VDMA 66413

ICS 21.020; 35.240.50

Supersedes
VDMA 66413:2012-07

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

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

Document comprises 43 pages

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

Contents

Foreword

This document describes a universal data format as a common base for the exchange of information (characteristic values) between machine manufacturers, device manufacturers, notified bodies and suppliers of calculation tools in the field of functional safety. Key features include:

– Definition of the required information;

– Unambiguous description of device data, independent of the manufacturer;

– Suitable for engineering, independent of industry sector;

– Independent of physical interfaces, calculation tools, communication protocols, database system formats or similar factors.

This VDMA Specification does not contain safety relevant specifications.

This VDMA Specification serves a contribution to a generic application of the actual state of technology in field of functional safety. It will be further developed under the joint effort of representatives of all involved parties and will be continuously adopted to the technical progress and its need. It is therefore not allowed to offer concepts of data formats with the universal data format of this VDMA Specification, which is deviating from this general purpose. Proposals on how to improve the universal data format are explicitly welcome.

The generation of this VDMA Specification involved representatives of manufacturers and users of safety related parts of control systems as well as the Deutschen Gesetzlichen Unfallversicherung e.V. (DGUV, im Auftrag der Berufsgenossenschaften).

The XML files referenced in Annex A may be requested via E-Mail from ea@vdma.org.

Amendments

This VDMA Specification differs from VDMA 66413:2012-07 as follows:

a) Figure 1: T_1 added for Device type 4.

b) Clause 5.2.2 – Explanation: „The device manufacturer may specify an MTBF …“ – MTBF replaced by MTTF.

c) Clause 5.2.3 – Explanation: Formula modified according to the standard.

d) Clause 6.4.1.1 – Note 1: „… Device.PartNumber or Device.Revision.“ replaced by „… Device.PartNumber and Device.Revision.“

e) Table 7: Tabular representation of the group MTTFD, LambdaD, MTTF, MTBF for Device type 2 modified.

f) Clause 6.4.3.6: „With the characteristic values MTTF, MTBF or B10D …“ – B10D replaced by B10.

Previous editions

VDMA 66413:2012-07

Introduction

The standards EN ISO 13849-1:2008, EN ISO 13849-2:2008 and EN 62061:2005 are harmonised under the Machinery Directive 2006/42/EC and call for assessments and calculations regarding the probability of a dangerous failure and systematic aspects of a machine's safety functions (functional safety).

NOTE This VDMA Specification does not cover the requirements of the process industry (IEC 61511).

– The machine manufacturer (as the "person placing the product on the market") must perform these assessments and calculations and provide documentary evidence.
– The relevant data (characteristic values) for the safety-related devices used in the machine shall and indeed can only be provided by the device manufacturers from a product liability perspective.
– The safety-related calculations may be made using calculation tools (software programs).

Application of the named standards requires the exchange of relevant data between all concerned: machine manufacturers, device manufacturers and calculation tools.

Device manufacturers

create characteristic value libraries for their devices in “universal data format".

The device manufacturer is the person who manufactures devices and/or components and makes them available to the machine manufacturer or user in the spirit of the free movement of goods. As a result, the creater of a characteristic value library can and indeed may only be the device manufacturer.

NOTE The provision of characteristic values is described in Clause 6 and 7.

Calculation tool (suppliers)

provide a mechanism for importing characteristic value libraries in database format. The characteristic values are prepared for display and selection within the tool.

NOTE 1 The use and display of characteristic values is described in Clause 6 and 7.

NOTE 2 Examples of calculation tools already available on the market include SISTEMA, Safety Evaluation Tool, PASCal.

Machine manufacturers

use the characteristic values library (file) provided by the device manufacturer to read and update the characteristic values (device data) within the calculation tool.

NOTE The device types are described in Clause 4 to aid understanding of the characteristic values.

Requirements of the “universal data format”

a) Requirements from a machine manufacturer’s perspective:
– The characteristic values from all device manufacturers should be available for all calculation tools.
– Characteristic values should be transparent for users in terms of content.
– Understandable, additional information for users.
– Ability to read and edit the characteristic value library using standard PC software.
– Ability to reuse sets of characteristic values, without additional software; for example: for archiving purposes or for use with ERP systems (Enterprise Resource Planning).

b) Requirements from a device manufacturer’s perspective:
– To provide characteristic values just once in a single electronic format, which can be used in all calculation tools.
– Minimise the work involved in providing characteristic values (e.g. export from ERP systems).
– Tool suppliers responsible for the mechanism used to import the calculation tool: The device manufacturer should not have to check the import results and whether these have been processed correctly.
– Characteristic values should be provided to all machine manufacturers (users, customers) in one standard format, as a characteristic value library.

c) As far as possible, the database format should meet the needs and requirements of the calculation tool.

1 Scope

This VDMA Specification determines

– Terms and definitions,

– definitions of characteristic values and

– the standardised electronic format

for components or parts of control systems in the field of functional safety.
This is described as a universal data format.

The universal data format should enable the probability of failure of safety functions to be calculated in accordance with ISO 13849 and IEC 62061. Familiarity with the standards is assumed.

These provide the normative requirements of this universal data format as well as the requirements for the device description (clear selection criteria), with regard to best possible validation.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
User
(de**: Anwender)**

Used in this document to describe the person using the characteristic values, e.g. machine manufacturer, control system designer, system integrator, etc.

3.2
Use case
(de**: Anwendungsfall)**

Intended use of the device

3.3
B_{10}

The mean number of cycles until 10% of the components fail

3.4
$B10_d$

The mean number of cycles until 10% of the components fail dangerously

[ISO 13849-1, C.4.2]

3.5
CCF
Common Cause Failure
(de**: Ausfall in Folge gemeinsamer Ursache)**

Failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel (redundant architecture) subsystem, leading to failure of a SRECS

NOTE This definition differs from that given in ISO 12100 and IEV 191-04-23.

[IEC 62061, 3.2.43]

3.6
DB
Database
(de**: Datenbasis)**

Defined structure for the collection of data

3.7
DC
Diagnostic Coverage
(de**: Diagnosedeckungsgrad)**

Measure for the effectivity of diagnostics, may be determined as ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures

[ISO 13849-1, 3.1.26]

3.8
Device
(de**: Gerät)**

Used in this document synonymously for: part, component, subsystem, subsystem element or safety-related part of a control system (SRP/CS)

NOTE The term "device" is not taken from the standards

3.9
HFT
Hardware fault tolerance
(de**: Fehlertoleranz)**

Ability of a SRECS, a subsystem or subsystem element to continue to perform a required function in the presence of faults or failures

[IEC 62061, 3.2.31]

4 Definition of device types

Devices vary in terms of technology, application, availability and use of diagnostic mechanisms and diagnostic information. As a result, different device types will be defined at this point.

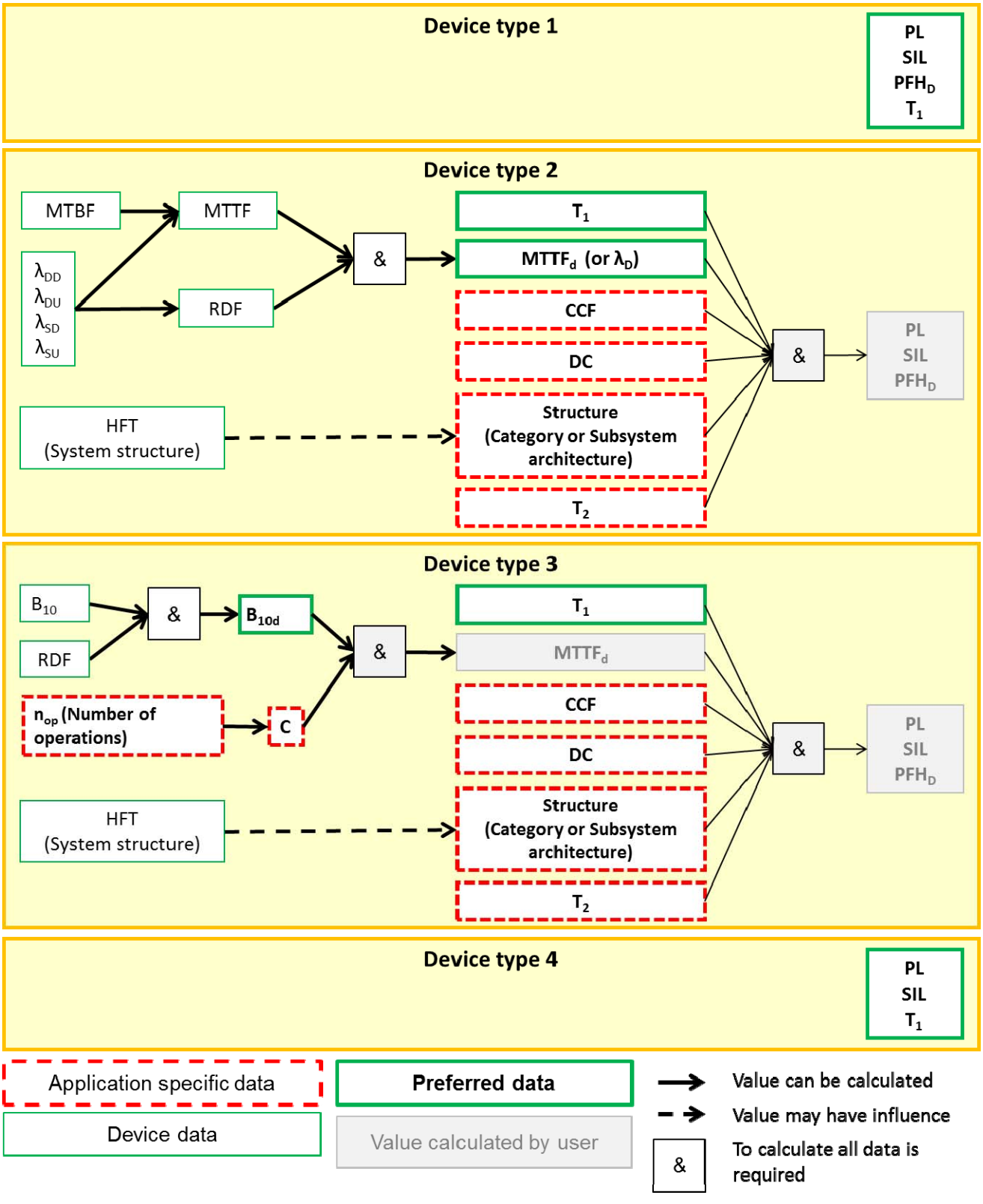


Figure 1 – Device types and characteristic values necessary for the calculation

Devices can generally be distinguished by the following features:

– Device that can be used directly as a SRP/CS or subsystem (subelement) in a safety function because the manufacturer has already developed the device for this specific application (device type 1 and device type 4).

– Device that is only defined and assessed as a SRP/CS or subsystem (subelement) through the user's design process (device type 2 and device type 3).

NOTE 1 A safety function normally uses a variety of device types.

NOTE 2 The normative relationships are described in Clause 5.

Figure 1 illustrates the different device types with the characteristic values necessary for the calculation as well as application-specific data.

4.1 Device type 1

Device type 1 has the highest integration level. Pre-designed safety systems with integrated diagnostics are typical. This type is SIL or PL-classified in line with the intended use. The classification is specified by the device manufacturer.

Devices of this type are developed in accordance with safety standards (e.g. IEC 61508).

NOTE 1 Examples for device type 1: Safety light curtain, safety light grid, safety-related control system components, safe drives/drive functions, safety relays

NOTE 2 Parameters may depend on other application-specific data (e.g. limitation of the maximum switching frequency).

4.2 Device type 2

Additional application data (circuit structure, diagnostic coverage (DC) and consideration of common cause failure (CCF)) are needed in order for the user to assess a safety function.

Devices of this type are not necessarily developed in accordance with safety standards; however, this does not exclude application in accordance with ISO 13849-1 or IEC 62061.

NOTE Examples for device type 2: Non-safety-related electronics, e.g. operational amplifier, proximity switch, pressure sensor, hydraulic valve

4.3 Device type 3

Type 3 devices are devices with a failure mode, which depends on the operating cycles. Additional application data (number of operations, number of activations, circuit structure, diagnostic coverage (DC) and consideration of common cause failure (CCF)) are needed in order for the user to assess a safety function.

Devices of this type are not necessarily developed in accordance with safety standards; however, this does not exclude application in accordance with ISO 13849-1 or IEC 62061.

NOTE Examples for device type 3: Electromechanical components that are subject to wear, e.g. power contactors, switches, pneumatic valves, interlocking devices, control devices

4.4 Device type 4

Device type 4 is a special case of device type 1. This device type does not appear in Clause 5 because for this type there are non random failures which lead to a dangerous fault, this means the probability of a dangerous fault occurring $PFH_D = 0$ (not just very low!). For components of this type, one of the following applies for each potential fault, either:

– Fault exclusion is in accordance with IEC 62061 / ISO 13849-2

or

– Fault always leads to a safe condition.

Where architectural requirements (see IEC 62061, Clause 6.7.7.2) or other considerations impose a restriction on sole (single-channel) use, a maximum achievable PL and SIL must be specified for single-channel use.

In order to provide the above information, devices must be assessed in accordance with safety standards (e.g. IEC 61508).

4.5 Characteristic values of device types

Table 1 – Device types and characteristic values necessary for the calculation

Character-istic value	DeviceTyp				Comment
	1	2	3	4	
PL	**X**			**X**	ISO 13849-1
SILCL	**X**			**X**	IEC 62061
PFH_D	**X**				ISO 13849-1 and IEC 62061
Category	**X**			**X**	ISO 13849-1
$MTTF_d$		**X**			ISO 13849-1 and IEC 62061 Exactly one of the characteristic values is required. Preferably $MTTF_d$.
λ_D		**X**			
MTTF		**X**			
MTBF		**X**			
RDF		**O**	**O**		ISO 13849-1 and IEC 62061
B_{10d}			**X**		ISO 13849-1 and IEC 62061 Exactly one of the characteristic values is required. Preferably the B_{10d} value.
B_{10}			**X**		
$T_M = T_1$	**X**	**X**	**X**	**X**	ISO 13849-1 and IEC 62061
NOTE **x** = Mandatory field, data required, **o** = Optional field, data optional (application-specific)					

5 Requirements

Application of the functional safety standards provides the normative requirements of the devices in use.

Information is also needed to obtain a unique description of a device.

5.1 Requirements of ISO 13849-1

5.1.1 Device type 1 application

Use of a variety of devices, which have been pre-designed by the device manufacturer as a ready-to-use SRP/CS (see term 3.25 "Pre-designed subsystem").

The safety function can be assessed based on the data from the device manufacturer.

Examples:

A guard door is monitored using a safety-related non-contact position switch. If the guard door is opened, a safely limited speed (SLS) should be triggered for the safety-related frequency converter via a failsafe control system.

A light curtain is to trigger a safe stop (STO) of a safety-related frequency converter via a failsafe control system if the light beams are interrupted, in order to shut down a hazardous movement.

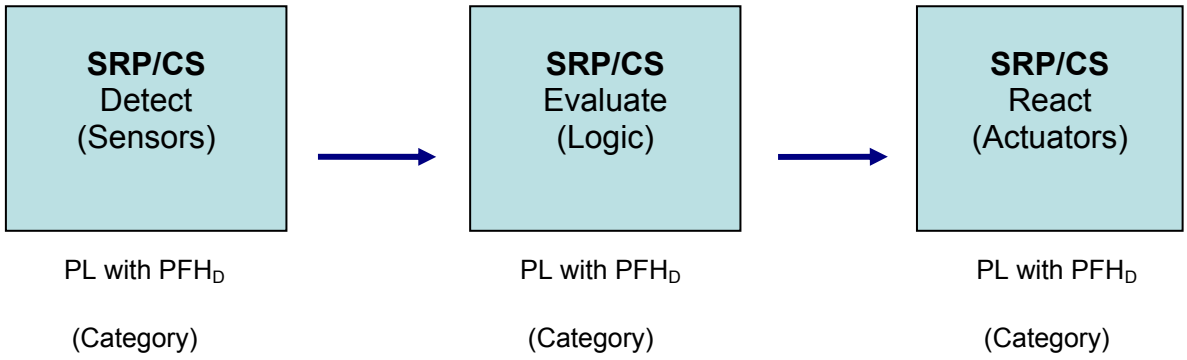


Figure 2 – Device type 1 (ISO 13849-1)

The highest possible PL that a safety function can achieve is limited by

– the lowest PL of all SRP/CSs and

– the PFH_D of the safety function, determined by adding the PFH_D of all SRP/CSs.

Explanation:

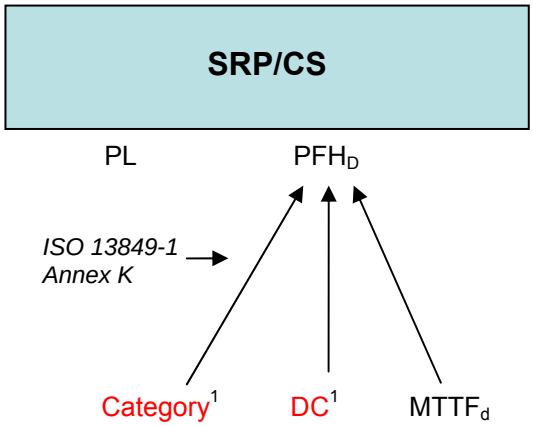
The PL and PFH_D are specified by the device manufacturer.

5.1.2 Device type 2 application

Use of a variety of devices, assessed as a SRP/CS by the user under his own responsibility. The PL and PFH_D cannot be specified at device level. The device manufacturer provides an $MTTF_d$ or MTBF for the devices. The user defines the SRP/CS by means of the selected configuration or design, based on the specific application (category as selected designated architecture and DC). On this basis it is possible to determine a PL and PFH_D for the SRP/CS. This SRP/CS is then used as a part of the whole safety function.

Example:

Redundant (2-channel) use of two hydraulic valves as SRP/CS (actuators) in a safety function; the assessment is based on Category 3 and a DC of 90%.



[1] The information in red (Category and DC) is to be defined by the user.

Figure 3 – Device type 2 (ISO 13849-1)

Explanation:

The device manufacturer may state an MTTF or may simply provide an MTBF for the devices. In this case an $MTTF_d$ must be derived from this MTBF. In simple terms it can be assumed that MTTF ≈ MTBF.

The ratio of dangerous failures should be available from the device manufacturer as additional information.

As a starting point, a ratio of dangerous failures of 50% is stated in the standards for electronic devices (in accordance with IEC 61508) if there are no manufacturer's specifications for the device.

A ratio of dangerous failures of 100% can be assumed as a worst case.

This results in $MTTF_d \approx 2 \times$ MTTF (electronic) and $MTTF_d \approx$ MTTF (worst case).

The PFH_D can be determined using the informative Annex K and the input variables Category, DC and $MTTF_d$.

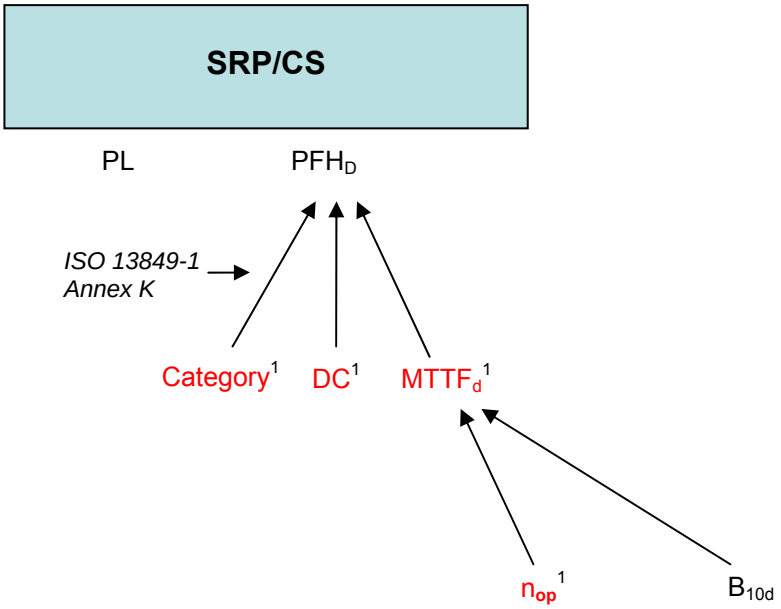
NOTE Additional requirements must be met for certain categories, such as CCF, for example.

5.1.3 Device type 3 application

Use of a variety of devices, assessed as a SRP/CS by the user under his own responsibility. The PL and PFH_D cannot be specified at device level. The device manufacturer does not supply an $MTTF_d$ for the devices because they are devices that are subject to wear. The $MTTF_d$ can only be determined based on the B_{10d} value (specified by the device manufacturer) and the application-dependent duty cycles per year (n_{op}, specified by the user). The user defines the SRP/CS by means of the selected configuration or design (category as selected designated architecture and DC). On this basis it is possible to determine a PL and PFH_D for the SRP/CS. This SRP/CS is then used as a part of the whole safety function..

Example:

Redundant (2-channel) use of two position switches as SRP/CS (sensors) in a safety function; the assessment is based on Category 4 and a DC of 99%.



[1] The information in red (Category, DC, $MTTF_d$ and n_{op}) is to be defined by the user.

Figure 4 – Device type 3 (ISO 13849-1)

Explanation:

The $MTTF_d$ is determined based on B_{10d} and n_{op}.

$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}}$, where n_{op} is the number of operations per year.

As a starting point, a ratio of dangerous failures of 50% is stated in the standards for devices that are subject to wear (in accordance with ISO 13849-1), if there are no manufacturer's specifications for the device .

This results in $B_{10d} \approx 2 \times B_{10}$.

The PFH_D can be determined based on the informative Annex K and the input variables Category, DC and $MTTF_d$.

NOTE Additional requirements must be met for certain categories, such as CCF, for example.

5.2 Requirements of IEC 62061

5.2.1 Device type 1 application

Use of a variety of devices, which have been pre-designed by the device manufacturer as a ready-to-use subsystem (see term 3.25 "Pre-designed subsystem").

The safety function can be assessed based on the data from the device manufacturer.

Example:

A guard door is monitored using a safety-related non-contact position switch. If the guard door is opened, a safely limited speed (SLS) should be triggered for the safety-related frequency converter via a failsafe control system.

A light curtain is to trigger a safe stop (STO) of a safety-related frequency converter via a failsafe control system if the light beams are interrupted, in order to shut down a hazardous movement.

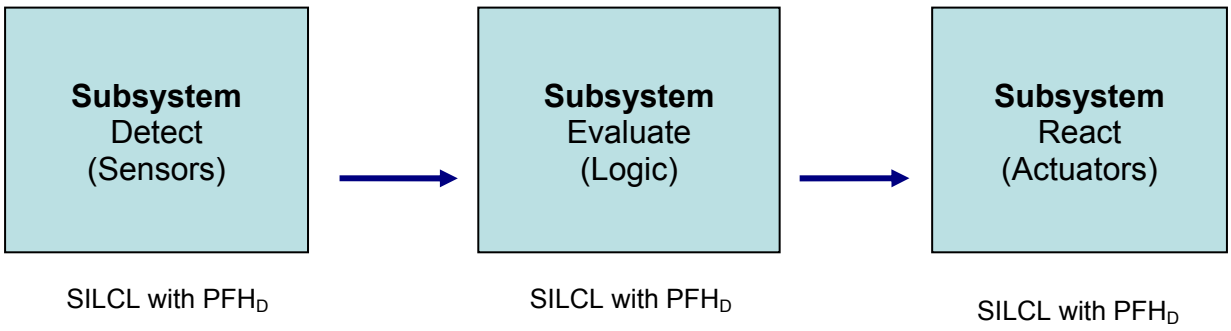


Figure 5 – Device type 1 (IEC 62061)

The highest possible SIL that a safety function can achieve is limited by

- the lowest SILCL of all subsystems and
- the PFH_D of the safety function, determined by adding the PFH_D of all subsystems.

Explanation:

The SILCL and PFH_D are specified by the device manufacturer.

The operating manual respectively the installation guideline of the device contains information about use and installation of the device as well as conditions for the operation of the device as part of a safety function.

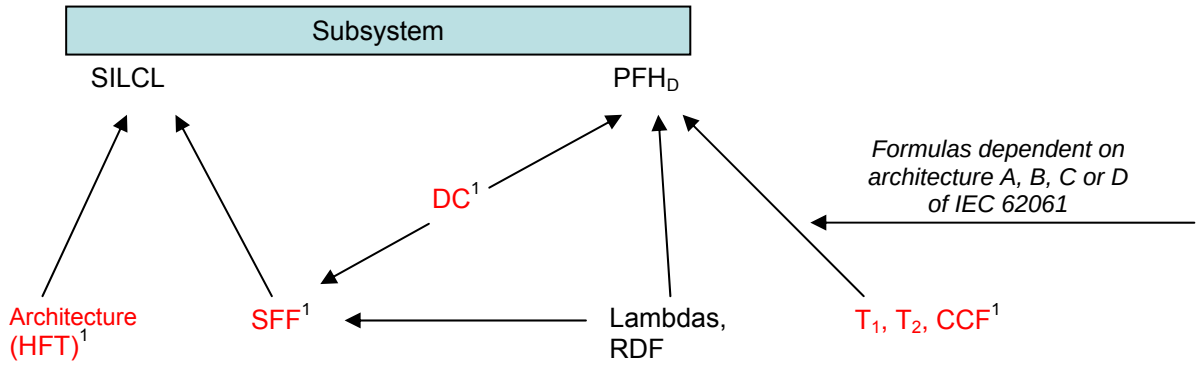
The machine builder may use the safety relevant data of the device, provided by the device manufacturer, as prove of the safety level of the documented safety functions, without further need for calculation.

5.2.2 Device type 2 application

Use of a variety of devices, assessed as a subsystem by the user under his own responsibility. The SIL and PFH_D cannot be specified at device level. The device manufacturer provides an $MTTF_d$, λ_D or MTBF for the devices. The user defines the subsystem by means of the selected configuration or design, based on the specific application (1 or 2-channel architecture as HFT equals 0 or 1 and DC). On this basis it is possible to determine a SILCL and PFH_D for the subsystem This SRP/CS is then used as a part of the whole safety function.

Example:

Redundant (2-channel) use of two current monitoring relays as subsystem (sensors) in a safety function. The assessment is based on an architecture with HFT of 1 and a DC of 90%.



[1] The information in red (architecture (HFT), DC, SFF, T_1, T_2 and CCF) is to be defined by the user.

Figure 6 – Device type 2 (IEC 62061)

Explanation:

The following always applies: $\lambda_D = RDF \times \lambda$.

With electronic components the following also applies $\lambda = \frac{1}{MTTF \times 8760}$ or $\lambda_D = \frac{1}{MTTF_d \times 8760}$.

The device manufacturer may specify an MTTF or may simply provide an MTBF for the devices. In this case an $MTTF_d$ must be derived from this MTBF. In simple terms it can be assumed that MTTF ≈ MTBF.

The ratio of dangerous failures should be available from the device manufacturer as additional information.

As a starting point, a ratio of dangerous failures of 50% is stated in the standards for electronic devices (in accordance with IEC 61508) if there are no manufacturer's specifications for the device.

A ratio of dangerous failures of 100% can be assumed as a worst case.

This results in $MTTF_d \approx 2$ x MTTF (electronic) or $MTTF_d \approx$ MTTF (worst case).

The PFH_D can be determined using the normative formulas and the input variables Architecture (HFT), T_1, T_2, CCF, DC and λ_D.

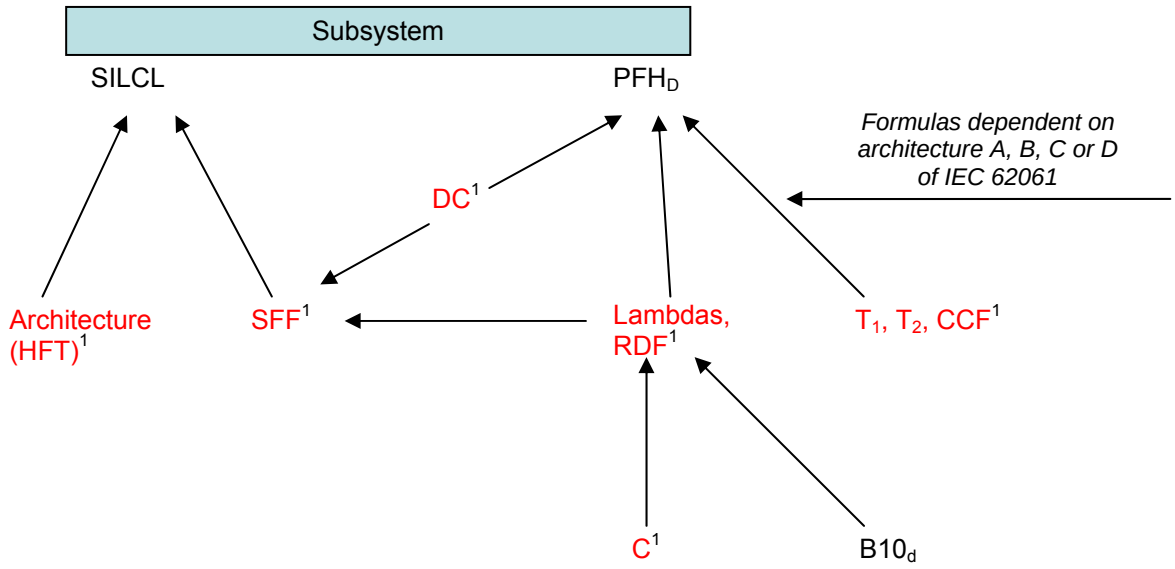
The SILCL is determined based on the SFF and the architecture (HFT).

5.2.3 Device type 3 application

Use of a variety of devices, assessed as a subsystem by the user under his own responsibility. The SIL and PFH_D cannot be specified at device level. The device manufacturer does not supply an $MTTF_d$ or λ_D for the devices because they are devices that are subject to wear. Lambda λ_D can only be determined based on the B_{10} value and the ratio of dangerous failures or the B_{10d} value (specified by the device manufacturer) and the application-dependent duty cycles per hour or per year (C and n_{op}, specified by the user). The user defines the subsystem by means of the selected configuration or design (1 or 2-channel architecture as HFT equals 0 or 1 and DC). On this basis it is possible to determine a SIL and PFH_D for the subsystem This SRP/CS is then used as a part of the whole safety function.

Example:

Redundant (2-channel) use of two power contactors as subsystem (actuators) in a safety function. The assessment is based on an architecture with HFT of 1 and a DC of 99%.



[1] The information in red (architecture (HFT), DC, C, SFF, lambdas, RDF, T1, T2 and CCF) is to be defined by the user.

Figure 7 – Device type 3 (IEC 62061)

Explanation:

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

$\lambda = \frac{0{,}1 \times C}{B10}$ or $\lambda_D = \frac{0{,}1 \times C}{B10_d}$, where C = operations per hour.

$C = n_{op} \times \frac{1}{365 \times 24}$ defines the relationship to operations per year n_{op} from ISO 13849-1.

The PFH_D can be determined using the normative formulas and the input variables Architecture (HFT), T_1, T_2, CCF, DC and λ_D.

SILCL is determined based on the SFF and the architecture (HFT).

6 Characteristic value library

6.1 Data structure

The information is structured as follows (see Figure 8):

– **VDMA66413** (Main Entity) – Details of the database format (see 6.2)

– **Manufacturer** – Details of the device manufacturer (see 6.3)

– **Device** – Details of the device (see 6.4.1)

– **UseCase** – Details of the use case (see 6.4.2)

– **DeviceType1..4** – Characteristic values (see 6.4.3)

– **Language** – Language texts (see 6.5)

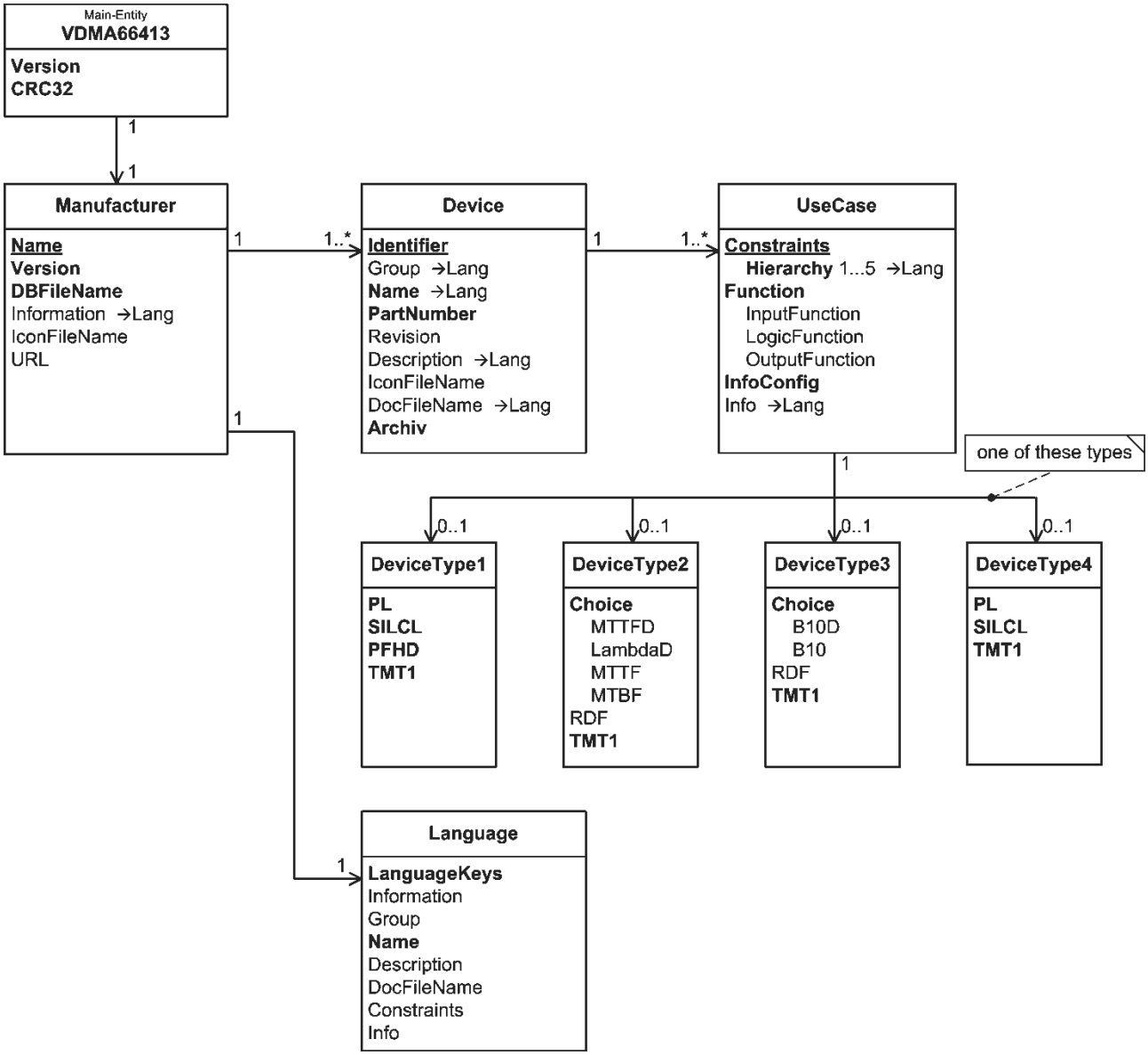


Figure 8 – Data structure of the characteristic value library (Database Entity Relationship Model)

Annex A

Files for the application

A.1 XML Schema file, characteristic value library

VDMA66413_2012-07_XML-Schema.xsd

The XML schema defines the formally correct structure and syntax of the characteristic value library.

The XML schema contains some additional, necessary structural constructs which are not addressed in the VDMA Specification.

The XML schema is used to check the characteristic value library for formal correctness.

NOTE Content and complex logic links cannot be checked using the XML schema. The XML schema does not replace the approval process validating the data.

A.2 XML example file, characteristic value library

VDMA66413_2012-07_XML-Example.xml

The example file contains devices, which are described using the correct syntax but are fictitious.

A.3 XML Schema file, language library

VDMA66413_2012-07_Language_XML-Schema.xsd

The XML schema defines the formally correct structure and syntax of the language library.

The XML schema contains some additional, necessary structural constructs which are not addressed in the VDMA Specification.

The XML schema is used to check the language library for formal correctness.

NOTE Content and complex logic links cannot be checked using the XML schema. The XML schema does not replace the approval process.

A.4 XML example file, language library

VDMA66413_2012-07_Language_XML-Example.xml

The example file contains language texts, which have the correct syntax but are fictitious.