



# Guidelines

Safety Integrity Level - SIL -

Valves and valve actuators

March 2009

VDMA  
German Engineering Federation

Valves Manufacturers Association  
Chairman:  
Prof.-Dr.-Ing. Heinfried Hoffmann  
Managing Director:  
Wolfgang Burchard

Lyoner Str. 18  
60528 Frankfurt am Main  
Germany  
Phone +49 69 66 03-12 42  
Fax +49 69 66 03-16 34  
E-Mail [armaturen@vdma.org](mailto:armaturen@vdma.org)  
Internet [www.vdma.org](http://www.vdma.org)

# Table of content

1.	Introduction	3
2.	Field of application	4
3.	Functional Safety	5
4.	Possible measures to implement SIL (Determination of parameters)	6
4.1	Safety systems	6
4.2	Determination of parameters	7
4.3	Methods of determining $\lambda$ -values	9
5.	Possibilities for the operator to change the safety system's SIL class (EN 61511- <b>ff</b> )	11

## Annex

Rules and standards

Terminology

## 1. Introduction

Process engineering systems in the chemical, pharmaceutical and petrochemical industry have to be operated “safely” as they have a high risk potential for human beings and the environment or may cause severe material damage. Of course, this also applies to other fields of industry (i.e. power plants).

In the framework of the development of appropriate protection concepts process control technology provides a major contribution to the systems’ safety with so-called PCT safety devices. It fulfils inter alia the requirements of the international standards EN 61508 and EN 61511.

Whilst the standard EN 61508 ‘Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems’ primarily addresses the manufacturers of safety device components, EN

61511 ‘Functional safety. Safety instrumented systems for the process industry sector’ is designed for operators and planners of safety devices. Standard EN 61511 includes recommendations and parameters to evaluate the damage risk of systems and offers assistance in selecting adequate safety-related components. This standard specifies four security levels the so-called Safety Integrity Levels 1 - 4. The higher the risk posed by the system the more reliable the risk reducing measures have to be and the higher the requirements for the electric, electronic and programmable electronic components.

For some time, system operators have been trying to extend the method to mechanical products and have therefore launched a debate among operators, manufacturers and certification bodies about the actual field of application and the relevance of the standards mentioned above for valves and valve actuators.

The present guidelines describe the application and implementation criteria which the valves industry considers relevant and may have to be taken into account. It is supposed to help prevent unnecessary discussions within all interested parties.

VDMA member companies participated in setting up these guidelines.

## 2. Field of application

Standard EN 61508 describes the state-of-the-art in terms of functional safety for electric, electronic and programmable electronic systems (E/E/PE) used for safety functions in safety-critical applications.

Valves that cannot be integrated in safety-oriented systems (e.g. manually-operated valves without feedback/end switch) are per se excluded from the standard's field of application.

The same applies to safety valves, as these never form part of the 'normal operational processes' whose functional safety is supposed to be tested according to SIL.

It is not possible to directly generate a SIL class for control valves and their separate components as mechanical components (for example valves, valve actuators, position regulators) in accordance with EN 61508-ff.

Yet, it is possible to define relevant parameters (for instance failure rates, hardware-failure-tolerances) which can be used to determine the SIL class of a complete safety-related system.

However, the following has to be taken into account: EN 61508 is not harmonised under any EU-Directive being relevant for valves. This means that in this case there is no automatic presumption of conformity with the protective objectives of a Directive. Therefore, the compliance with this standard is voluntary and non-binding in the sense of EU-Directives.

As a result, each valve manufacturer can decide (ideally together with his customer) whether and to what extent parameters should be defined as a basis for evaluating the valve in the framework of a SIL system classification.

Note: Depending on the construction type, the function, the field of application and operating conditions of a SIL relevant component, other rules and

regulations than the standards mentioned in these guidelines may also need to be taken into account (for instance Pressure Equipment Directive, ATEX, EMC).

### 3. Functional Safety

Functional safety is the part of the overall safety that depends on the correct functioning of a safety-related E/E/PE system, of safety-related systems of other technologies and external risk minimising devices. This safety is given when each specified safety function is performed and each safety function has reached the required degree of fulfilment. The main requirement of EN 61508 consists in providing a quantitative proof of the remaining residual risk in terms of functional safety. In order to reduce this risk, the standard describes two major steps:

- Definition and risk evaluation on the basis of detailed failure probabilities for the application's full life cycle.
- Periodical check of the correct fulfilment of parameters. The observed life cycle is subdivided into 16 aspects (picture 2, EN 61508-1, Nov. 2002).

Section 8.2 of the standard EN 61508-1 specifies requirements for the evaluation of functional safety. One aspect of these requirements is the so-called independence rate of persons, departments and organisations. Tables 4 and 5 describe the interaction of independence rates and Safety Integrity Levels in the framework of these 16 sub-aspects of the safety life cycle.

#### **SIL-conforming products and failure probability**

Modern safety technology is necessary to reduce the risks in systems with a high danger potential (for instance in process technology). This requires an overall safety concept from the sensor via the control up to the actuator.

The risk potential of a system (or part of a system) can be determined for example by means of EN 61511. Depending on the identified risk, this risk has to be reduced. When this is done with electric components, these have to fulfil the requirements of EN 61508. Both standards divide the procedural system into four safety levels (SIL) required for risk reduction. A Safety Integrity Level is one of four discrete levels. Each level corresponds to a probability range of failure of a safety function. SIL 4 is the highest level, SIL 1 the lowest. It has to be noted that a Safety Integrity Level represents a characteristic of a system or of a part of a system and not a component. Tables 1 and 2 below show examples of failure limit values and the corresponding Safety-Integrity-Levels according to EN 61508.

Safety-Integrity-Level	Type of operation with <b>low demand rate</b> (average probability of failure to perform a design function on demand; according to table 2 EN 61508-1)
4	$>10^{-5}$ bis $<10^{-4}$
3	$>10^{-4}$ bis $<10^{-3}$
2	$>10^{-3}$ bis $<10^{-2}$
1	$>10^{-2}$ bis $<10^{-1}$

**Table 1** (Source: EN 61508-1, Nov. 2002)

Safety-Integrity-Level	Type of operation with <b>high demand rate</b> or continuous demand (probability of a danger-inducing failure per hour; according to table 3 EN 61508-1)
4	$>10^{-9}$ bis $<10^{-8}$
3	$>10^{-8}$ bis $<10^{-7}$
2	$>10^{-7}$ bis $<10^{-6}$
1	$>10^{-6}$ bis $<10^{-5}$

**Table 2** (Source: EN 61508-1, Nov. 2002)

**Note:** The types of operation with low demand rates usually apply to the fields of application of valves.

#### 4. Possible measures to implement SIL (Determination of parameters)

##### 4.1 Safety systems

The SIL relevance does not depend on a component's physical characteristics, but comes up with a concrete safety requirement of an operator or customer. Mechanical components (for instance valves) can be parts of an electric / electronic / programmable electronic safety system and are subject to the same safety consideration as the system itself.

Such a safety system consists for example of interlinked partial systems, i.e. mainly of the sensor, the logic (SPS and control system), the actuator (valve, actuation and additional elements like regulators or solenoid valves) and other mechanical/non-electric construction components.

## 4.2 Determination of parameters

Parameters allow the operator to determine a system's SIL class depending on the considered safety area. Therefore, a valves manufacturer's certificate will only include parameters and not the SIL class itself.

The indicated parameters are always to be seen in relation to the respectively considered product-specific application and the relevant operating conditions.

In case of new constructions of components or systems it is useful to check the relevance of the safety subject SIL beforehand and, if applicable, to involve notified bodies or other external expertise at an early stage.

Possible evaluation method for the safety function according to SIL

- Definition of the safety function of the actuating element and the scope
- Breakdown into safety-relevant functional blocks
- Risk analysis for instance by means of FME(D)A
- Field data as a basis for the reliability aspect („proven in use“)
- Tests / Product validation
- Product observation
- Quality-assured manufacturing
- Determination of parameters (detailed below)
- Integration and follow-up of the safety aspect in the quality management system
- Adding safety-relevant indications in the operating instructions
- Issuing a manufacturers certificate

**Table 3** below describes the parameters already mentioned in these guidelines that are applicable to actuating elements as well as their determination possibilities.

Parameter	Definition	Unit	Value
HFT	Hardware-Failure-Tolerance: Ability of a functional unit to continue to perform a required function in the presence of errors or deviations (see also EN 61511-1, sect.11.4, May 2005).  The HFT is determined by the user.  (Industriearmaturen 04/2005)		
SFF	Safe Failure Fraction	%	
PFD <sub>avg</sub> Total system	Average probability of failure to perform its design function on demand		
PFD <sub>avg</sub> Part system Actuator: valve	Average probability of failure to perform its design function on demand		About 50 % of the SIL quota can be assessed for the actuator
PFD <sub>avg</sub> Part system Actuator: Solenoid valve/ regulator	Average probability of failure to perform its design function on demand		About 15 % of the SIL quota can be assessed for the actuator
PFD <sub>avg</sub> Part system Actuator: Adjustment valve	Average probability of failure to perform its design function on demand		About 15 % of the SIL quota can be assessed for the actuator
PFD <sub>avg</sub> Part system Actuator: Adjustment actuator	Average probability of failure to perform its design function on demand		About 15 % of the SIL quota can be assessed for the actuator
MTTF <sub>d</sub>	Assumed average time until dangerous	[Time	

Parameter	Definition	Unit	Value
	failure (mean time to failure dangerous)	unit]	
$\lambda_{SD}$	Rate of safe, identified failures	FIT (failure in time)	
$\lambda_{SU}$	Rate of safe, non-identified failures	FIT	
$\lambda_{DD}$	Rate of dangerous, identified failures	FIT	
$\lambda_{DU}$	Rate of dangerous, non-identified failures	FIT	
DC	Diagnostic coverage: Percentage of failures identified by diagnosis tests compared to the total failure rate of components or the part system. The Diagnostic Coverage includes no failures identified with proof tests (for further indications, also with regard to $\lambda$ , see EN 61511-1, sect. 3.2.15, Edition May 2005)	%	
CCF	Common caused failure. Failures of different units due to a single event – these failures have no mutual consequences (draft EN ISO 13489-1, 2004, Sect. 3.1.6)		
Performance Level PL	Ability of safety-related parts to perform a safety function under predictable conditions (which should be taken into consideration) in order to fulfil the expected risk reduction (draft EN ISO 13489-1, 2004, Sect. 3.1.23)		

**Table 3** Parameters

The key parameters PL, MTTFd , DC and CCF show the following features:

- Result of a calculation
- Suitable to determine the safety in mechanical systems
- Also integrate electric systems

After the determination of the  $\lambda$ -values as described below, the other values can be calculated as set in the standard EN 61508-ff:

SFF, DC, PFD<sub>avg</sub>

### 4.3 Methods of determining $\lambda$ -values

Apart from the approaches briefly described below, there are certainly other ways to determine the  $\lambda$ -values. The choice depends on many parameters and has to be made by each manufacturer individually. It is recommended to check whether the customer should be involved.

**Approach 1**

The manufacturer makes use of existing data and the experience of active institutions (exida, oreda etc.) on the market.

**Approach 2**

The methodology according to EN ISO 13849 can be used to determine the parameters.

**Approach 3**

General proof of fitness for a Safety Integrity Level (SIL):

- • Component testing according to a relevant equipment standard
- • Determination of the type of failures over the full life cycle on the basis of DIN V 19251
- • Gradation of measures designed to prevent and control failures on the basis of DIN V 19251
- • Implementation of a FME(D)A
- • Preparation of all data for the configuration management (in accordance with EN 61511)
- • Ensuring the production-accompanying quality assurance measures
- • Comparison of requirements classes on the basis of DIN V 19250 with SIL by using the standard EN 61511-3 Annex E

**Approach 4**

Test steps to examine the fitness of control devices according to DIN EN 61508-ff

- • Component testing according to a relevant equipment standard (for instance EN 161)
- • Implementation of a component FME(D)A
- • Practical endurance testing of representative control devices to prove a PFD value
- • Statistical analysis of the operational reliability in various procedural systems
- • Manufacturing the products on a proven high quality level

The tests combined with the statistical data allow generate sufficiently reliable statements about the failure probability.

Determination of the parameters (table 3) for the SIL classification (adjustment of the parameters insofar as statistical data are available).

## 5. Possibilities for the operator to change the safety system's SIL class (EN 61511-ff)

The operator has two possibilities to change the SIL class of his safety system, which read as follows:

- Changing the proof-test-intervals
- Changing the system architecture, for instance by means of redundancy (for instance two valves connected in a row).

## Annex

### Rules and standards

EN ISO 13849	Safety of machinery - Safety-related parts of control
Part 1:	General principles for design (2007-07)
Part 2:	Validation (2003-12)
EN 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
Part 0:	Functional safety and EN 61508 (2005-10)
Part 1:	General requirements (2002-11)
Part 2:	Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems (2002-12)
Part 3:	Software requirements (2002-12)
Part 4:	Definitions and abbreviations (2002-11)
Part 5:	Examples of methods for the determination of safety integrity levels (2002-12)
Part 6:	Guidelines on the application of EN 61508-2 and EN 61508-3 (2003-06)
Part 7:	Overview of techniques and measures (2003-06)
EN 61511	Functional safety – Safety instrumented systems for the process industry sector
Part 1:	Framework, definitions, system, hardware and software requirements (2005-05)
Part 2:	Guidelines for the application of part 1 (2005-05)
Part 3:	Guidance for the determination of the required safety integrity levels (2005-05)

EN 62061	Correction 1 – Safety of machinery - Functional safety of safety related electrical, electronic and programmable electronic control systems (2006-06)
VDI 2180	Safeguarding of industrial process plants by means of process control engineering (2007-04)
NE 031	Safety of process plants using process control equipment (NAMUR-recommendation 2006-07)
NE 93	Verification of the safety-related reliability of PCT safety instruments (NAMUR-recommendation 2003-02)

### **Terminology**

EUC = Equipment under control (EN 61508-4) [called process in EN 61511]

Failure = End of the ability of a functional unit to perform a required function (EN 61508-4)

Proof test = Recurrent test to identify failures in a safety-related system, so that, if necessary, the system can return to a state that is "as good as new" or as close as practically possible to it. (EN 61508-4)

Actuating element = Unit composed of control actuator, control valve and accessories (solenoid valve/position regulator, adapter, etc.)

## **Contact**

Hartmut Tembrink  
VDMA - Valve Manufacturers Association  
Lyoner Straße 18  
60528 Frankfurt / Main  
Phone +49 69/66 03-12 46  
Fax + 49 69/66 03-22 46  
E-Mail [hartmut.tembrink@vdma.org](mailto:hartmut.tembrink@vdma.org)