-2:2003, Safety of machinery – Safety-related parts of control systems – Part 2: Validation

IEC 61508:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 62061:2005, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems

ISO 639-1:2002, Codes for the representation of names of languages – Part 1: Alpha-2 code

3 Begriffe

Für die Anwendung dieses Dokumentes gelten die folgenden Begriffe.

3.1

Anwender

(en: **user**)

wird in diesem Dokument synonym verwendet für den Benutzer der Kennwerte, zum Beispiel Maschinenhersteller, Steuerungsbauer, Systemintegrator, und andere.

3.2

Anwendungsfall

(en: **use case**)

bestimmungsgemäße Verwendung des Gerätes

3.3

B₁₀

Mittlere Anzahl von Zyklen bis 10% der Bauteile ausgefallen sind

4 Definition der Geräte-Typen (DeviceType)

Die Geräte unterscheiden sich in Technologie und Anwendung sowie Verfügbarkeit und Nutzung von Diagnosemechanismen und -informationen. Deshalb werden an dieser Stelle vier Geräte-Typen definiert.

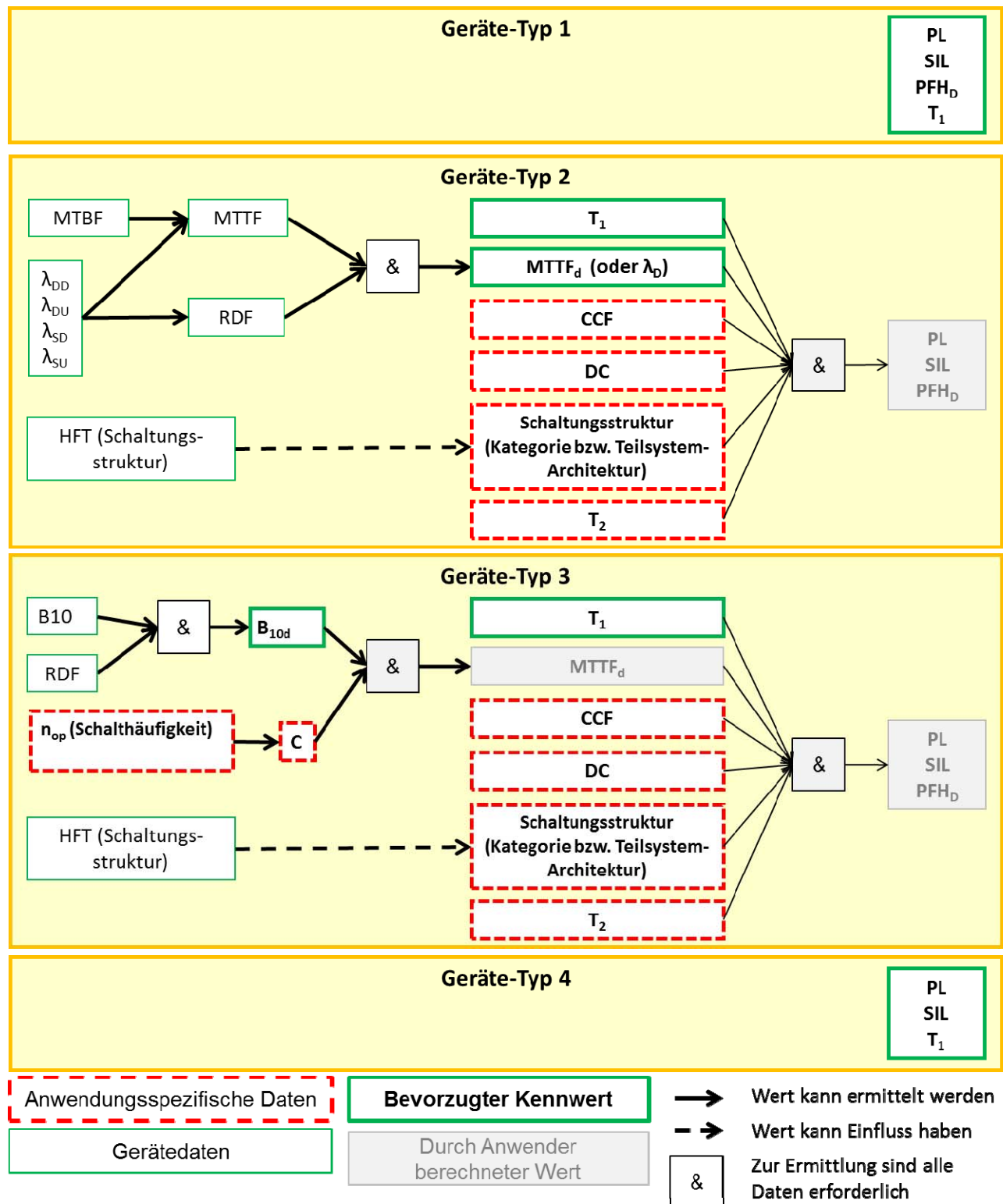


Bild 1 – Geräte-Typen und für die Berechnung notwendige Kennwerte

Die Geräte werden nach folgenden Merkmalen unterschieden:

- Gerät, das direkt als SRP/CS bzw. als Teilsystem (Teilelement) in einer Sicherheitsfunktion verwendet werden kann, weil der Hersteller das Gerät bereits für diesen Einsatzfall entwickelt hat (Geräte-Typ 1 und Geräte-Typ 4).
- Gerät, das erst durch den Entwurfsprozess des Anwenders als SRP/CS bzw. als Teilsystem (Teilelement) definiert und bewertet wird (Geräte-Typ 2 und Geräte-Typ 3).

ANMERKUNG 1 In einer Sicherheitsfunktion werden üblicherweise verschiedene Geräte-Typen verwendet.

ANMERKUNG 2 Die normativen Zusammenhänge sind in Abschnitt 5 beschrieben.

Bild 1 zeigt die unterschiedlichen Geräte-Typen mit den notwendigen Kennwerten zur Berechnung sowie den anwendungsspezifischen Daten.

4.1 Geräte-Typ 1

Der Geräte-Typ 1 hat den höchsten Integrationslevel. Typisch sind bereits entwickelte (en: pre-designed) Sicherheitsgeräte mit integrierter Diagnose. Dieser Typ ist im Rahmen der bestimmungsgemäßen Verwendung SIL- oder PL- klassifiziert. Die Klassifizierung wird vom Gerätehersteller angegeben.

Geräte dieses Typs sind gemäß Sicherheitsnormen (zum Beispiel IEC 61508) entwickelt.

ANMERKUNG 1 Beispiele für Geräte-Typ 1: Sicherheitslichtvorhang, Sicherheitslichtgitter, Komponenten sicherheitsgerichteter Steuerungen, sichere Antriebe/Antriebsfunktionen, Sicherheitsschaltgeräte

ANMERKUNG 2 Die Kenngrößen können von weiteren anwendungsspezifischen Daten (zum Beispiel Begrenzung der maximalen Schalthäufigkeit) abhängen.

4.2 Geräte-Typ 2

Zur Bewertung einer Sicherheitsfunktion durch den Anwender sind zusätzliche Anwendungsdaten (Schaltungsstruktur, Diagnosedeckungsgrad (DC) und die Betrachtung der Ausfälle infolge gemeinsamer Ursache (CCF)) erforderlich.

Geräte dieses Typs sind nicht zwangsläufig nach Sicherheitsnormen entwickelt, was einen Einsatz nach ISO 13849-1 oder IEC 62061 aber nicht ausschließt.

ANMERKUNG Beispiele für Geräte-Typ 2: nicht-sicherheitsgerichtete Elektronik, zum Beispiel Operationsverstärker, Näherungsschalter, Drucksensor, Hydraulikventil

4.3 Geräte-Typ 3

Geräte-Typ 3 sind Geräte mit einem Ausfallverhalten, das von der Schalthäufigkeit abhängig ist. Zur Bewertung einer Sicherheitsfunktion durch den Anwender sind zusätzliche Anwendungsdaten (Schalthäufigkeit, Betätigungshäufigkeit, Schaltungsstruktur, Diagnosedeckungsgrad (DC) und die Betrachtung der Ausfälle infolge gemeinsamer Ursache (CCF)) erforderlich.

Geräte dieses Typs sind nicht zwangsläufig nach Sicherheitsnormen entwickelt, was einen Einsatz nach ISO 13849-1 oder IEC 62061 aber nicht ausschließt.

ANMERKUNG Beispiele für Geräte-Typ 3: verschleißbehafte elektromechanische Komponenten, zum Beispiel Leistungsschütze, Schalter, Pneumatikventile, Verriegelungseinrichtungen, Befehlsgeräte

4.4 Geräte-Typ 4

Geräte-Typ 4 ist ein Sonderfall des Geräte-Typ 1. Dieser Geräte-Typ erscheint nicht in Abschnitt 5, da es für diesen Typ keine gefahrbringenden zufälligen Ausfälle gibt, das heißt die Wahrscheinlichkeit des gefahrbringenden Ausfalles $PFH_D = 0$ (nicht nur sehr klein). Bei Komponenten diesen Typs ist für jeden möglichen Fehler entweder:

- Fehlerausschluss gemäß IEC 62061 bzw. ISO 13849-2
oder

- Fehler führt immer zum sicheren Zustand.

Sofern strukturelle Anforderungen (siehe IEC 62061, Kap. 6.7.7.2) oder andere Betrachtungen eine Beschränkung der alleinigen (einkanaligen) Verwendung vorsehen, ist die Angabe eines maximal erreichbaren PL und SIL für die einkanalige Verwendung erforderlich.

Um die oben genannten Aussagen treffen zu können ist eine Bewertung der Geräte gemäß Sicherheitsnormen (zum Beispiel IEC 61508) erforderlich.

4.5 Kennwerte der Geräte-Typen

Tabelle 1 – Geräte-Typen und für die Berechnung notwendige Kennwerte

Kennwert	Geräte-Typ (DeviceTyp)				Kommentar
	1	2	3	4	
PL	x			x	ISO 13849-1
SILCL	x			x	IEC 62061
PFH _D	x				ISO 13849-1 und IEC 62061
Kategorie	x			x	ISO 13849-1
MTTF _d		x			ISO 13849-1 und IEC 62061 Genau einer der Kennwerte ist erforderlich. Vorzugsweise der MTTF _d .
λ _D		x			
MTTF		x			
MTBF		x			
RDF		o	o		ISO 13849-1 und IEC 62061
B _{10d}			x		ISO 13849-1 und IEC 62061 Genau einer der Kennwerte ist erforderlich. Vorzugsweise der B _{10d} -Wert.
B ₁₀			x		
T _M = T ₁	x	x	x	x	ISO 13849-1 und IEC 62061
ANMERKUNG x = Muss-Feld, Angabe erforderlich, o = Kann-Feld, Angabe optional (anwendungsspezifisch)					

5 Anforderungen

Bei der Anwendung der Normen der Funktionalen Sicherheit ergeben sich normative Anforderungen an die verwendeten Geräte.

Darüber hinaus werden zur eindeutigen Beschreibung eines Gerätes Informationen benötigt.

5.1 Anforderungen der ISO 13849-1

5.1.1 Anwendung Geräte-Typ 1

Verwendung verschiedener Geräte, die durch den Gerätehersteller bereits als fertig verwendbares SRP/CS entwickelt wurden (siehe Begriffe 3.25 „bereits entwickeltes Teilsystem“).

Die Sicherheitsfunktion lässt sich auf Basis der Daten der Gerätehersteller bewerten.

Beispiele:

Eine Schutztür wird mit einem sicherheitsgerichteten berührungslosen Positionsschalter überwacht. Wenn die Schutztür geöffnet wird, dann soll über eine fehlersichere Steuerung eine sicher begrenzte Geschwindigkeit (SLS) eines sicherheitsgerichteten Frequenzumrichters ausgelöst werden.

Ein Lichtvorhang soll bei Unterbrechung der Lichtstrahlen über eine fehlersichere Steuerung ein sicheren Halt (STO) eines sicherheitsgerichteten Frequenzumrichters auslösen, damit eine gefahrbringende Bewegung beendet wird.

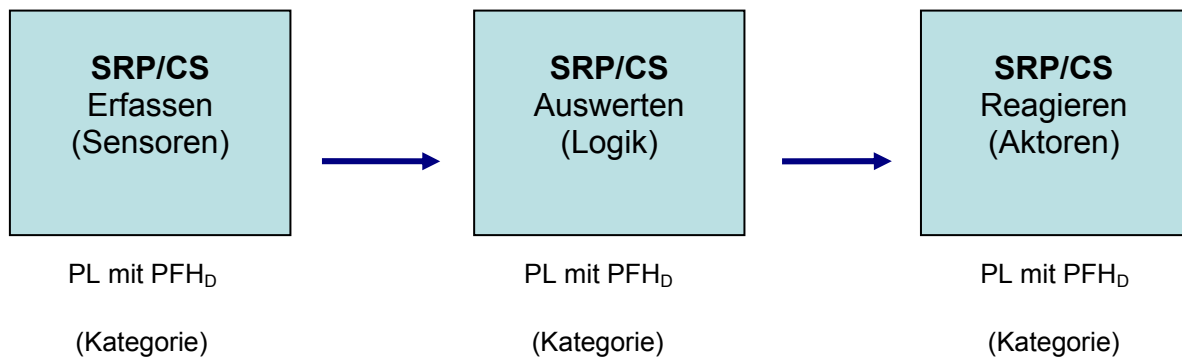


Bild 2 – Geräte-Typ 1 (ISO 13849-1)

Der höchst möglich erreichbare PL einer Sicherheitsfunktion wird begrenzt durch

- den niedrigsten PL aller SRP/CSen und
- die PFH_D der Sicherheitsfunktion, ermittelt durch die Addition der PFH_D aller SRP/CSen.

Erläuterung:

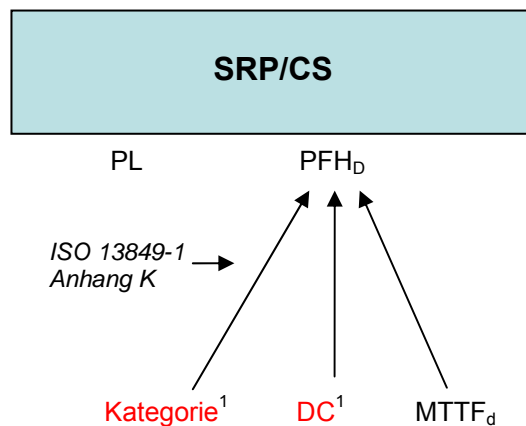
Der PL und die PFH_D sind Angaben des Geräteherstellers.

5.1.2 Anwendung Geräte-Typ 2

Verwendung verschiedener Geräte, die durch den Anwender als SRP/CS eigenverantwortlich bewertet werden. Eine Angabe des PL und PFH_D ist auf Geräte-Ebene nicht möglich. Der Gerätehersteller liefert einen $MTTF_d$ oder einen MTBF für die Geräte. Der Anwender definiert anwendungsspezifisch das SRP/CS durch den gewählten Aufbau bzw. Entwurf (Kategorie als ausgewählte vorgesehene Architektur und DC). Auf dieser Basis kann ein PL und PFH_D für das SRP/CS ermittelt werden. In einer Sicherheitsfunktion wird dieses SRP/CS dann als ein Teil der Sicherheitsfunktion verwendet.

Beispiel:

Redundante (2-kanalige) Verwendung von zwei Hydraulik-Ventilen als SRP/CS (Aktoren) in einer Sicherheitsfunktion; die Bewertung erfolgt auf Basis einer Kategorie 3 und einem DC von 90%.



¹ Die Angaben in roter Schriftfarbe (Kategorie und DC) sind durch den Anwender zu definieren.

Bild 3 – Geräte-Typ 2 (ISO 13849-1)

Erläuterung:

Es kann sein, dass der Gerätehersteller einen MTTF angibt oder lediglich ein MTBF für die Geräte vorliegt. Es muss dann ein $MTTF_d$ von diesem MTBF abgeleitet werden. Es kann vereinfacht angenommen werden, dass $MTTF \approx MTBF$ ist.

Der Anteil gefahrbringender Ausfälle sollte eine zusätzliche Information des Geräteherstellers sein.

In den Normen wird für elektronische Geräte als Ansatz ein Anteil von 50% gefahrbringender Ausfälle genannt (gemäß IEC 61508) wenn keine Herstellerangaben für das Gerät vorliegen.

Als ‚worst case‘ kann ein Anteil von 100% gefahrbringender Ausfälle angenommen werden.

Daraus ergibt sich $MTTF_d \approx 2 \times MTTF$ (elektronisch) bzw. $MTTF_d \approx MTTF$ (‚worst case‘).

Die Ermittlung der PFH_D erfolgt mit Hilfe des informativen Anhangs K und den Eingangsgrößen Kategorie, DC und $MTTF_d$.

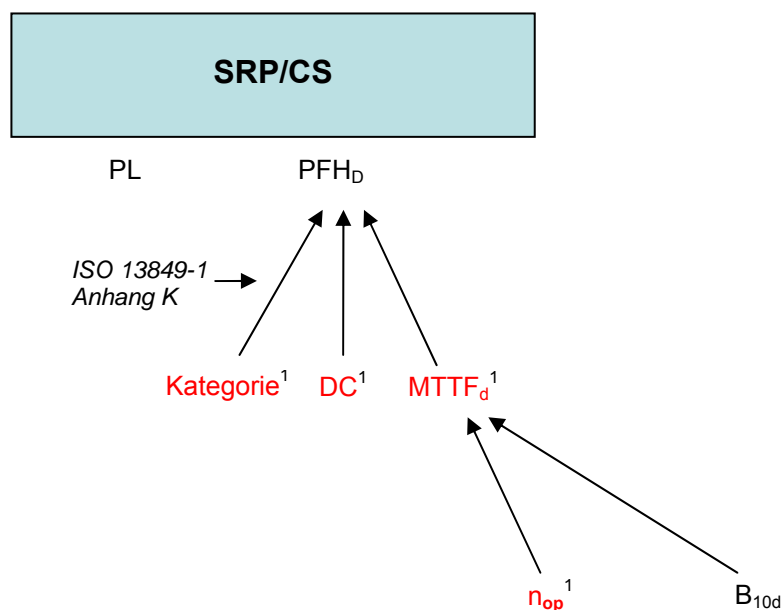
ANMERKUNG Für bestimmte Kategorien müssen zusätzliche Anforderungen erfüllt werden, wie zum Beispiel CCF.

5.1.3 Anwendung Geräte-Typ 3

Verwendung verschiedener Geräte, die durch den Anwender als SRP/CS eigenverantwortlich bewertet werden. Eine Angabe des PL und PFH_D ist auf Geräte-Ebene nicht möglich. Der Gerätehersteller liefert keinen $MTTF_d$ für die Geräte, da es sich um verschleißbehafte Geräte handelt. Der $MTTF_d$ kann nur auf Basis des B_{10d} -Wertes (Angabe des Geräteherstellers) und der applikationsabhängigen Betätigungszyklen pro Jahr (n_{op} , Angabe des Anwenders) ermittelt werden. Der Anwender definiert das SRP/CS durch den gewählten Aufbau bzw. Entwurf (Kategorie als ausgewählte vorgesehene Architektur und DC). Auf dieser Basis kann ein PL und PFH_D für das SRP/CS ermittelt werden. In einer Sicherheitsfunktion wird dieses SRP/CS dann als ein Teil der Sicherheitsfunktion verwendet.

Beispiel:

Redundante (2-kanalige) Verwendung von zwei Positionsschaltern als SRP/CS (Sensoren) in einer Sicherheitsfunktion; die Bewertung erfolgt auf Basis einer Kategorie 4 und einem DC von 99%.



¹ Die Angaben in roter Schriftfarbe (Kategorie, DC, $MTTF_d$ und n_{op}) sind durch den Anwender zu definieren.

Bild 4 – Geräte-Typ 3 (ISO 13849-1)

Erläuterung:

Die Ermittlung des $MTTF_d$ erfolgt auf Basis von B_{10d} und n_{op} .

$$MTTF_d = \frac{B_{10d}}{0,1 \times n_{op}}, \text{ mit den Betätigungen pro Jahr } n_{op}.$$

In den Normen wird für verschleißbehafte Geräte als Ansatz ein Anteil von 50% gefahrbringender Ausfälle genannt (gemäß ISO 13849-1) wenn keine Herstellerangaben für das Gerät vorliegen.

Daraus ergibt sich $B_{10d} \approx 2 \times B_{10}$.

Die Ermittlung der PFH_D erfolgt auf Basis des informativen Anhangs K und den Eingangsgrößen Kategorie, DC und $MTTF_d$.

ANMERKUNG für bestimmte Kategorien müssen zusätzliche Anforderungen erfüllt werden, wie zum Beispiel CCF.

5.2 Anforderungen der IEC 62061

5.2.1 Anwendung Geräte-Typ 1

Verwendung verschiedener Geräte, die durch den Gerätehersteller bereits als fertig verwendbares Teilsystem entwickelt wurden (siehe Begriffe 3.25 „bereits entwickeltes Teilsystem“).

Die Sicherheitsfunktion lässt sich auf Basis der Daten der Gerätehersteller bewerten.

Beispiele:

Eine Schutztür wird mit einem sicherheitsgerichteten berührungslosen Positionsschalter überwacht. Wenn die Schutztür geöffnet wird, dann soll über eine fehlersichere Steuerung eine sicher begrenzte Geschwindigkeit (SLS) eines sicherheitsgerichteten Frequenzumrichters ausgelöst werden.

Ein Lichtvorhang soll bei Unterbrechung der Lichtstrahlen über eine fehlersichere Steuerung ein sicheren Halt (STO) eines sicherheitsgerichteten Frequenzumrichters auslösen, damit eine gefahrbringende Bewegung beendet wird.

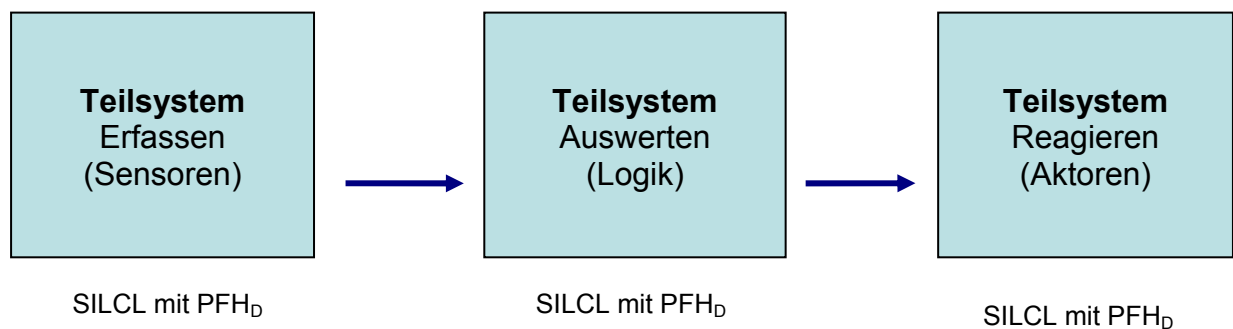


Bild 5 – Geräte-Typ 1 (IEC 62061)

Der höchst möglich erreichbare SIL einer Sicherheitsfunktion wird begrenzt, durch

- den niedrigsten SILCL aller Teilsystem und
- die PFH_D der Sicherheitsfunktion, ermittelt durch die Addition der PFH_D aller Teilsysteme.

Erläuterung:

Der SILCL und die PFH_D sind Angaben des Geräteherstellers.

Die Betriebs- bzw. Montageanleitung des Gerätes enthält konkrete Angaben zur Verwendbarkeit und zur Montage des Gerätes sowie zu den Betriebsbedingungen, unter denen das Gerät in Sicherheitsfunktionen eingesetzt werden darf.

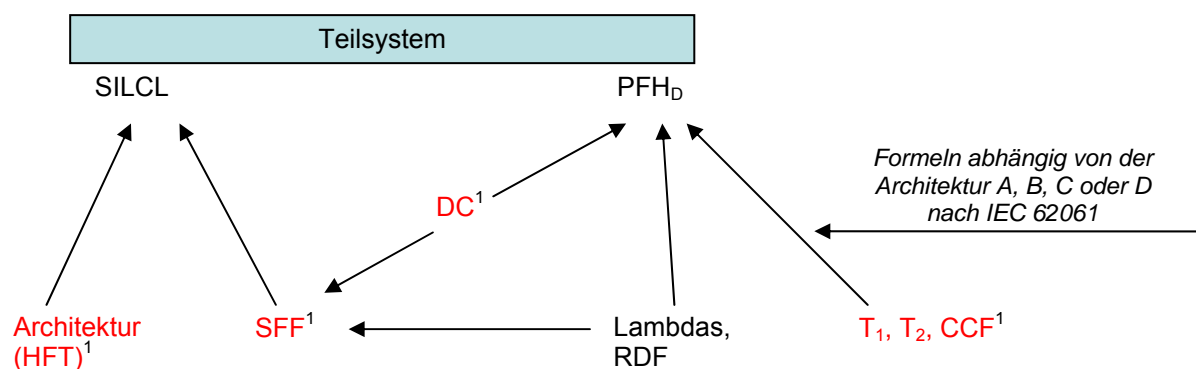
Der Maschinenhersteller kann die sicherheitstechnischen Angaben des Geräteherstellers als Nachweis des erreichten Schutzniveaus für die beschriebene Sicherheitsfunktion ohne weitere Berechnungen verwenden.

5.2.2 Anwendung Geräte-Typ 2

Verwendung verschiedener Geräte, die durch den Anwender als Teilsystem eigenverantwortlich bewertet werden. Eine Angabe des SIL und PFH_D ist auf Geräte-Ebene nicht möglich. Der Gerätehersteller liefert einen $MTTF_d$, λ_D oder einen MTBF für die Geräte. Der Anwender definiert anwendungsspezifisch das Teilsystem durch den gewählten Aufbau bzw. Entwurf (1- oder 2-kanalige Architektur als HFT gleich 0 oder 1 und DC). Auf dieser Basis kann ein SILCL und PFH_D für das Teilsystem ermittelt werden. In einer Sicherheitsfunktion wird dieses Teilsystem dann als ein Teil der Sicherheitsfunktion verwendet.

Beispiel:

Redundante (2-kanalige) Verwendung von zwei Stromüberwachungsrelais als Teilsystem (Sensoren) in einer Sicherheitsfunktion. Die Bewertung erfolgt auf Basis einer Architektur mit HFT von 1 und einem DC von 90%.



¹ Die Angaben in roter Schriftfarbe (Architektur (HFT), DC, SFF, T₁, T₂ und CCF) sind durch den Anwender zu definieren.

Bild 6 – Geräte-Typ 2 (IEC 62061)

Erläuterung:

Es gilt immer: $\lambda_D = RDF \times \lambda$.

Bei elektronische Komponenten gilt zusätzlich $\lambda = \frac{1}{MTTF \times 8760}$ oder $\lambda_D = \frac{1}{MTTF_d \times 8760}$.

Es kann sein, dass der Gerätehersteller einen MTTF angibt oder lediglich ein MTBF für die Geräte vorliegt. Es muss dann ein $MTTF_d$ von diesem MTBF abgeleitet werden. Es kann vereinfacht angenommen werden, dass $MTTF \approx MTBF$ ist.

Der Anteil gefahrbringender Ausfälle sollte eine zusätzliche Information des Geräteherstellers sein.

In den Normen wird für elektronische Geräte als Ansatz ein Anteil von 50% gefahrbringender Ausfälle genannt (gemäß IEC 61508) wenn keine Herstellerangaben für das Gerät vorliegen.

Als ‚worst case‘ kann ein Anteil von 100% gefahrbringender Ausfälle angenommen werden.

Daraus ergibt sich $MTTF_d \approx 2 \times MTTF$ (elektronisch) bzw. $MTTF_d \approx MTTF$ (‚worst case‘).

Die Ermittlung der PFH_D erfolgt mit Hilfe der normativen Formeln und den Eingangsgrößen Architektur (HFT), T₁, T₂, CCF, DC und λ_D .

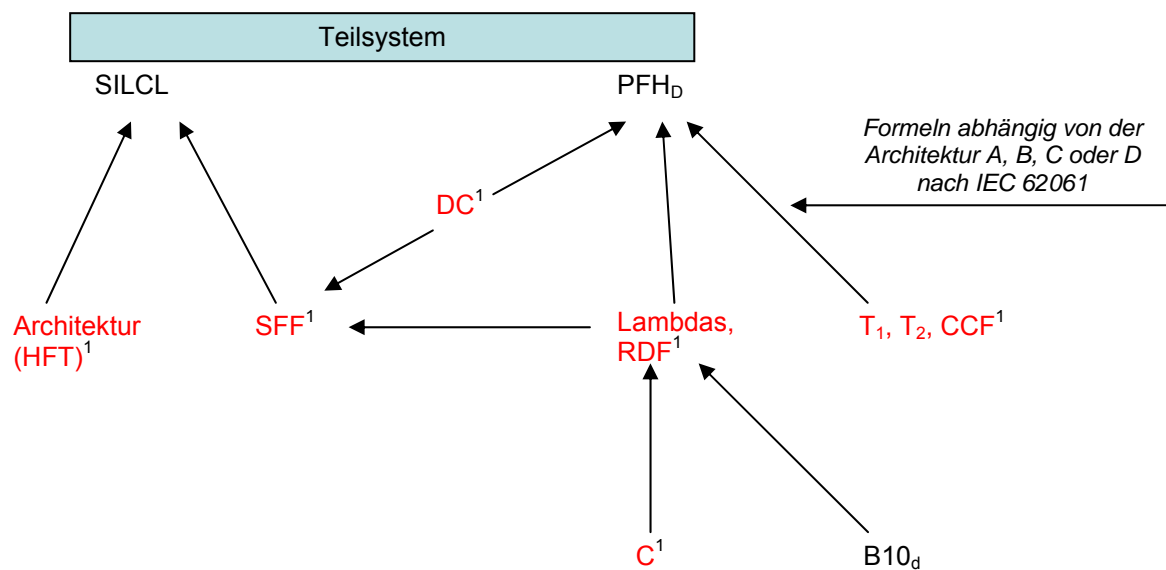
Die SILCL wird auf Basis des SFF und der Architektur (HFT) ermittelt.

5.2.3 Anwendung Geräte-Typ 3

Verwendung verschiedener Geräte, die durch den Anwender als Teilsystem eigenverantwortlich bewertet werden. Eine Angabe des SIL und PFH_D ist auf Geräte-Ebene nicht möglich. Der Gerätehersteller liefert keinen MTTF_d oder λ_D für die Geräte, da es sich um verschleißbehaftete Geräte handelt. Das Lambda λ_D kann nur auf Basis des B_{10d} -Wertes und des Anteil gefahrbringender Ausfälle oder des B_{10d} -Wertes (Angabe des Geräteherstellers) und der applikationsabhängigen Betätigungszyklen pro Stunde oder pro Jahr (C bzw. n_{op} , Angabe des Anwenders) ermittelt werden. Der Anwender definiert das Teilsystem durch den gewählten Aufbau bzw. Entwurf (1- oder 2-kanalige Architektur als HFT gleich 0 oder 1 und DC). Auf dieser Basis kann ein SIL und PFH_D für das Teilsystem ermittelt werden. In einer Sicherheitsfunktion wird dieses Teilsystem dann als ein Teil der Sicherheitsfunktion verwendet.

Beispiel:

Redundante (2-kanalige) Verwendung von zwei Leistungsschützen als Teilsystem (Aktoren) in einer Sicherheitsfunktion. Die Bewertung erfolgt auf Basis einer Architektur mit HFT von 1 und einem DC von 99%.



¹ Die Angaben in roter Schriftfarbe (Architektur (HFT), DC, C, SFF, Lambdas, RDF, T1, T2 und CCF) sind durch den Anwender zu definieren.

Bild 7 – Geräte-Typ 3 (IEC 62061)

Erläuterung:

$$B10_d = \frac{B10}{RDF}$$

$$\lambda = \frac{0,1 \times C}{B10} \text{ oder } \lambda_D = \frac{0,1 \times C}{B10_d}, \text{ mit } C = \text{Betätigungen pro Stunde.}$$

Mit $C = n_{op} \times \frac{1}{365 \times 24}$ ist die Beziehung zu Betätigungen pro Jahr n_{op} der ISO 13849-1 definiert.

Die Ermittlung der PFH_D erfolgt mit Hilfe der normativen Formeln und den Eingangsgrößen Architektur (HFT), T_1 , T_2 , CCF, DC und λ_D .

SILCL wird auf Basis des SFF und der Architektur (HFT) ermittelt.

6 Kennwert-Bibliothek

6.1 Datenstruktur

Die Informationen werden wie folgt strukturiert (siehe Bild 8):

- **VDMA66413** (Main-Entity) – Angaben zum Datenbasis-Format (siehe 6.2)
- **Manufacturer** – Angaben zum Gerätehersteller (siehe 6.3)
- **Device** – Angaben zum Gerät (siehe 6.4.1)
- **UseCase** – Angaben zum Anwendungsfall (siehe 6.4.2)
- **DeviceType1..4** – Kennwerte (siehe 6.4.3)
- **Language** – Sprachtexte (siehe 6.5)

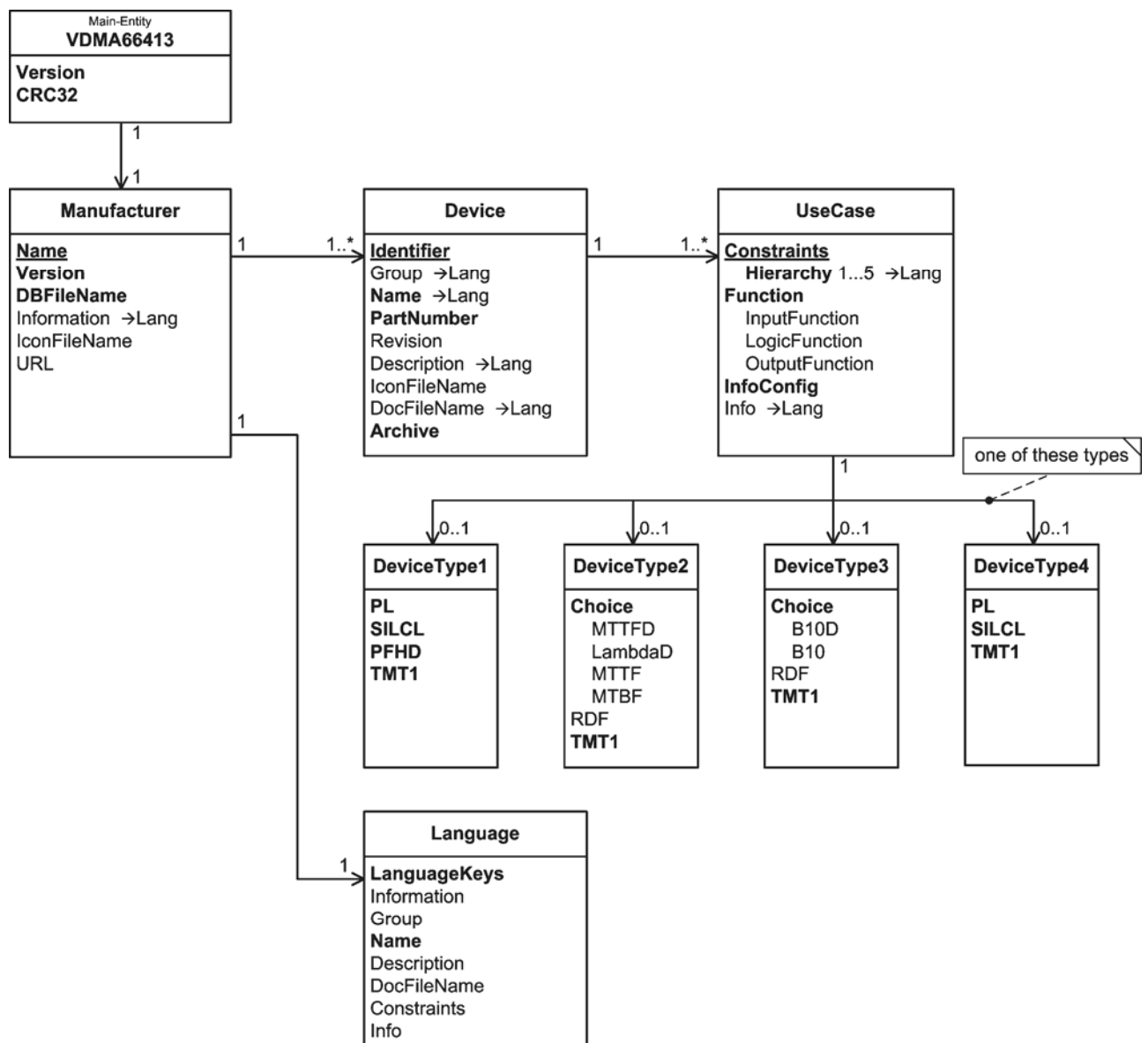


Bild 8 – Datenstruktur der Kennwert-Bibliothek (Entity Relationship Modell der Datenbasis)

Anhang A

Dateien für die Anwendung

A.1 XML-Schema-Datei Kennwert-Bibliothek

VDMA66413_2012-07_XML-Schema.xsd

Das XML-Schema definiert die formal korrekte Struktur und Syntax der Kennwert-Bibliothek.

Das XML-Schema enthält zusätzliche strukturell notwendige Konstrukte, auf die im VDMA-Einheitsblatt nicht eingegangen wird.

Das XML-Schema wird verwendet, um die Kennwert-Bibliothek auf formale Fehlerfreiheit zu prüfen.

ANMERKUNG Inhalte und komplexe Verknüpfungen können mit dem XML-Schema nicht geprüft werden. Das XML-Schema ersetzt nicht den Freigabeprozess, Validierung der Kennwerte.

A.2 XML-Beispiel-Datei Kennwert-Bibliothek

VDMA66413_2012-07_XML-Beispiel.xml

Die Beispiel-Datei enthält einige syntaktisch korrekt beschriebene, jedoch fiktive Geräte.

A.3 XML-Schema-Datei Sprach-Bibliothek

VDMA66413_2012-07_Language_XML-Schema.xsd

Das XML-Schema definiert die formal korrekte Struktur und Syntax der Sprach-Bibliothek.

Das XML-Schema enthält zusätzliche strukturell notwendige Konstrukte, auf die im VDMA-Einheitsblatt nicht eingegangen wird.

Das XML-Schema wird verwendet, um die Sprach-Bibliothek auf formale Fehlerfreiheit zu prüfen.

ANMERKUNG Inhalte und komplexe Verknüpfungen können mit dem XML-Schema nicht geprüft werden. Das XML-Schema ersetzt nicht den Freigabeprozess.

A.4 XML-Beispiel-Datei Sprach-Bibliothek

VDMA66413_2012-07_Language_XML-Beispiel.xml

Die Beispiel-Datei enthält einige syntaktisch korrekte, jedoch fiktive Sprachtexte.