Industrial Automation

SILence

Manual

HIMA Paul Hildebrandt GmbH + Co KG
Industrial Automation

HI 800 131 BEA

Important Notes

All HIMA products mentioned in this manual are protected under the HIMA trademark. Unless not explicitly noted, this may apply for other referenced manufacturers and their respective products.

All listed modules are CE certified and meet the requirements of the European Union’s EMC Guideline.

All technical statements and data in this manual have been written with great care and effective quality measures have been taken to ensure their validity; however this manual may contain flaws or typesetting errors. For this reason, HIMA does not offer any warranties nor assume legal responsibility nor any liability for possible consequences of any errors in this manual. HIMA appreciates any correspondence noting potential errors.

Technical modifications reserved.

Delivery Conditions

Either the “General Conditions for Delivery of Products and Services” of the German Electrical Industry - edition January 2002 - or the “Conditions of Delivery for System Software and Peripheral Devices for the HIMA Automation System“ apply for all deliveries.

Potential claims can only be recognized only if received within 14 days of receipt of the merchandise.

TÜV Rheinland/
Berlin-Brandenburg

TÜV

TÜV Anlagentechnik GmbH
Automation, Software und Informationstechnologie

BESCHEINIGUNG

CONFIRMATION

Nr./No. 968/EL 246.00/03

Prüfgegenstand **Product tested**	Software tool SILence	**Hersteller** **Manufacturer**	HIMA Paul Hildebrandt GmbH + Co. KG Albert-Bassermann-Straße 28 D-68782 Brühl bei Mannheim
Typbezeichnung **Type designation**	SILence Version 1.0	**Verwendungs-zweck** **Intended application**	Software tool for safety integrity level calculations
Prüfgrundlagen **Codes and standards forming the basis of testing**	IEC 61508, Part 6:2000 IEC 61508, Part 1, 2 and 7:2000, so far applicable		
Prüfungsergebnis **Test results**	The software tool SILence is fit for use as a safety integrity level calculator according to basis of testing considering the results of the test report no. 968/EL 246.00/03 dated 2003-10-30.		
Besondere Bedingungen **Specific requirements**	For the use of the software tool the test report mentioned above and the User Manual Version 1.0 released by HIMA and TÜV Rheinland have to be considered.		

TÜV Anlagentechnik GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 09 51, 51101 Köln

H. Gall

2003-10-30

Datum/Date | Firmenstempel/Company seal | Unterschrift/Signature

About this Manual

As specified in IEC/EN 61508, the ***SILence*** software described in this manual enables the user to determine the Safety Integrity Level (SIL) for entire loops (consisting of sensor, signal processing, actuator) of plants to be engineered.

SILence is the first tool verified by the German TÜV to calculate the SIL. ***SILence*** supports the Safety Consultant or operator during the design of safety loops. ***SILence*** documents the SIL calculations in the definition phase. Based of the SIL value achieved, the correct definition of the loop is documented in the total safety validation.

SILence is able to administer a variety of libraries. The user can create his modules or libraries and work with them. Additionally, he can exchange the libraries independently of one another.

HIMA systems are always developed, produced and certified in accordance with the valid national and international standards. In this regard, one of the most important international standards is IEC/EN 61508.

IEC/EN 61508 does not only cover numerical values such as PFD and PFH, which provide information about the probabilities of a system failure, but it describes the overall safety life cycle of a system.

Target Audience

This manual is meant for engineers working in project engineering for safety-related automation technology.

Knowledge of the IEC/EN 61508 standards, safety engineering and statistical computation is a prerequisite for using ***SILence*** correctly.

Post Office Box 1261
D - 68777 Brühl by Mannheim
Phone +49 (0) 6202 709-0
Fax +49 (0) 6202 709-107
E-mail info@hima.com
Internet http://www.hima.com

Terminology

Term	Definition
λ_{DD}	Detectable dangerous failure rate (per hour)
λ_{DU}	Undetectable dangerous failure rate (per hour)
λ_S	Detectable safe failure rate (per hour)
β	Dangerous undetectable common-cause failure
β_D	Dangerous detectable common-cause failure
CRC	Cyclic Redundancy Check
DC	Diagnostic Coverage Factor is the proportion of the dangerous detectable failures related to all dangerous failures
E/E/PES	Electrical / Electronic / Programmable Electronic Systems
EUC	Equipment Under Control
HFT	Hardware Failure Tolerance
MTTF	Mean Time To Failure
MTTR	Mean Time to Repair
PFD	Probability of Failure on Demand, (A function is requested up to a maximum of twice per year)
PFH	Probability of Failure per Hour (A function is requested more than two times per year)
SFF	Safe Failure Fraction Part of safe failures and dangerous detectable failures related to all failures
SIL	Safety Integrity Level discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.
*.sdd	File format for “***SILence*** <u>D</u>atabase <u>D</u>evice“
*.sds	File format for “***SILence*** <u>D</u>atabase Predefined <u>S</u>ystem“
*.spr	File format for “***SILence*** <u>Pr</u>oject“
*.ssy	File format for “***SILence*** <u>Sy</u>stem“

Table of contents

1 Introduction

The number of safety-relevant systems developed, produced and offered on the market is constantly increasing. For this reason, it is essential to know the current international standards for “Functional safety” and to use them correctly in order to effectively and safely implement systems in safety-critical environments.

Functional safety is a part of the overall safety relating to the EUC and the EUC control system, which depends on the correct functioning of the E/E/PE safety related systems, other technology safety-related systems and external risk reduction facilities.

Fig. 1 shows the accepted distribution of failures over the system’s life cycle. With this in mind, it is not important whether the system is a controller or a complete plant.

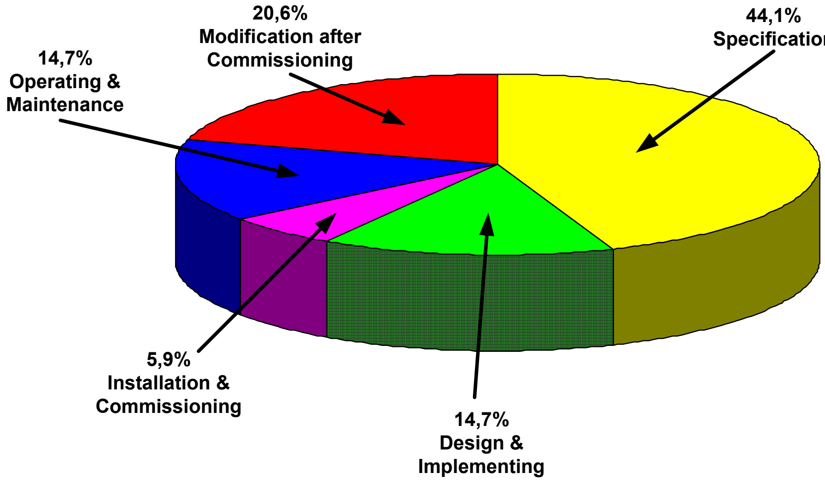


Fig. 1: Failure Rates in Different Phases of a System’s or a Plant’s Life Cycle

In considering failures, a basic distinction is made between safe and dangerous failures. Safe failures are further divided into two categories:

- Safe detectable failures and
- Safe undetectable failures.

Safe failures, whether detected or not, are failures that exert no influence on the safety function of the system. This is not the case with dangerous failures. When these failures occur, they lead to a dangerous situation in the system, which may even, under certain circumstances, seriously endanger human lives. These failures are also divided into two categories:

- Dangerous detectable failures and
- Dangerous undetectable failures.

In the event of dangerous detectable failures, the safety-related system, if properly designed, can bring the entire system or plant into a safe state. It is undetectable, dangerous failures that bring about a critical state. In fact, no safety-related system is able to detect such failures, when they occur. They may be present in the system until it switches off or, in the worst-case scenario, until it fails dangerously, without knowledge of the user.

The failure rates λ of a system or a plant are categorised as follows:

Failure Rate	Type of Failure
λ_S	Safe failures
λ_{SD}	Safe detectable failures
λ_{SU}	Safe undetectable failures
λ_D	Dangerous failures
λ_{DD}	Dangerous detectable failures
λ_{DU}	Dangerous undetectable failures

Table 1: Failure Rates and Type of Failure

Obviously, a failure distribution such as the one presented in Fig. 2 can only be qualitative. The occurrence of dangerous failures in the proportions as shown in this figure is unacceptable for any safety-related system.

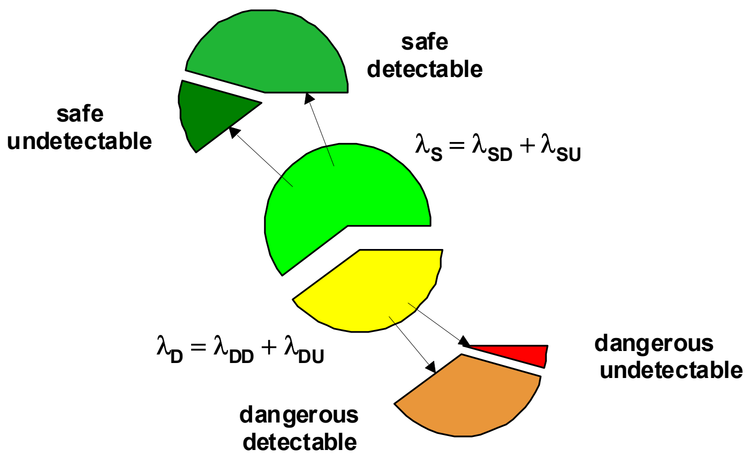


Fig. 2: Failure Rates Distribution for Safe and Dangerous Failures

To operate systems or plants in safety-related environments, extensive development and certification measures are necessary. These serve to avoid the dangerous situations described above, or, if this is not possible, to bring the system or the plant into a safe state.

The standard IEC/EN 61508 with its seven sections covers the overall life cycle of a system or a plant.

- Part 1 of the standard defines the plant or system's life cycle, the requirements on safety-related systems, as well as the values for PFD (Probability of Failure on Demand) and PFH (Probability of Failure per Hour), referring respectively to a low and high demand mode of operation.
- Part 2 specifies the requirements on safety-related systems and their respective architecture.
- Part 3 describes the actual life cycle of software and hardware, as well as the methods for achieving and maintaining safety.
- Part 4 presents the terms and abbreviations used in the standards. It is an important resource for studying and applying these standards.
- Part 5 defines the analysis methods for using safety-related systems.
- Part 6 presents the application of parts 2 and 3.
- Part 7 explains the methods specified in all preceding sections.

Fig. 3 shows the norm's overall framework, which is generally accepted and applicable to all safety-related electrical / electronic / programmable electronic systems (E/E/PES), independently of their operating environment. IEC/EN 61508 integrates different safety standards and can therefore be considered both a stand-alone and a basic standard.

In order to conform to this standard, it must be demonstrated that the requirements have been satisfied to the required criteria specified. An exception is made only for systems with lower complexity, for which sufficient, reliable experience is available.

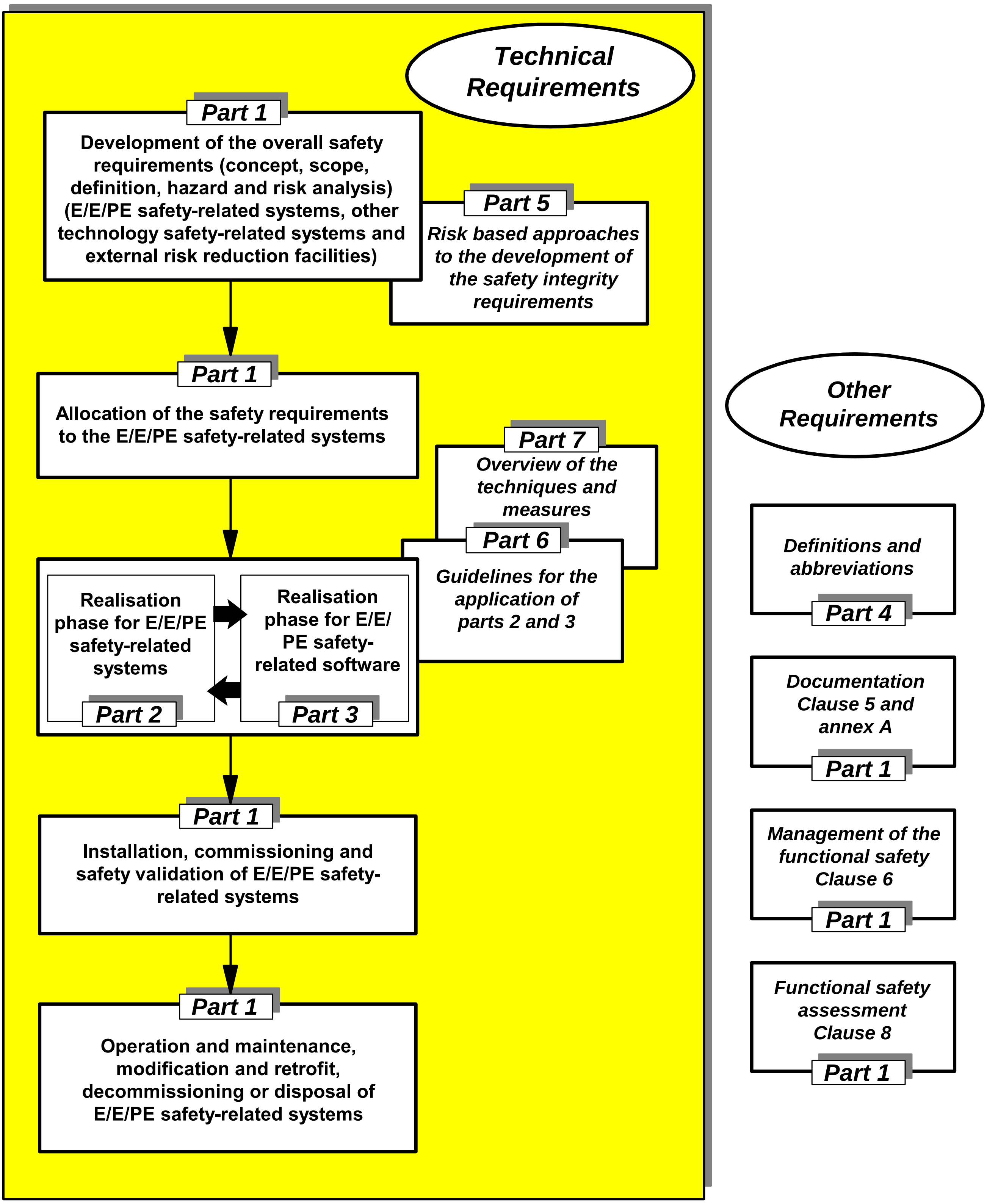


Fig. 3: General Structure of IEC/EN 61508

2 General Comment on IEC/EN 61508

Part 1 describes all aspects relating to the use of electrical or electronic programmable systems in safety-relevant applications. It explains the definition of "Functional Safety Management" and provides clarification of the planning of all phases of the safety life cycle.

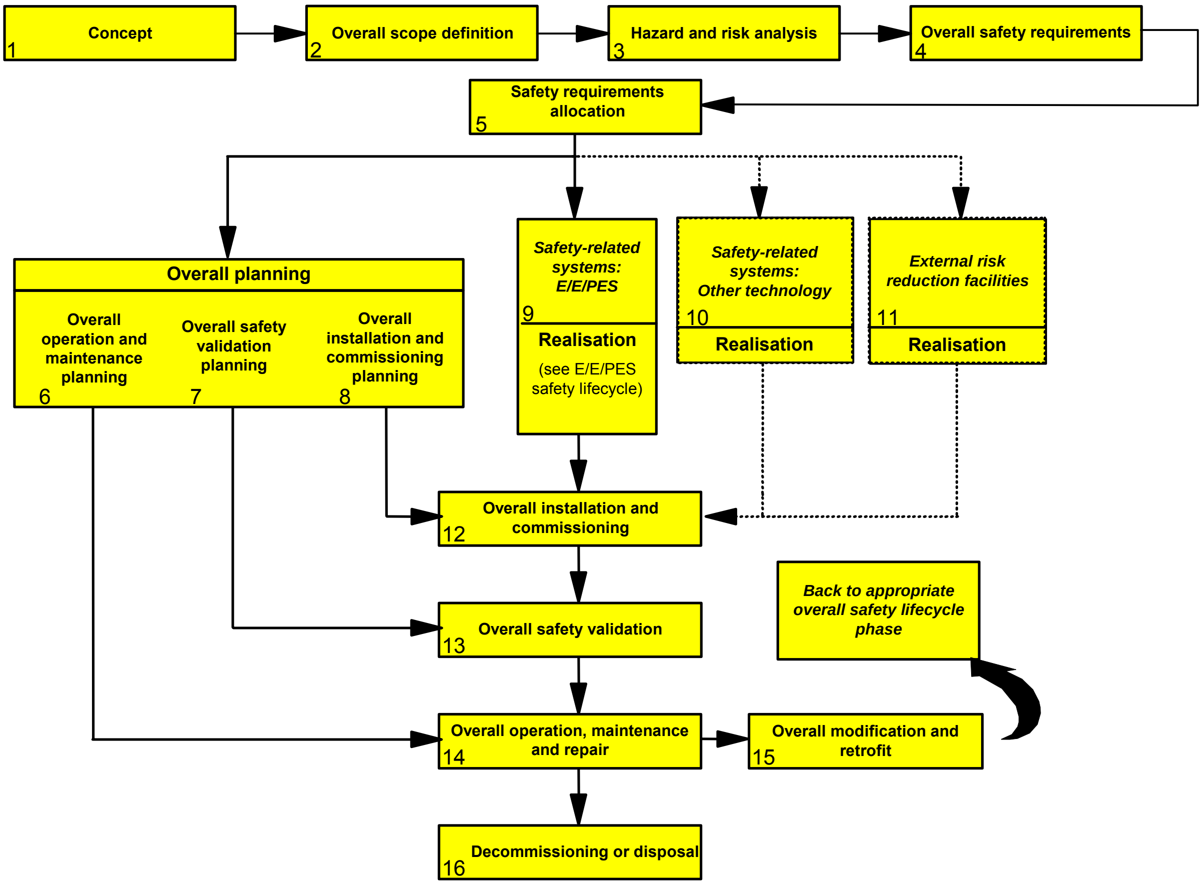


Fig. 4: Safety Life Cycle

Analysis of the safety life cycle allows a systematic approach to the problems of functional safety, consisting of three vertical phases:

- Determination of the safety requirement
- Implementation of the system or the plant
- Start-up, total safety validation, operation, maintenance and decommissioning

The individual phases depicted in Fig. 4 are explained below.

In the concept phase, a sufficient level of understanding for the EUC and its environment must be developed. This analysis must take into account all probable sources of danger and applicable legislative provisions.

In the next phase the entire range of application including the limits and the possible external dangers is to be defined. So in the following phase, the endangerment and risk analysis are practicable. There must be included all predictable circumstances, dangers and potentially dangerous events in a reasonable measure. Further the probability and potential consequences of these dangerous events must be determined.

In the next phase, the overall scope of the operating environment must be defined, including all boundaries and potential hazards. This permits one to proceed with the hazard and risk analysis phase in which one must adequately consider all reasonably foreseeable circumstances, hazards and potentially hazardous events. This analysis also considers the probability with which the hazardous events might occur, as well as the risk associated with them.

In the next two phases the overall safety requirements and their respective allocation must be formulated. The first step is to specify the the safety functions and their respective safety integrity in order to achieve the necessary level of functional security. The second step is to determine the level of risk reduction using external systems. Finally, the third step is to define which safety-related systems are used to achieve the required functional security. At this stage, the SIL (Safety Integrity Level) of each individual safety function must be specified (see Table 2).

Safety Integrity Level (SIL)	**Low Demand Mode** (Average Probability of Failure to Perform Designed Safety Function on Demand)	**High Demand Mode** (Probability of a Dangerous Failure per Hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Table 2: SIL for Low and High Demand Mode

In addition to the specification of the concept and design phases, IEC/EN 61508 defines steps beyond the commissioning phase. Specifically, the planning of the overall operation and maintenance phases are prescribed. If necessary, these phases must detail standard maintenance routines for maintaining functional safety. At this stage, a plan for validating the overall system is created, taking all potential operating states into account. Furthermore, the strategy for validation is defined, including all criteria for passing or failing verification. Measures must be planned to ensure safety during maintenance.

The total safety validation is also illustrated in Fig. 4. At this stage, a plan for validating the overall system is created, taking all potential operating states into account. Furthermore, the strategy for validation is defined, including all criteria for passing or failing verification.

The overall planning consists of two other stages, the planning of the overall installation and the overall start-up phases, which include the controlled installation and controlled start-up stages respectively. In these phases, responsibilities and installation procedures must be considered, and the criteria for declaring the system or plant's installation finished must be specified.

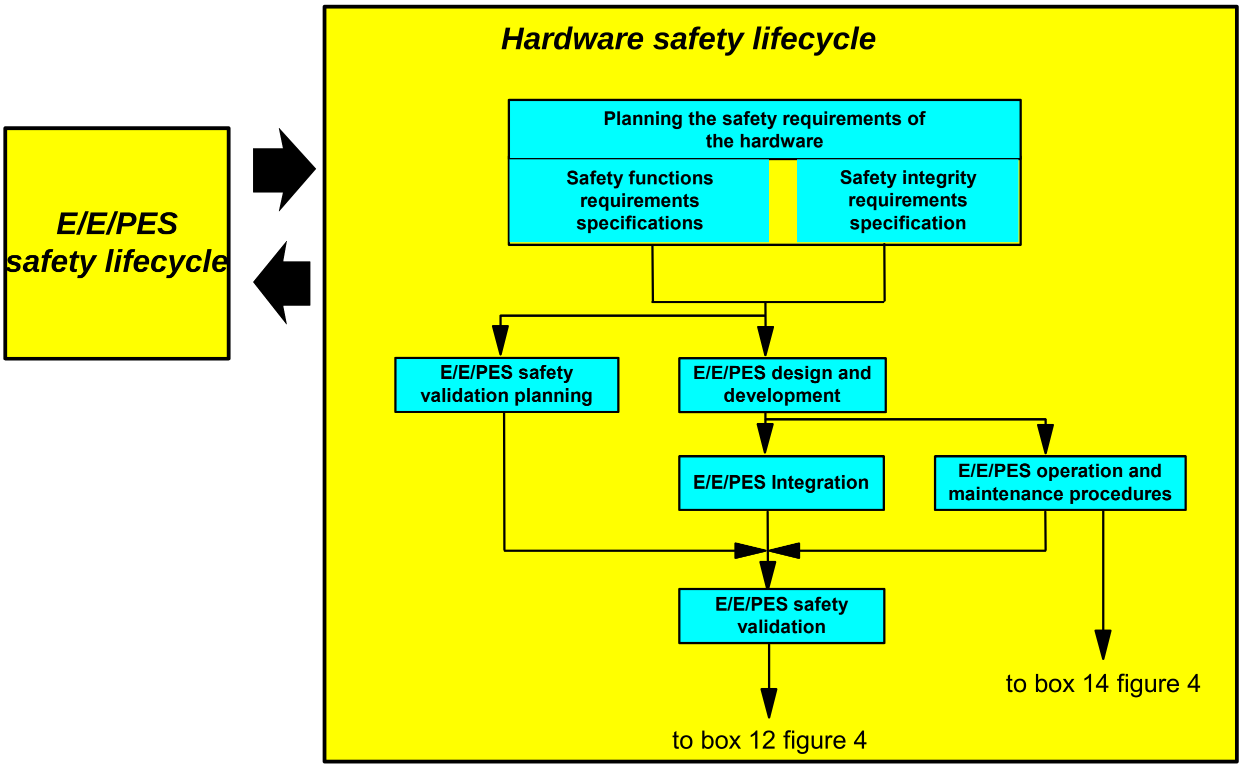


Fig. 5: Hardware Safety Life Cycle

Obviously, the realization phase is one of the most decisive moments in the overall planning. In this phase, the actual execution of the designed safety-related system must be planned and the actual developments must be realized. In this context, one should consider parts 2 and 3 of the standard, which depict the hardware and software development and requirements.

Once the concept and realization phases are completed, it is possible to realize the overall installation, start-up and validation of the planned system. These steps must be performed following the instructions specified in previous stages.

The standard prescribes how to proceed during a global modification or update, focussing on the importance of preserving the functional safety during and after modifications. In this context, all modification activities must be carefully planned and their potential effects analyzed.

Finally, the norm describes the decommissioning and scrapping phases. In this context, one must consider and analyze how decommissioning may influence the functional safety of systems connected with the safety-related system. The system decommissioning may only be authorized after this analysis.

3 Hardware Requirements

Part 2 of the standard specifies the hardware requirements, including the hardware safety life cycle and the architecture requirements. It makes and explains the distinction between type A and type B subsystems (i.e. in the first case, if a failure occurs, the subsystem's behaviour is completely known; in the second case, the subsystem's behaviour is only partially known) and defines the corresponding SFF (Safe Failure Fraction). Moreover, it describes all actions and instructions that are necessary to develop hardware systems. The methods, measures and techniques that can be deduced from this information are detailed in the tables located in the norm's corresponding appendix. In this context, two documents are required. The first document is the specification of the safety function containing exact details on how to achieve and maintain the necessary safety. The specification must also consider all relevant modes of operation. The second document is the specification of the safety integrity containing details on the safety integrity level of each safety-related function.

	Type A Subsystem			Type B Subsystem		
Safe Failure Fraction (SFF)	Hardware Failure Tolerance N			Hardware Failure Tolerance N		
	0 Failures	1 Failure	2 Failures	0 Failures	1 Failure	2 Failures
< 60 %	SIL 1	SIL 2	SIL 3	Not allowed	SIL 1	SIL 2
60 % to < 90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 % to < 99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Table 3: Type A and Type B Subsystems

Note: A hardware failure tolerance of N means that N + 1 failures can lead to a loss of safety function

Type A:
Subsystems belong to this category if all subsystem components required achieving the safety function meet the following conditions:

- The failure behaviour of all implemented components has been sufficiently specified;
- The subsystem failure behaviour under failure conditions can be completely determined;
- Reliable failure specifications for the subsystem based on field experience exist and can be used to demonstrate that the presumed failure rates for detectable or non-detectable failures may be achieved

Type B
Subsystems belong to this category if the subsystem components required achieving the safety function meet one of the following conditions:

- The failure behaviour of at least one of the implemented component has not been sufficiently specified;
- The subsystem failure behaviour under failure conditions cannot be completely determined;

- No reliable failure specifications for the subsystem based on field experience exist to support the presumed failure rates for detectable or non-detectable failures.

Note	In other words, if at least one subsystem component responds in greater degree to the requirements for type B subsystems, the subsystem must be categorized type B rather than type A.

In planning safety validation, all requirements for test procedures, test environment and all criteria for passing or failing verification must be considered.

The design of a safety-related system must be realized in accordance with the defined safety specification, adapting the hardware architecture requirement to the demanded SIL. The integrity level is determined using the hardware failure tolerance and the Safe Failure Fraction (see Table 3).

Other important factors in the normative design and development processes include the estimation results calculated for the probabilities of failure of the component safety functions due to accidental hardware failures. In particular, the estimated subsystems' failure rate, the probability of detecting a failure by diagnostic facilities as well as the time period necessary to eliminate detected failures must be taken into account.

For each safety level, the norm recommends technologies and measures to control accidental hardware failures, systematic failures, environment-related failures, as well as failures caused by operating factors.

The norm dictates that the safety-related validation must follow the plan defined in previous stages. Additionally, it is necessary to validate each specified safety function using tests or analysis procedures and to document each individual step. This procedure also requires that each individual modification is carefully verified and documented.

IEC/EN 61508 prescribes the verification of the correctness of each single phase of the development cycle.

4 Software Requirements

Part 3 of IEC/EN 61508 defines the software requirements for safety-related systems. As in part 2 for the harware, it specifies the software safety life cycle and the quality management for all phases of the software development, including the validation and modification stages. Using the results presented in parts 1 and 2, it provides the procedure for developing safety-related softwares. Using this information in conjunction with the tables in the norm's appendix, one can deduce how to proceed in developing the safety-related software.

In the first stage, the software safety requirements must be carefully specified. The software developer must verify the specification by means of a review to ensure that all resulting software requirementshave been sufficiently specified and can thus be met by the software. Additionally, the specification must contain details on the software self monitoring and the hardware monitoring procedures. Upon completing the specification, the planning of the safety validation can begin. As with the hardware described in part 2, this stage requires specification of all requirements for test procedures, including the criteria for passing or failing verification. Finally, the actual software development can be realized. The developed software must be analyzable and verifiable to ensure that the verification of the safety integrity level can be safely performed. Splitting the development into separate modules offers the advantage of reduce complexity. With this procedure, it is essential to ensure that each module is sufficiently and precisely specified and verified during the design phase. The standard reccomends careful selection of tools and compilers.

During the integration of the software into the target hardware, the compatibility between software and hardware must be examined using tests to ensure that the desired safety integrity level can be achieved. Examples for such tests include cyclic memory tests, to check the memory, or walkingbit tests to check the implemented bus system. The resulting system must adhere to the specified requirements.One must proceed in accordance with the validation plan and the software's validity with test results.
During later software modifications it must be guaranteed that they do not affect the specified requirements of safety. For this purpose an effect analysis of the planned modification is prescribed.
As with the hardware verification stage, the correctness of the results must be examined during the software verification. This is why the software verification must be planned during the development phase. Each individual software component (i.e. source code, data, modules or architecture) must be verified.

Note	For redundant interconnections of type A modules, the SIL X can be improved to SIL X+1. The prerequisite for such improvements is that the module software has already been certified for the higher SIL. Redundant interconnections only improve the hardware. A software failure would occur in both systems at the same time as the software, and consequently the probability of failure, is the same in both devices.

5 Examples of Methods for the SIL Determination

Part 5 of the standard shows methods for the determining the safety integrity levels. In particular, it offers methods for specifying systems, for each individual safety function. A basic distinction between qualitative and quantitative methods is made.

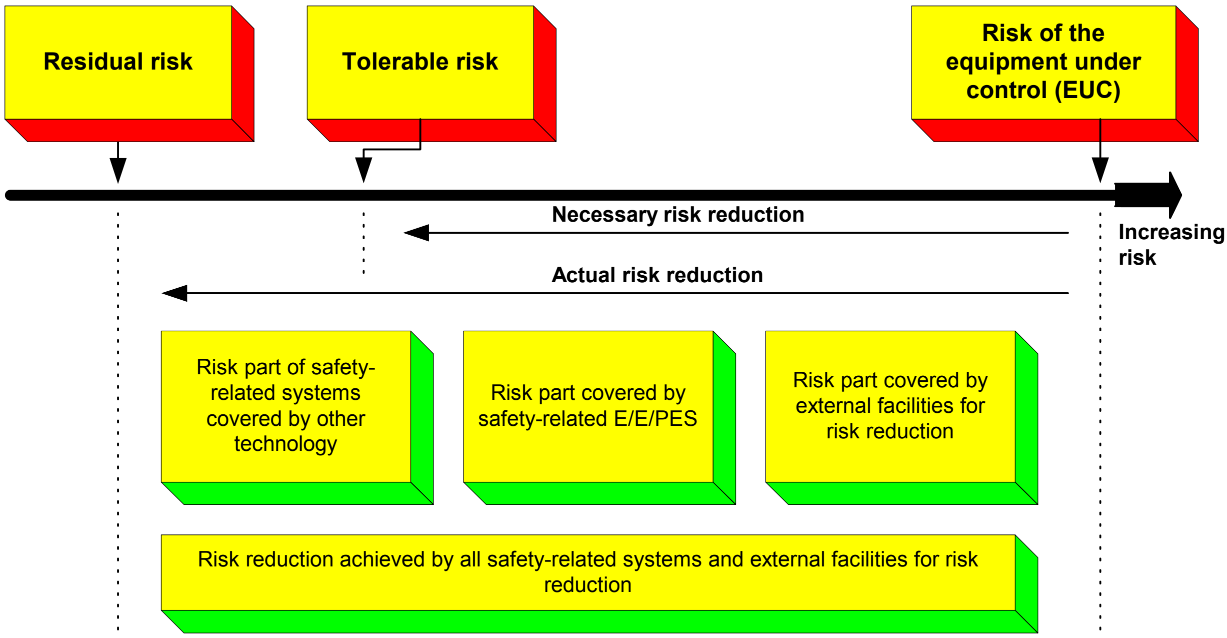


Fig. 6: General Concepts for Risk Reduction

The term "tolerable risk" is often mentioned when considering risks. A "tolerable risk" depends on different factors such as the severity of injuries, the number of people exposed to the danger, or the frequency and duration of the exposure to the danger. Generally, the ALARP (As Low As Reasonable Practicable) method is used, which defines the following general risk classes:

- Intolerable risk
- Undesirable, tolerable risk
- Tolerable risk
- Negligible risk

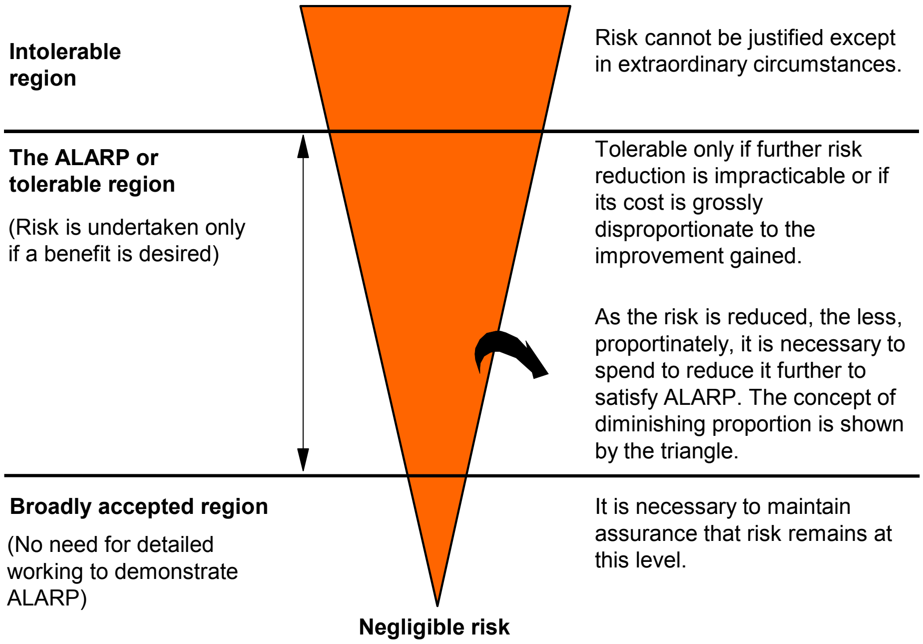


Fig. 7: Tolerable Risk and ALARP

When evaluating accidents, one should not only define the risk, but also estimate the probability that the risk will occur and the potential consequences. Using these parameters, a risk classification results as suggested in Table 4:

Risk Class	Interpretation	Valuation
Class I	Intolerable risk	Relevant
Class II	Undesirable risk, and tolerable only if risk reduction is impracticable or the costs are grossly disproportionate to the improvement gained	Relevant
Class III	Tolerable risk if the cost of risk reduction would exceed the improvement gained	Relevant
Class IV	Negligible risk	Relevant

Table 4: Risk Classification

Quantitative methods are applied for determining the safety integrity level. The standard explains how to achieve the required safety integrity using risk graph and knowledge of risk factors. This method is based on DIN V 19250 [7].

A quantitative method for determining the target safety integrity level is presented in IEC/EN 61508 in the figure below. Using this procedure, the necessary risk reduction is determined by systematically linking the tolerable risk to the risk of the EUC:

$$PFD_{avg} \leq \frac{F_t}{F_{np}} = \Delta R \quad (1)$$

Where

PFD_{avg}	is the average probability of failure on demand
F_t	is the tolerable risk frequency
F_{np}	is the demand rate on the system
ΔR	is the necessary risk reduction

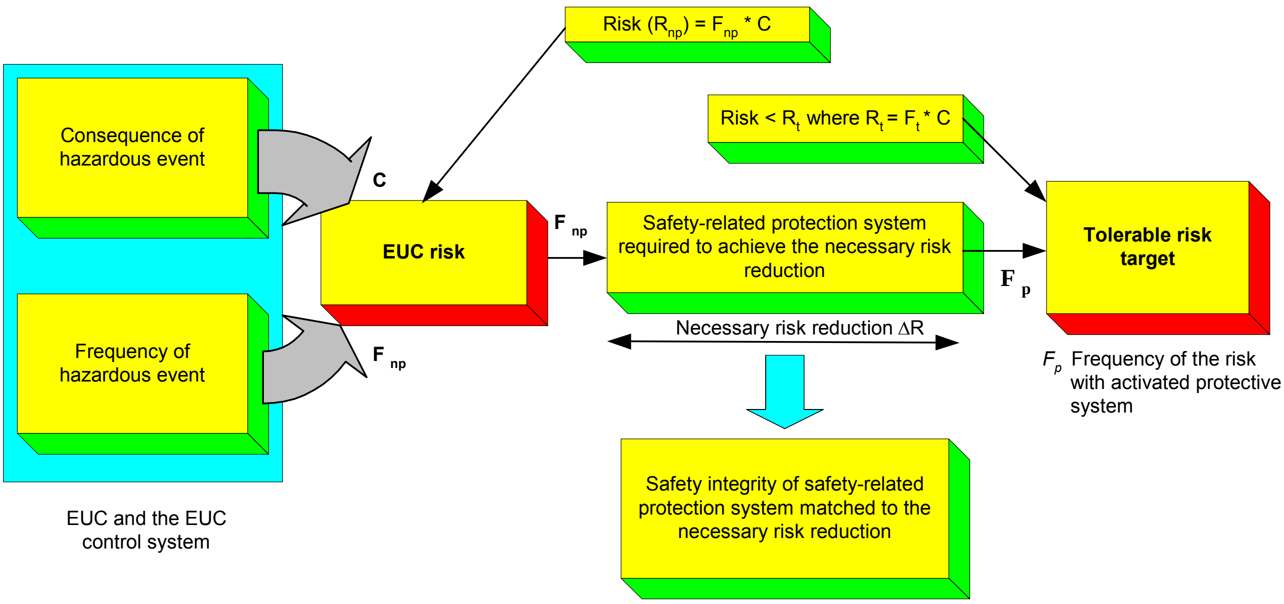


Fig. 8: Procedure for Determining a System's Safety Integrity Level (SIL)

6 Application

In addition to parts 2 and 3, part 6 of the standard contains key information on the development of safety-related systems. It provides a detailed description of quantitative calculation for safety-related systems. Further, it offers block diagrams and formulas for calculating PFD and PFH values, as well as tables for β-factors for estimating the system's diagnostic coverage capability are indicated. Finally, the standard provides tables with calculated PFD and PFH values, as well as all relevant parameters for all modified system configurations described in the norm.

The next chapters present examples of equations for determining PFD and PFH values for different HIMA systems. These calculations are based on the valid equations quoted in IEC/EN 61508 and include common-cause failures, failures that occur in the MTTR, and system failures detected during the diagnosis.

These considerations are always taken into account in all calculation and certification processes relating to HIMA systems, which consequently fully conform to IEC/EN 61508.

6.1 Conditional Equations

In this section, the individual IEC/EN 61508 equations for the various system's architectures must be presented.

6.1.1 Equation for Determining PFD of a 1oo1 System

$$\begin{aligned} PFD_{G,1oo1} &= (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE} \\ &= \lambda_D \cdot t_{CE} \\ &= \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR \right) + \lambda_{DD} \cdot MTTR \end{aligned} \qquad (2)$$

with

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \qquad (3)$$

6.1.2 Equation for Determining PFH of a 1oo1 System

$$PFH_{G,1oo1} = \lambda_{DU} \tag{4}$$

6.1.3 Equation for Determining PFD of a 1oo2 System

$$\begin{aligned} PFD_{G,1oo2} = {} & 2 \cdot \left((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU} \right)^2 \cdot t_{CE} \cdot t_{GE} \\ & + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR \right) \end{aligned} \tag{5}$$

with

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{6}$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{3} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{7}$$

Equation (5) consists of three additive terms. The first term with the squared element describes normal cause failures. The second and third terms calculate express the probability of dangerous common-cause failures due to dangerous detectable failures (failure rate λ_{DD}) and to dangerous undetectable failures (failure rate λ_{DU}) respectively.

The factor β is introduced in equation (5) to weight the individual terms and expresses the ratio between the probability of common-cause failures and the probability of incidental failures. A distinction is made between the factor β_D, which weights the common-cause element in of dangerous detectable failures, and the factor β, which weights the common-cause element in dangerous undetectable failures (see chapter 6.2 "Factors in the equations").

6.1.4 Equation for Determining PFH of a 1oo2 System

$$\begin{aligned} PFH_{G,1oo2} = {} & 2 \cdot \left((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU} \right)^2 \cdot t_{CE} \\ & + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} \end{aligned} \tag{8}$$

with

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{9}$$

6.1.5 Equation for Determining PFD of a 2oo3 System

$$PFD_{G,2oo3} = 6 \cdot \left((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU}\right)^2 \cdot t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR\right) \quad (10)$$

with

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (11)$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (12)$$

6.1.6 Equation for Determining PFH of a 2oo3 System

$$PFH_{G,2oo3} = 6 \cdot \left((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU}\right)^2 \cdot t_{CE} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} \quad (13)$$

with

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (14)$$

6.1.7 Determination of the SFF and DC Factors

The SFF (Safe Failure Fraction) and DC (Diagnostic Coverage) factors represent two other important indicators for safety-related systems. SFF expresses the proportion of safety-related failures and DC the system's diagnostic coverage capability.

The SFF factor can be calculated using the equation:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum (\lambda_{DD} + \lambda_{DU})} \quad (15)$$

The DC factor can be determined with the equation:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \quad (16)$$

6.2 Factors Used in the Conditional Equations

The meanings of the individual factors in the equations described in previous sections are listed as follow:

β	Weighting factor for dangerous undetectable common-cause failures
β_D	Weighting factor for dangerous detectable common-cause failures
λ_D	Failure rate due to dangerous failures
λ_{DD}	Failure rate due to dangerous detectable failure
λ_{DU}	Failure rate due to dangerous undetectable failure
MTTR	Mean Time To Repair
$PFD_{G*)}$	Average Probability of Failure on Demand
$PFH_{G*)}$	Average Probability of Failure per Hour
T_1	Proof-test interval
t_{CE}	Channel equivalent mean down time
t_{GE}	Voted group equivalent mean down time

*) General

Note	The equations depicted in chapter 6 are based on IEC 61508, part 6, B1.

7 Determination of the Safety Integrity

The standard shows exemplarily the procedure for determining the probability of hardware failures. First, it specifies the principles and assumptions on which the calculations are based.

For analysing the safety integrity of safety-related systems many methods are possible. Reliability block diagrams and Markov models, however, belong to the most frequently applied. If correctly applied, both methods provide almost the same results. Nevertheless, the Markov models are still more exact (but more difficult) and provide accurate values, even for complex systems.

To determine the safety integrity of safety-related systems (i.e. consisting of several individual systems), the average probability of a failure PFD_{System} or PFH_{System}, is required for the overall system.

To determine the PFD_{System} or PFH_{System} values of a safety-related overall system (i.e. consisting of the sensor system, the logic system and the actuator system), one must add the determined average probabilities for the individual systems:

$$PFD_{System} = PFD_{Sensor} + PFD_{Logic} + PFD_{Actuator} \quad (17)$$

or

$$PFH_{System} = PFH_{Sensor} + PFH_{Logic} + PFH_{Actuartor} \quad (18)$$

To determine the average probability of failure for each subsystem, following elements must be known:

- The basic architecture
- The diagnostic cover of each channel
- The failure rate of each channel
- The factors β and β_D for common-cause failures

The target is to detect common-cause failures as early as possible and to bring the system into a safe state.

Chapter 15 presents various system architectures and describes how PFD and PFH values for individual systems are determined.

The parameters listed below must be identical for all systems:

Parameter	Description	Values
β	Dangerous undetectable common-cause failure	2 %
β_D	Dangerous detectable common-cause failure	1 %
T_1	Proof-test interval	10 years
$MTTR$	Mean Time To Repair	8 hours

8 Working with *SILence*

SILence allows the calculation of the functional safety of safety-related systems and modules according to the IEC/EN 61508. The user can assemble these systems and modules using the libraries provided. Furthermore the user has the option to freely configure modules.

The calculation of the functional safety is *one* condition for the SIL classification of a plant. Further conditions must be determined together with the responsible certification authority or with an expert.

SILence enables the user to assemble a complete system or only individual modules and to calculate them within a short time frame. In his system configuration, the user can also modify and calculate within a short period:

- Different parameters,
- Different combinations of modules and
- Different proof-test intervals

This permits to immediately recognize the effects that a modification may have on the plant.

8.1 Short Description of Architectures

Architecture	Description
1oo1	The architecture consists of a single channel for the safety function; any hazardous failure causes the failure of the safety function, if this is demanded.
1oo2	The architecture consists of two redundant channels and both of them can process the safety function. In this case, the safety function on demand will only fail if a hazardous failure occurs in both channels (AND principle).
2oo2	The architecture consists of two parallel channels and both must demand the safety function before it can be processed (OR principle).
2oo3	The architecture consists of three redundant channels that are connected with a majority output device. The output state does not change if the result of only one channel does not conform to the other two.

oo Abbreviation for ”out of”

Table 5: Short Description of Architectures

8.2 Program Description

The user can create, save and load projects. A project consists of at least one system (loop), which is made up of single systems such as sensor (input), a CPU (logic subsystem) and actuator (output).

The software calculates the SIL category and the MTTF, PFD, PFH and SFF values for systems and modules created by the user.

Note	In ***SILence***, not more than 20 systems should be created in one project. If more than 20 systems are needed, the systems must be distributed over different projects.

Note	It is only possible to process projects and systems which have been created in ***SILence***.

The following chapter explains the structure of a project.
Knowledge of the structure is an important prerequisite for correctly operating ***SILence***.

The structure describes the layout of a system in ***SILence***, from the "Project" down to the lowest "Function Unit".

8.2.1 Project Structure

8.2.1.1 Projects

In ***SILence***, a project contains the created systems.

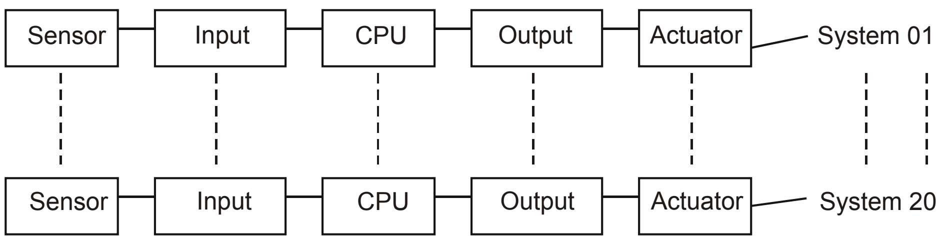


Fig. 9: Project with 20 Systems

8.2.1.2 Systems

In ***SILence***, a system consists of single systems such as sensors (input), a CPU (logic subsystem) and actuators (output).

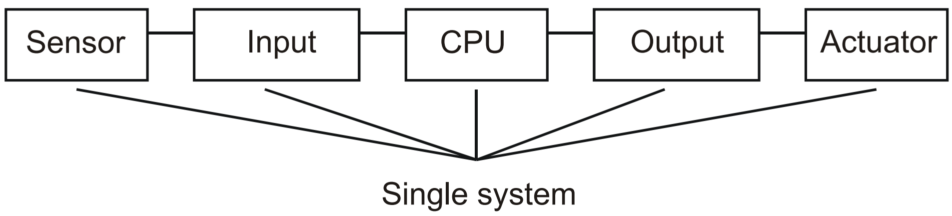


Fig. 10: A New System with Five Single Systems

8.2.1.3 Single Systems

Each single system has an architecture, which consists of one or more modules.

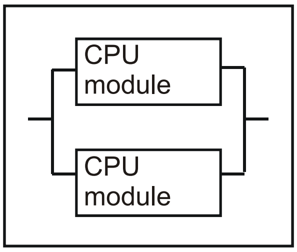


Fig. 11: Single System with Two Modules

8.2.1.4 Modules

The user can select predefined modules from the libraries or freely configure his modules.

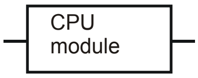


Fig. 12: One Module

8.2.1.5 Components

A module consists of components, such as CPU, watchdog, power supply monitoring unit, etc.

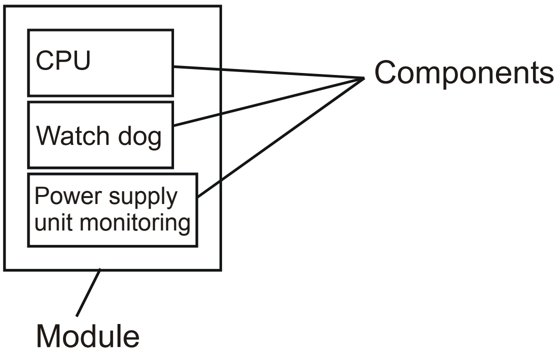


Fig. 13: Module with Three Components

8.2.1.6 Units

A component has its own architecture (1oo1, 1oo2, 2oo2, 2oo3), made up of individual units. These units are described by the parameters λ_{DD}, λ_{DU} and λ_S.

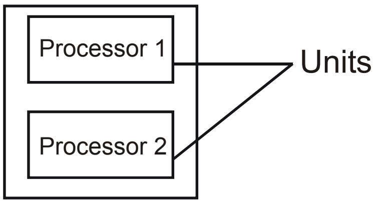


Fig. 14: CPU Component Consisting of Two Units

9 Quick-Start

- Start ***SILence*** to automatically create a new project.
- Select *File → New System.* The dialog box “Select System” opens.
- Select the option “Predefined System” to automatically open the editor and the predefined system.
- Right-click on the system’s empty module fields to open the context menu for the selection of modules.
- After configuration, the calculated results for PDF and PFH are displayed in the “Computation” tab.

Note	See chapter 13 for more details on the configuration and calculation of systems (loops) in ***SILence***.

Note	References to the installation and registration of ***SILence*** are located on the CD and in the appendix B of this manual.

10 Main Window

The ***SILence*** main window consists of the two following sub-windows: the tabs “Libraries” and “Systems”, and the “Working Area”.

The software is operated using menu functions and buttons.

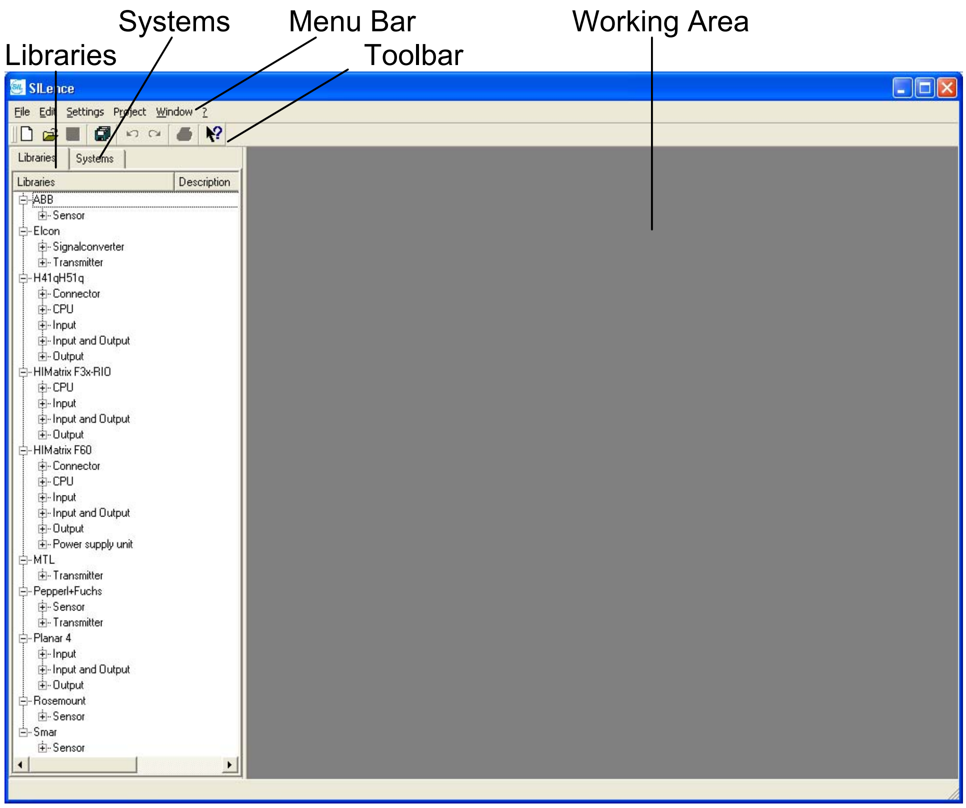


Fig. 15: *SILence* Main Window

10.1 “Libraries” Tab

The “Libraries” tab is located in the left side of the main window and contains the “Libraries” and “Description” columns. The libraries are grouped in directories and subdirectories.

10.1.1 “Libraries” Column

The libraries delivered with ***SILence***, as well as any new module libraries are displayed in the “Libraries” column.

10.1.1.1 HIMA Module Libraries

The HIMA module libraries contain the modules for the following HIMA systems:

- Planar 4
- HIMA H41q/H51q
- *HIMatrix* F3x
- *HIMatrix* F60

Note	For HIMA modules, you may only use libraries authorized by HIMA.

10.1.1.2 Manufacturer Module Libraries

The manufacturer module libraries provided by HIMA contain a selection of different third party manufacturers modules (e.g. sensors, valves, transmitters). The manufacturer module libraries cannot be modified.

The calculation is based on the same mathematical principles as the HIMA modules.

Note	HIMA does not take responsibility for the data of third party manufacturer modules, stored in the manufacturer module libraries, nor for the SIL classification in particular, derived from this data. For the correct usage of third party manufacturer modules, the instructions in the safety manual and the respective hardware manuals must be obeyed.

10.1.1.3 New Module Libraries

The user can create new module libraries.

Refer to chapter ”Adding new modules in ***SILence***” for more details.

Note	The user is responsible for the correctness of the newly created module libraries.

10.1.2 “Description” Column

The description of the modules is displayed in the “Description” column.

10.2 “Systems” Tab

The “Systems” tab lists all systems used in the current project. The “Systems” tab contains the “Systems” and “File” columns.

10.2.1 “System” Column

The system name is displayed in the column “System”.

10.2.2 “File” Column

The file root is displayed in the “File” column.

10.3 Working Area

The working area is located on the right side of the main window. The editor, in which the systems are configured, is opened in the working area.

10.4 Toolbar

The toolbar is located above the “Libraries” and “Systems” tabs. It provides quick access to frequently used commands. All commands can also be called via the menu.

10.5 Menu Bar

The menu bar is located just below the headline of the main window.

All menu options are explained in the following chapters.

11 Menus

11.1 Menu “File“

The menu “File” contains the options detailed in the following sections.

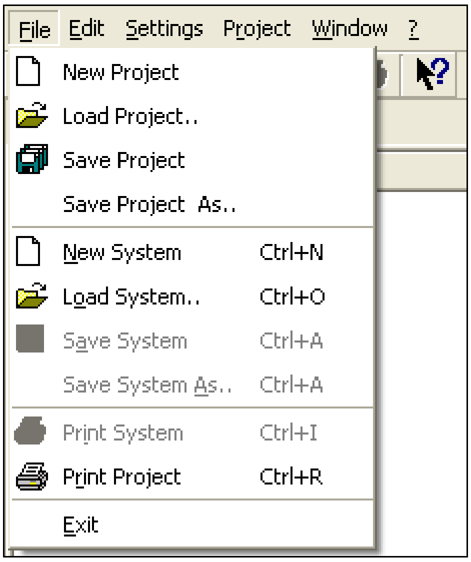


Fig. 16: Menu “File”

11.1.1 New Project

A new project can be created in two ways:

1. When started, ***SILence*** automatically creates a new project.
2. Select *File* → *New Project* menu option.

Note	Only one project at any given time may be opened. To avoid data loss, always save the current project before opening a new project.

11.1.2 Load Project…

Select *File* → *Load Project*.. to open the standard dialog box containing all projects with the “*.spr” file extension. After selecting and loading a project, all of the project’s systems will be listed in the *Systems* tab.

11.1.3 Save Project

Select *File → Save Project* to save the current project in the directory in which it was created. If the project is new, a standard dialog box opens. Select the path and enter the project name. After confirming the action, the project is automatically saved with the "*.spr" file extension.

When a project is saved, all of the project's systems are saved as well; however, systems can be saved individually for use in other projects by selecting *Save System*.

11.1.4 Save Project As..

Select *File → Save Project As..* A standard dialog box opens. Select the path and enter the project name. After confirming the action, the project is automatically saved with the "*.spr" file extension.

11.1.5 New System

Select *File → New System* to create a new system. The dialog box "SILence-System Selection" opens. Specify whether you want to create a new system or a predefined system.

11.1.5.1 Create New System

In a new system, the Editor contains only the single system "CPU". The user must configure the entire system.

11.1.5.2 Select Predefined System

Select a predefined HIMA System to open the system editor and the selected system.

The user cannot modify a predefined HIMA System, but he can add single systems to the left (inputs) or/and to the right (outputs) of the HIMA System.

In addition, he can create his own predefined systems using the System Editor.

In a project, the user can configure as many systems as desired; the only restrictions are the PC resources.

11.1.6 Load System..

Select *File → Load System..* to open the standard dialog box containing all systems with the "*.ssy" file extension. Select and load the system, to open the Editor and to edit the system.

11.1.7 Save System

Select *File → Save System* to save the current system in the directory in which it was created. If the system is new, a standard dialog box opens. Select the path and enter the system name. After confirming the action, the system is automatically saved with the "*.ssy" file extension.

11.1.8 Save System As..

Select *File → Save System As..* A standard dialog box opens. Select the path and enter the project name. After confirming the action, the project is automatically saved with the "*.ssy" file extension

11.1.9 Print System

Select *File → Print System.* A standard dialog box opens. If required, select the printer and change printer settings. Click *OK* to confirm the action. Optionally, click the printer button on the toolbar to print the current system with the default printer.

11.1.10 Print Project

Selecting *File → Print Project.* A standard dialog box opens. If required, select the printer and change printer settings. Click *OK* to print the current project, including all systems.

Note	In ***SILence***, the project documentation printout is an important element. For this reason, it is a part of the TÜV approval process.

11.1.11 Exit

Select *File → Exit* to close ***SILence***.

Note	To avoid data loss, always save the current project before closing ***SILence***.

11.2 Menu “Edit”

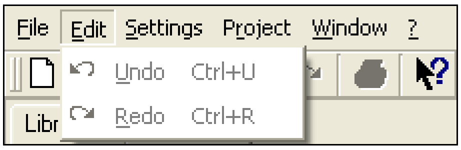


Fig. 17: Menu “Edit”

11.2.1 UNDO

Select *EDIT → UNDO* to cancel the last five actions in the project editor. This function can also be executed, if the project have been saved and reloaded.

The *UNDO* function can either be selected via the menu or by clicking the *UNDO* button on the toolbar.

11.2.2 REDO

Select *EDIT → REDO* to repeat the last five *UNDO* actions. This function can also be executed, if the project have been saved and reloaded.

The *REDO* function can either be selected via the menu or by clicking the *UNDO* button on the toolbar.

11.3 Menu “Settings”

The menu “Settings” contains the options detailed in the following sections:

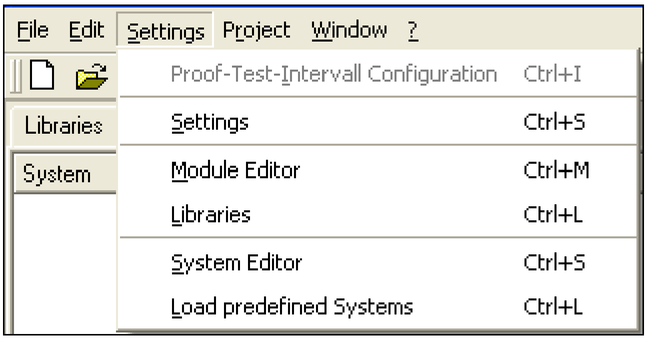


Fig. 18: Menu “Settings”

11.3.1 Proof-Test-Interval-Configuration

Fig. 19: “Proof-Test-Interval Configuration” Dialog Box

PFD and PFH results depend on the proof-test interval. The proof-test interval is the time span, for which the user wants to observe the probability of failure of the overall system.

For each system, the user can set up to five proof-test intervals:

- Range: 1 month … 20 years and 11 month
- Resolution: 1 month

The proof-time intervals set in the dialog box are automatically assigned to the current systems.

Note The user can only set the “Proof-Test-Interval Configuration“ option if a system is opened.

11.3.2 Settings

Select *Settings* → *Settings.* The dialog box “SILence-Settings” with the following options opens:

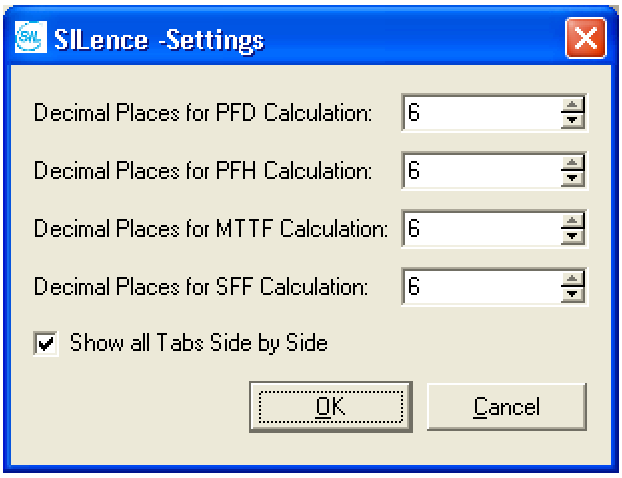


Fig. 20: „Settings“ Dialog Box

11.3.2.1 Decimal Number Places

In this record, the user can choose the number of decimal places for PFD, PFH, MTTF and SFF calculations (1 to 6).

This action only affects the display and printout, but has no influence on the calculation accuracy.

11.3.2.2 Show all Tabs Side by Side

If the check box is activated, the system is displayed in the editor's "System" tab.

If the check box is deactivated, the Editor is divided into two halves:

- The system is displayed in the upper half
- The tabs "Calculation" and "History" are displayed in the lower half.

11.3.3 Module Editor

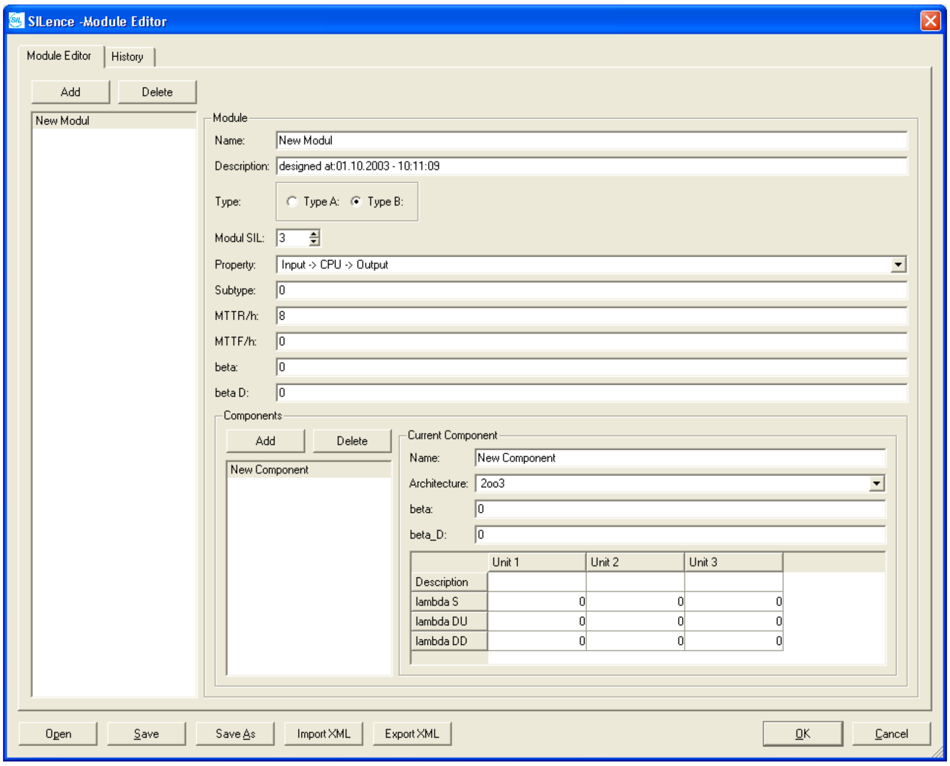


Fig. 21: "Module Editor" Dialog Box

Note	In the Module Editor, the user can create, configure and extend modules and module libraries. See chapter 14 "Adding new modules" for more details.

Select *Settings → Module Editor* to open the Module Editor.

The “Module Editor” dialog box contains the “Module Editor” and “History” tab, as well as the following common buttons:

Open
Using this option a standard dialog box opens. Select the module library from the corresponding list (all module libraries have the “*.sdd” file extension) and confirm the action. Loaded module libraries are displayed in the editor’s module list.

Save
Choose this option to save the module library in the directory, in which it was created. If the library is new, a standard dialog box appears. Select the path and enter the library name. After confirming the action, the library is automatically saved with the “*.sdd” file extension.

Save As
Using this option a standard dialog box opens. Select the path and enter the library name. After confirming the action, the library is automatically saved with the “*.sdd” file extension.

Note	Optionally, the user can add own module libraries clicking on the *Save As* button located in the Module Editor.

Import XML
Choose this option to open a standard dialog box containing all module libraries with extension “*.xml”. Select and load the XML module library. The corresponding modules are displayed in the Editor’s module list.

Export XML
Using this option a standard dialog box opens. Select the path and enter the module library name. After confirming the action, the library is saved automatically with the “*.xml” file extension.

Note	The XML files must keep the library structure of ***SILence***. See also to chapter 14.1.2 “Adding new modules using XML import”.

OK
Click *OK* to confirm recent actions (e.g. Add, Remove). The dialog box will close.

Cancel
Click *Cancel* to abort all actions (e.g. Add, Remove) without changing the project. The dialog box will close.

11.3.3.1 “Module Editor” Tab

In the “Module Editor” tab, the user can edit modules and module libraries. The modules are displayed in the module list.

The *Add* and *Delete* buttons are located above the module list.

Add
Choose this option to add a new module to the module list, which with the default name “New Module”. New modules require unique names.

Delete
Choose this option to remove a selected module from the module list.

Configuring Module Parameters
After selecting a module from the module list, the parameters of the selected module are displayed in the “Module” field. From this field, the user can edit the parameters.

Module Parameter	Description
Name	Name of the selected module (max. 15 characters)
Description	Description of the module
Type	See chapter 3 “Hardware Requirements” (Type A/B)
Module SIL (1 to 4)	Certified SIL (according to the module manufacturer’s specifications)
Property	Module type (e.g. Sensor, Input, CPU, Output, Actuator…)
Subtype (0 to 9999)	Only modules of the same subtype may be interconnected redundantly.
MTTR/h (Default: 8 h)	Mean Time To Repair
MTTF/h	Mean Time To Failure
β [1)]	Weighting factor for dangerous undetectable common-cause failures of the module
$β_D$ [1)]	Weighting factor for dangerous detectable common-cause failures of the module

1) For modules of third-party manufacturers, the β-factors are located in the corresponding data sheets

Configuring Module’s Component Parameters
A module consists of individual components, which are considered during the calculation of failures with their respective λ and β values. Module components are for example CPU, I/O bus, serial port or the power supply monitoring unit. All module components are displayed in the module editor’s component list.

The *Add* and *Delete* buttons are located above the module list.

Add
Choose this option to add a new module to the module list with the default name “New Component”. New components require unique names.

Delete
Choose this option to remove a selected component from the component list.

After selecting a component from the component list, the parameters of the selected module are displayed in the "Current Component" field. From this field, the user can edit the parameters.

Component Parameters	Description
Name	Name of the selected component
Architecture	Select the component architecture in the drop-down list (1oo1, 1oo2, 2oo2, 2oo3)
β [1)]	Weighting factor for dangerous undetectable common-cause failures of the module
β_D [1)]	Weighting factor for dangerous detectable common-cause failures of the module

1) For modules of third-party manufacturers, the β-factors are located in the corresponding data sheets. The β-factors of a component can differ from the β-factors of the module

Configuring Unit Parameters
Depending on its architecture (1oo1, 1oo2, 2oo2, 2oo3), a component can consist of up to four "units". The units are automatically displayed with the component.

The unit parameters of the selected component are displayed in the field "Current Component" at the bottom of the Module Editor tab and can be changed by the user.

Unit Parameters	Description
Description:	Name of the unit
λ_S [1)]	Safe failure rate (per hour)
λ_{DU} [1)]	Undetected dangerous failure rate (per hour)
λ_{DD} [1)]	Detected dangerous failure rate (per hour)

1) For modules of third-party manufacturers the λ-factors have to be taken from their data sheets.

Note	Modules of third-party manufacturers can be configured freely. HIMA modules and manufacturer modules from the ***SI-Lence*** Libraries are predefined and cannot be changed.

Note	The user is responsible for ensuring the correctness of the parameters he entered.

11.3.3.2 “History“ Tab

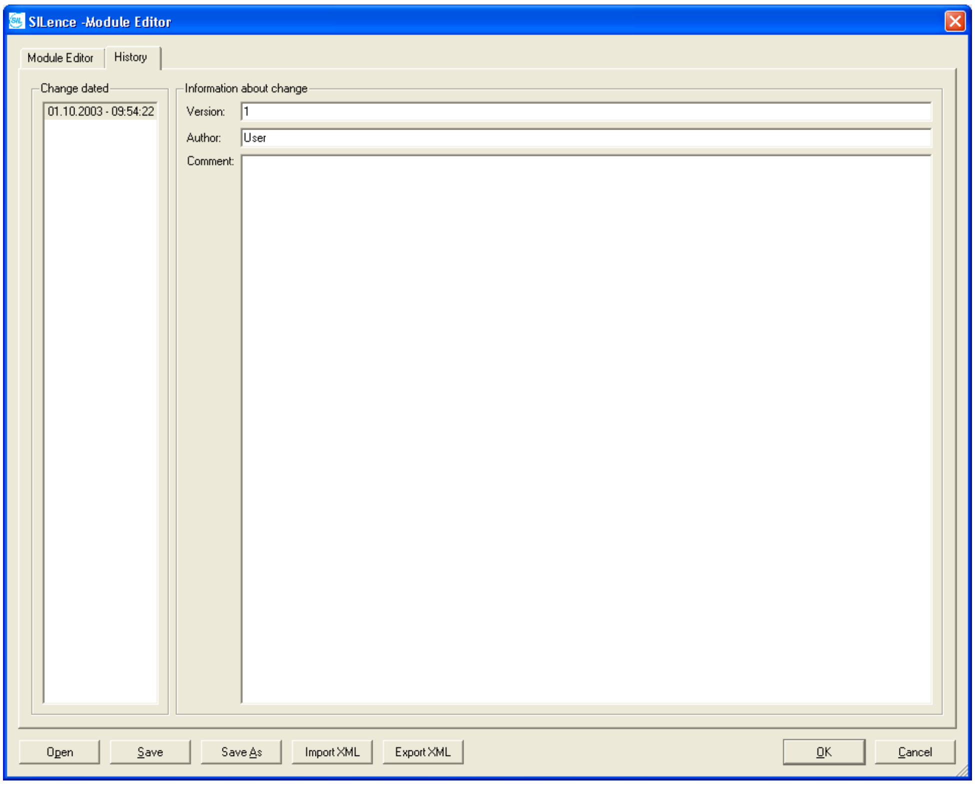


Fig. 22: “History” Tab

The “History” tab contains the “Date/Time”, “Version”, “Author” and “Comment” records for the current library. From the history list on the left, the user can select the record he wants to view.

Only entries of the current library history may be changed. All other entries are write-protected.

11.3.4 Libraries

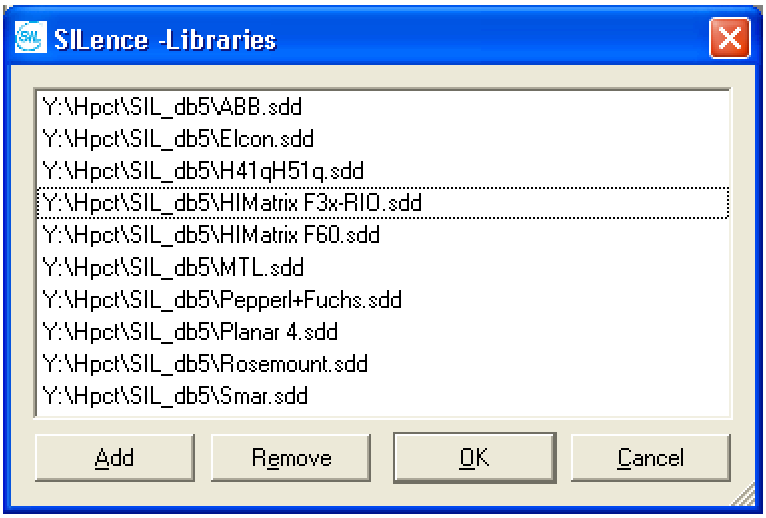


Fig. 23: “Libraries“ Dialog Box

Select *Settings* → *Libraries* to open the dialog box “Libraries”, containing the *Add* and *Remove* buttons.

Add
Click *Add* to open a standard dialog box in which all library files with the extension “*.sdd” are listed. Select a library and add it to the project. The library modules are displayed in the main window library list.

Remove
Select the library in the “Libraries” dialog box and click *Remove* to remove a library from a project.

OK
Click *OK* to confirm recent actions (e.g. Add, Remove). The dialog box will be closed.

Cancel
Click *Cancel* to abort all actions (e.g. Add, Remove) without changing the project. The dialog box will be closed.

11.3.5 System Editor

Use the "System Editor" to add, remove and configure systems.

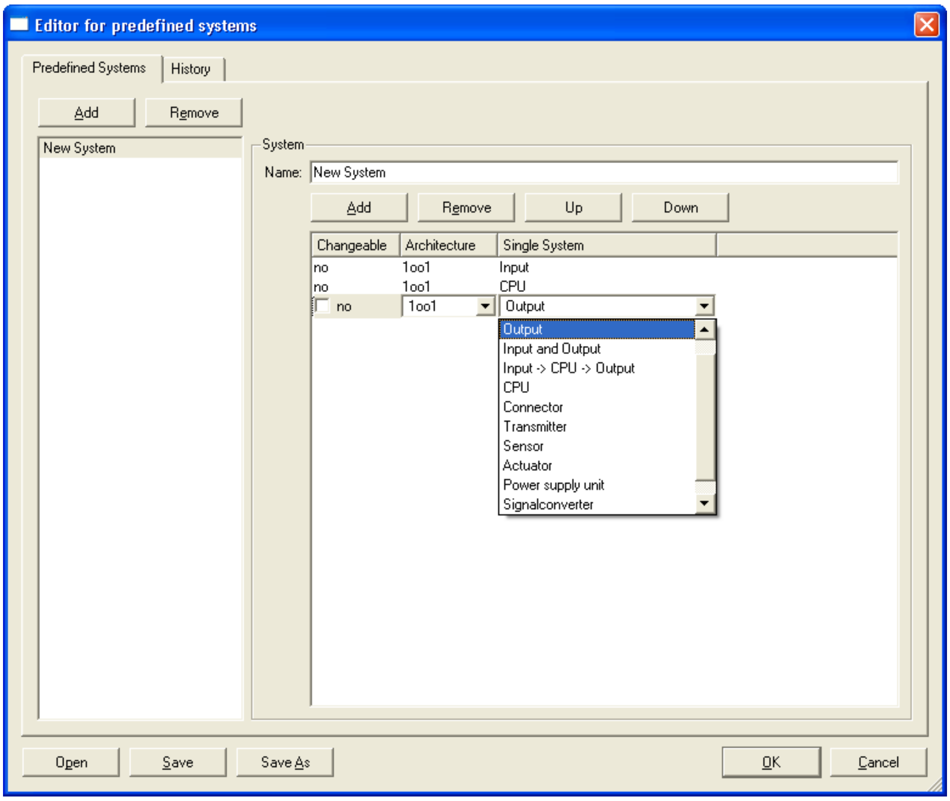


Fig. 24: "System Editor" Dialog Box

The System Editor contains the "Predefiened System" and "History" tab and the common buttons explained below:

Open
Using this option a standard dialog box opens. Select the system from the corresponding list (all systems have the “*.sds” file extension) and confirm the action. Loaded systems are displayed in the System Editor's system list.

Save
Choose this option to save the system in the directory, in which it was created. If the system is new, a standard dialog box appears. Select the path and enter the system name. After confirming the action, the system is automatically saved with the “*.sds” file extension.

Save As
Using this option a standard dialog box opens. Select the path and enter the system name. After confirming the action, the system is automatically saved with the “*.sds” file extension.

OK
Click *OK* to confirm recent actions. The System Editor will be closed.

Cancel
Click *Cancel* to abort all recent actions. The System Editor will be closed.

11.3.5.1 “Predefined System“ Tab

Above the system list there are the following buttons:

Add
Click *Add* to add a new system to the system list. Newly created system have the default name “New System”.

Remove
Click *Remove* to remove a selected system from the system list.

In the “System“ dialog box on the right side of the “Predefined System” tab, the properties of the selected system are displayed and can be modified.

In this input field appears the name of the selected system. If requiered, the user can change it.

Add
Click *Add* to add a single system to the current system.

Remove
Click *Remove* to remove the selected syngle system from the corresponding list.

Up and *Down*
Use the *Up* and D*own* button to change the sequence of the single systems in the current system.

Select a single system from the corresponding list to activate the drop-down box in each column of the single system. The drop-down box contains the options described below:

Column	Description of the drop-down boxes
Changeable	Activate “yes” or “no” to allow or not allow the editing option in the editor
Architecture	Admitted architectures: 1oo1, 1oo2, 2oo2, 2oo3
Single System	Single system's type: “Sensor”, “Input”, “CPU”, “Output”, “Actuator”, etc.

11.3.5.2 "History" Tab

The "History" tab contains the "Date/Time", "Version", "Author" and "Comment" records for the current library. From the history list on the left, the user can select the record he wants to view.

Only the entries of the current history of a library may be changed. All other entries are write-protected.

11.3.6 Load Predefined System

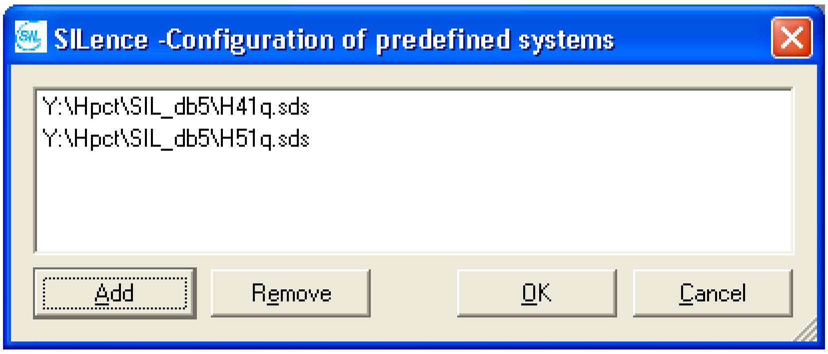


Fig. 25: "Configuration a Predefined System" Dialog Box

Select *Settings* → *Load Predefined System* to open the "Configuration of predefined systems" dialog box containing the following buttons:

Add
Click *Add* to open a standard dialog box containing the list of all system libraries with the "*.spr" file extension. Select a library to add it to the project.

Remove
Select a predefined system library and click *Remove* to remove the predefined system library from a project.

The user can create and edit predefined system libraries in the System Editor. He can use system libraries located in the library list to create predefined systems. Predefined system libraries have the "*.sds" file extension.

11.4 Menu “Project“

11.4.1 Project History

Fig. 26: Menu “Project“

Select this option to display the “Date/Time”, “Version”, “Author” and “Comment” records for the current library. From the history list the user selects the record he wants to view.

Only the entries of the current project history may be changed. All other entries are write-protected.

11.5 Menu “Window“

Fig. 27: Menu “Window“

This menu contains the standard options for arranging windows (e.g Cascading, Horizontal Tile, Tile), as well as the list of all active windows.

11.6 Menu “?“

Standard menu providing information about ***SILence***.

Fig. 28: Menu “?“

12 Editor

12.1 “System” Tab

Fig. 29: “System” Tab

A system is divided into single systems and displayed in the editor's "System" tab. Single systems are generally configured in the “System” tab by dragging modules from the module list into module dummies (See Menu “Settings”).

12.1.1 Edit Single Systems

A ***SILence*** system consists of at least one single system, to which the user can add further single systems.

The following sections describe how to configure single systems.

12.1.1.1 Defining an Architecture

The drop-down list is located at the top of each single system.

The user can select one of the following architectures in the drop-down list:

Architecture	Number of Modules
1oo1	1
1oo2	2
2oo2	2
2oo3	3

12.1.1.2 Single System's Context Menu

Right-clicking on the single system opens the corresponding context menu, which contains the following options:

Remove single system
Select this option to remove the single system, from which the context menu has been opened.

Add single system right/left
Select this option to add one of the following single systems to the right or left of the current single system:

Single System	Description
Input	Input module
Output	Output Module
Input and Output	Input/Output Module
Input → CPU → Output	HIMatrix Compact System
CPU	CPU Module
Connector	Coupling Module
Transmitter	Current, Voltage Transmitter
Sensor	Pressure, Temperature, Gas Sensor
Actuator	Valve, Pump, Motor
Power supply unit	Power Supply Unit
Booster	Booster

Move single system one step to the right/left
Select this option to swap the current single system's position with the single system adjacent to it (i.e. to the right or left).

12.1.1.3 Insert/Remove Modules

In a single system, empty module dummies are represented by rectangles. The number of rectangles depends on the architecture chosen for the single system. A right-click on a rectangles opens a context menu, which allows the user to fill the rectangles with modules.

Insert Module
This option displays the list of all modules allowed for this module dummy. Select one of the modules to fill the rectangles with a module icon.

Delete Module
A right-click on the module dummy opens a context menu containing the list of all modules and the option *Delete Module.*
Click the *Delete Module* option to remove the module from the module dummy.

12.2 “Calculation” Tab

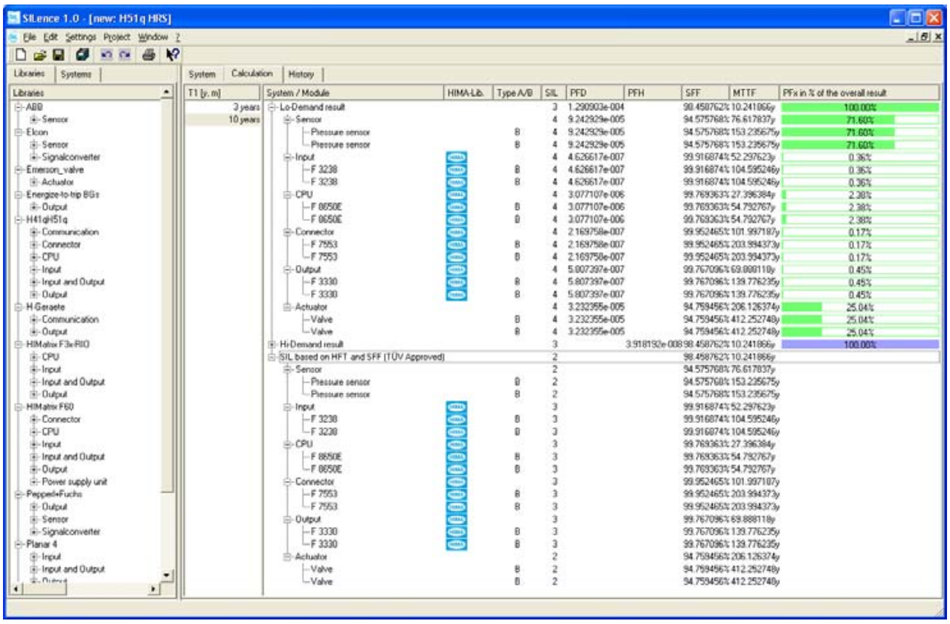


Fig. 30: “Calculation” Tab

The "Calculation" tab is divided into several columns, in which the calculations for the current system and its modules are displayed.

The following sections describe the properties of each column.

12.2.1 “T1[y, m]” Column

The results calculated for PFD and PFH depend on the proof time interval. The proof time interval is the time span, for which the user wants to observe the probability of failure of the overall system.

12.2.2 “System/Module” Column

The “System/Module” column lists all project systems and modules in a structure tree. Systems and modules are grouped in Lo-Demand and Hi-Demand results.

12.2.2.1 “Lo-Demand-Result”, “Hi-Demand-Result” and “SIL based on HFT and SFF (TÜV Approved)” Directories

The “Lo-Demand-result” directory provides the results calculated for Low Demand Mode. Lo-Demand-results’ calculations are based on the equations for determining PFD cited in IEC 61508.

The “HI-Demand-result” directory provides the results calculated for High Demand Mode. HI-Demand-results’ calculations are based on the the equations for determining PFH presented in IEC 61508.

The „SIL based on HFT and SFF (TÜV Approved)” directory shows the TÜV approved SIL. Configuring the module using the Module Editor,

SILence estimates the SFF and HFT and considers the resulting values for determining the SIL.

Note	The overall system's SIL depends on the module or single system with the worst values.

Note	The functional safety of every safety function's target SIL must be proven, in accordance with the applicable norms. The SIL specified in the manufacturer's documentation is a deciding factor for the SIL specification of a component. The documentation details the examination and certification of this SIL.

12.2.2.2 “Single Systems“ Subdirectory

The single systems are listed in the same order as configured in the editor's “System” tab.

12.2.2.3 “Modules“ Subdirectory

The number of modules in the module list depends on the architecture configured for the single system.

12.2.3 “HIMA-Lib.“ Column

If a library module provided by HIMA is opened, the HIMA logo will appear in this column.

12.2.4 “Type A/B“ Column

The “Type A/B“ column displays the type of module. See chapter 3 “Hardware Requirements” for more details.

12.2.5 “SIL“ Column

The “SIL“ column displays the theoretical or certified “Safety Integrity Level” (SIL) for the system and modules.

12.2.6 “PFD“ Column

The “PFD“ column displays the results for “Probability of Failure on Demand” calculated for the system and modules.

Note	If PFD $\geq$ 0.1, it is not possible to classify the SIL in a SIL category (1 to 4). In this case, verify the parameters entered in the system and consider the examples in IEC/EN 61508, part 6.

12.2.7 “PFH“ Column

The “PFH“ column displays the results for “Probability of Failure per Hour” calculated for the system and modules.

Note	If PFH ≥ 10^{-5}, it is not possible to classify the SIL in a SIL category (1 to 4). In this case, verify the parameters entered in the system and consider the examples in IEC/EN 61508, part 6.

12.2.8 “SFF“ Column

The “SFF“ column displays the percentage for the „Safe Failure Fraction“ value.

12.2.9 “MTTF“ Column

The “MTTF“ Column displays the “Mean Time To Failure” value for the system and modules and is expressed in years.

12.2.10 “PFx in % of the overall result“ Column

The “PFx in % of the overall result” column contains the ratio between the results (PFH and PFD) calculated for the modules and the system’s overall result, expressed in percentage. It is displayed as a bar chart.

$$PFx\ in\%\,einer\ Baugruppe = \frac{PFx_{Baugruppe}}{PFx_{System}} * 100\%$$

At this stage, the user can note which modules have a stronger or weaker effect on the overall result and can improve the system’s overall result by replacing the appropriate module.

Note	If the system is not complete and does not contain all modules, it is not possible to calculate any kind of results. The entire line will be displayed in red. All columns whose results cannot be calculated are empty.

12.3 “History“ Tab

The “History” tab contains the “Date/Time”, “Version”, “Author” and “Comment” records for the current system.

From the history list on the left, the user can select the records he wants to view.

Only entries of the current system’s history may be changed. All other entries are write-protected.

13 Configuring and Calculating Systems

The following chapters describe how to configure and calculate HIMA systems in ***SILence***, using the examples of a H51q-HRS and a *HIMatrix* system

13.1 General Settings in *SILence*

Before configuring new systems in ***SILence***, one must specify the following general settings:

Load required libraries
SILence standard libraries are loaded automatically when ***SILence*** starts. If additional libraries are required for a new system, they must be loaded before configuring the new system:

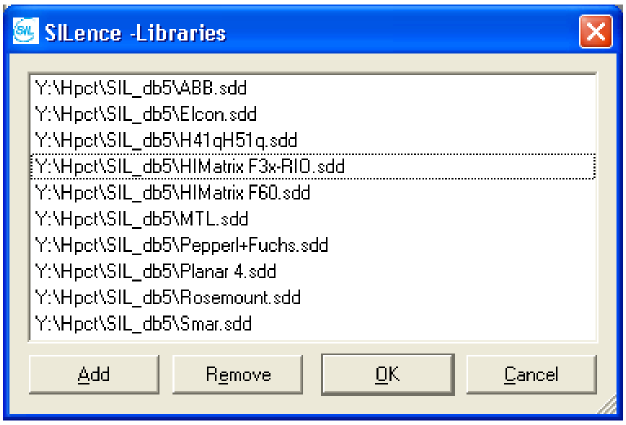


Fig. 31: Load Required Libraries

- Select *Settings* → *Libraries* to open the “Libraries“ dialog box.
- Click *Add* to open the standard dialog box for opening files.
- Select the required library file.
- Click *OK* to confirm the action.

System Representation and Decimal Number Place Settings

The system representation in the editor and the number of decimals places in the "Calculation" tab must be configured in the "Settings" dialog box.

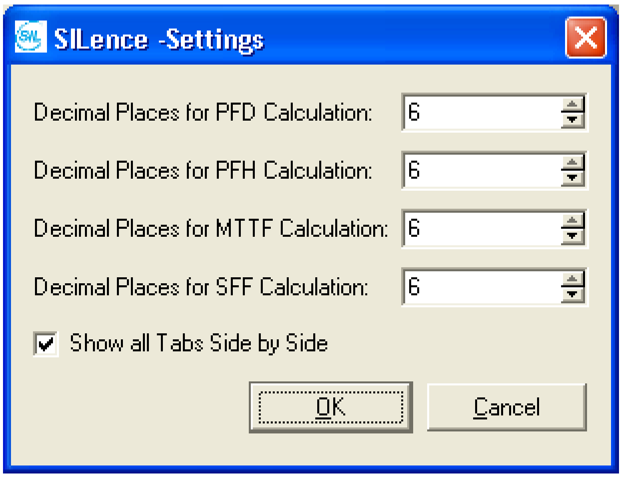


Fig. 32: System Representation and Decimal Number Settings

- Select *Settings* → *Settings* to open the "Settings" dialog box.
- Set the number of decimal places for the PFD, PFH, MTTF and SFF values (1 to 6) in the corresponding fields.
- If all registers should be displayed side by side, activate the check box *Show all Tabs Side by Side* , or
- Deactivate the check box if the *System* tab should be displayed in the upper half of the editor.

Note	The general settings may no longer be changed once the configuration is completed.

13.2 Configuring Systems in *SILence*

In ***SILence***, loops are configured in the same way as systems. A system must be configured for each loop in a controller.

Note	In ***SILence***, not more than 20 systems should be created in one project. If there are needed more than 20 systems, the systems must be distribute to different projects.

In ***SILence***, the HIMA system “H41q/H51q” is available as a predefined system in the HIMA library. The architecture of the single systems as well as their order, are strictly prescribed.
The single system modules can be selected from the respective context menu of a module reactangle.
The user can freely configure the single systems he has added on the right or left of the predefined HIMA system.

13.3 Configuring Systems using the Example of H51q-HRS

The H51q-HRS system (part of the H41q/H51q system family) has been chosen for the following example.

13.3.1 Configuration of *SILence* Loops

- On the left of the H51q-HRS system: a single system “Sensor“
- Predefined H51q-HRS-system
- On the right of the H51q-HRS system: a single system “Actuator“

***SILence* Predefined H51q-HRS System**

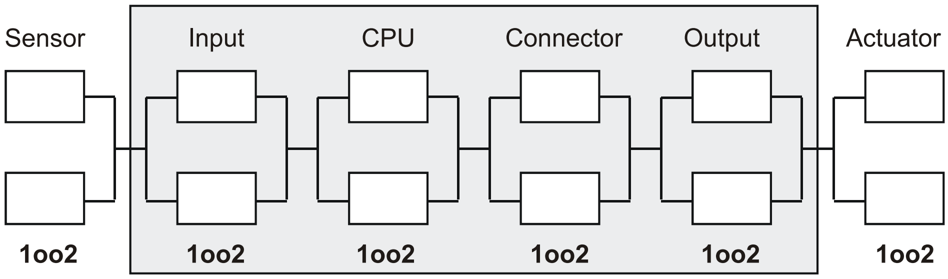


Fig. 33: Loop of a *SILence* H51q-HRS-System

Single System	Architecture	Module	Module Description
Sensor	1oo2	Pressure Sensor	Standard Pressure Sensor
Input	1oo2	F 3238	8-channel Input Module, safety related
CPU	1oo2	F 8650E	Central Module, safety related
Connector	1oo2	F 7553	Connector module
Output	1oo2	F 3330	8-channel Output Module, safety related
Actuator	1oo2	Valve	Standard Valve

Table 6: Single Systems and Modules Used for *SILence* Loop

13.3.2 Configuring Loops in *SILence*

Open the project in which the new system should be saved, or create a new project.

To create a “New System” in ***SILence***:

- Select *File → New System*. The “Select System“ dialog box opens.

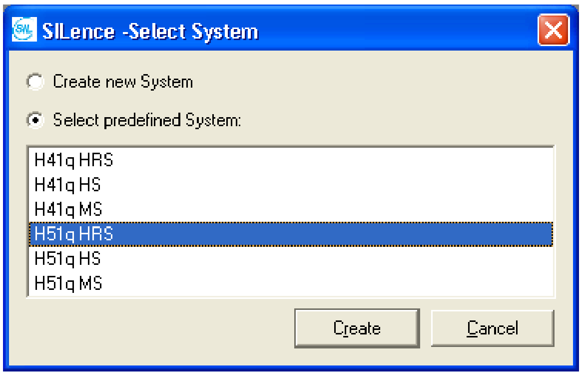


Fig. 34: “Select System“ Dialog Box

To create a predefined System (in this case “H51q-HRS“):

- Activate the option *Select predefined System* in the “Select System“ dialog box.
- Select the predefined system “H51q-HRS“ in the list of the predefined systems.
- Click *Create*. The editor opens and the new system “H51q-HRS“ is displayed in the “System” tab.

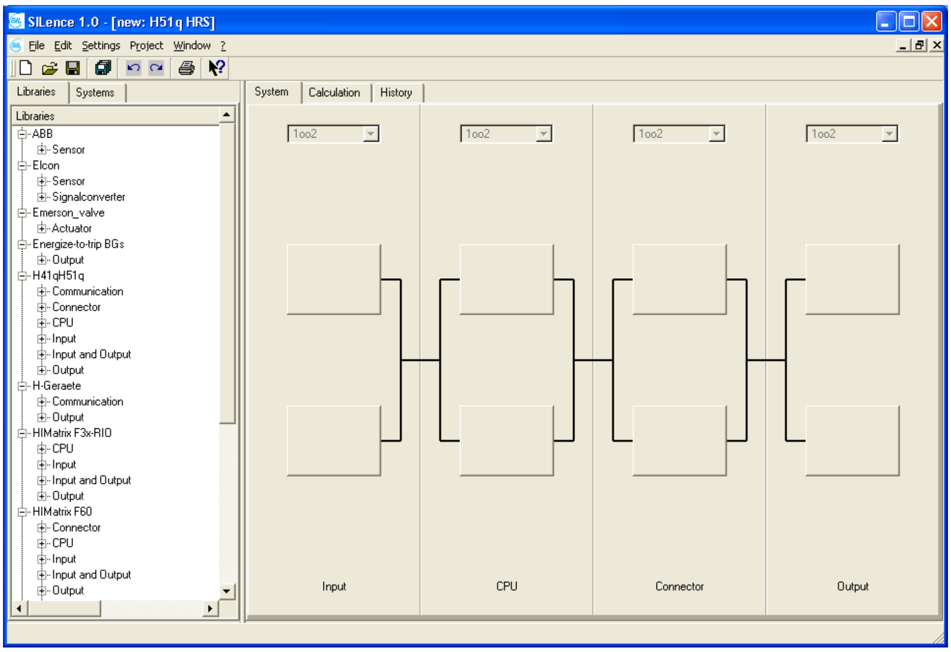


Fig. 35: A Newly Created H51q-HRS System Displayed in the Editor

To add the single system “Sensor“ to the predefined system “H51q-HRS“:

- Right-click on the single system “Input“.
- Select *Add single system to the left→ Sensor* using the context menu.
- Select an architecture (1oo2) for the new single system “Sensor“ in the drop-down list.

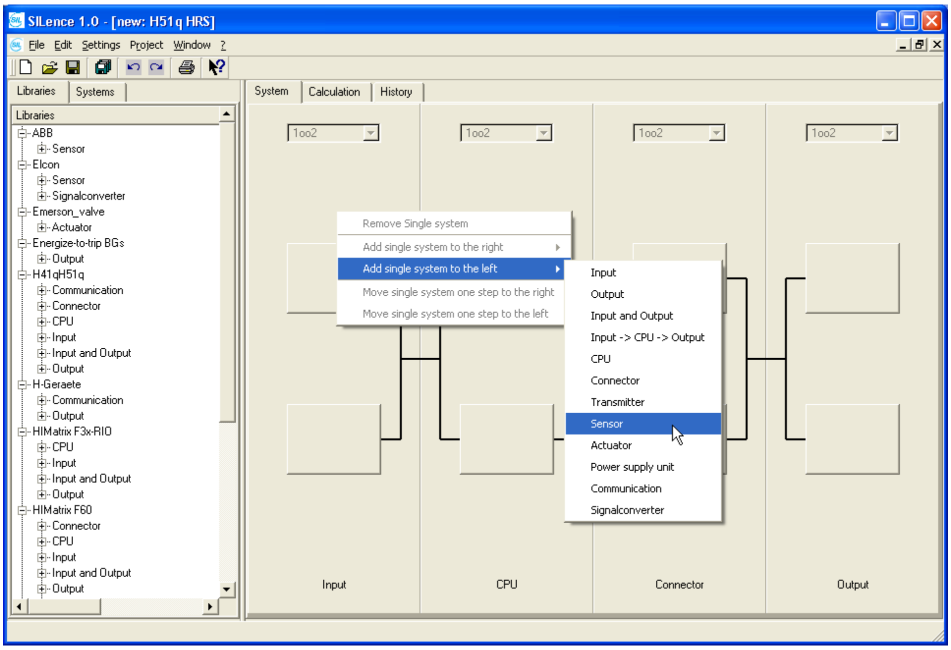


Fig. 36: Single System are Added Using the Context Menu

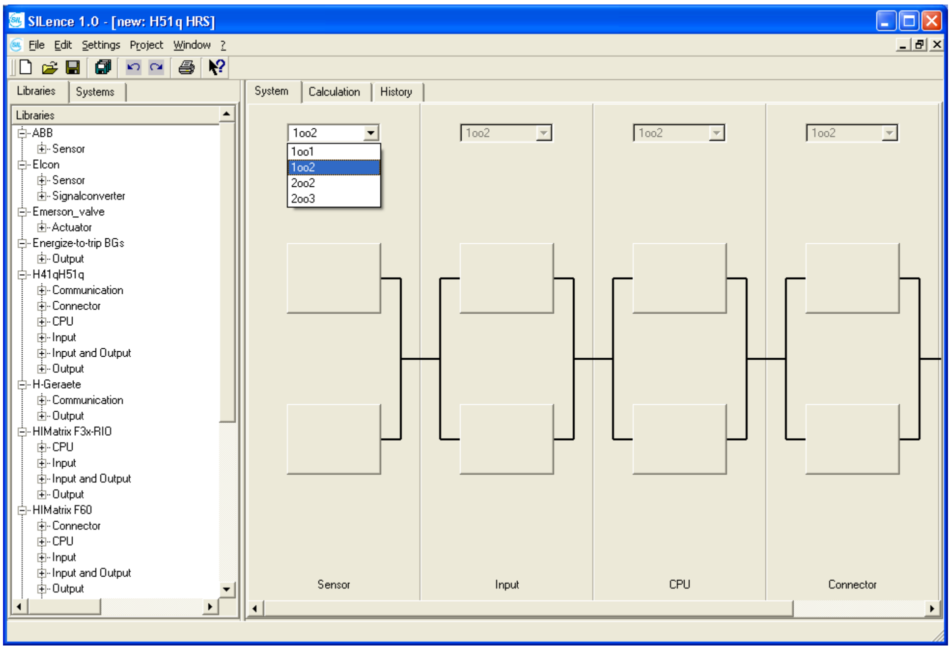


Fig. 37: Architecture Selection for a Single System

To add the single system “Actuator“ to the predefined system “H51q-HRS“:

- Right-click on the single system “Output“.
- Select *Add single system before* → *Actuator* using the context menus.
- Select an architecture (1oo2) for the new single system “Actuator“ in the drop-down list.

To set the “Proof-Test-Interval-Configuration“:

- Select *Settings* → *Proof-Test-Interval-Configuration.* The “Proof-Test-Interval-Configuration” dialog box opens.
- Select the proof-test intervals using the arrows near the field (by default: 3 and 10 years).
- Click *OK* to confirm the actions.

Fig. 38: “Proof-Test-Interval-Configuration” Settings

To add modules to the predefined system “H51q-HRS“:

- Right-click on a single system rectangle.
- Select one of the possible modules using the context menu.
- Add the following modules to the system:

Sensor	Input	CPU	Connector	Output	Actuator
Pressure sensor	F 3238	F 8650E	F 7553	F 3330	Valve
Pressure sensor	F 3238	F 8650E	F 7553	F 3330	Valve

Table 7: Modules Used for the Predefined H51q-HRS System

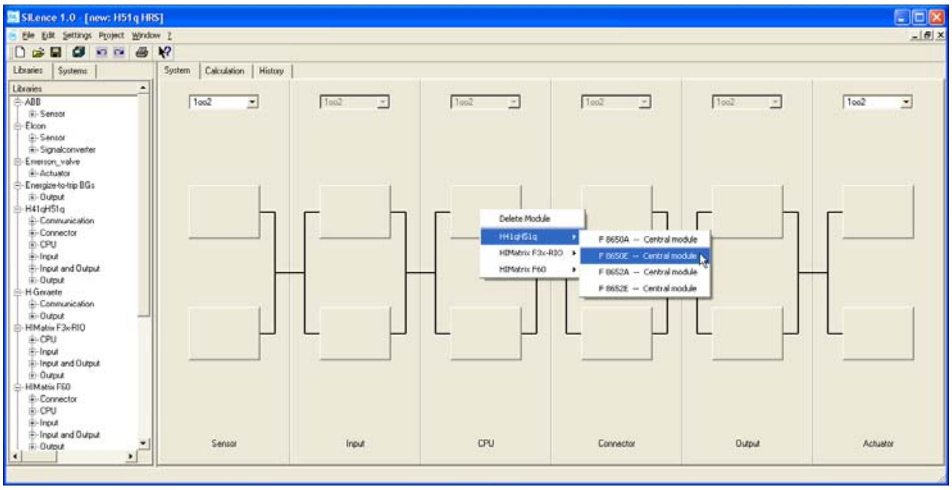


Fig. 39: Selection of Possible Modules in the Context Menu

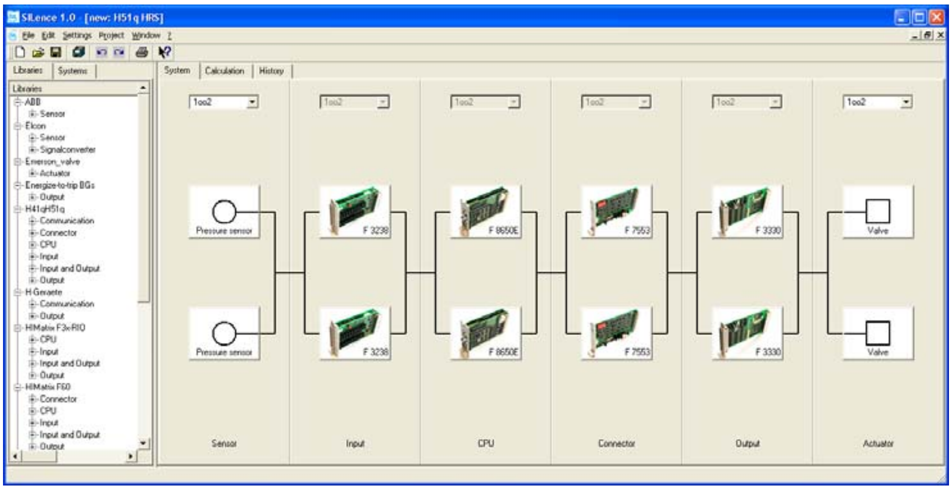


Fig. 40: Configured H51q-HRS System

To save the project and all created systems:

- Select *File* → *Project save as.. .*
- A standard dialog box opens.
- Select the directory in which the project should be saved.
- Enter the project name in the input field “File Name”.
- Click *Save* to save the project.

13.3.3 Results Calculated for the H51q-HRS System Loop

After configuring the system, the results for the configured system are displayed in the “Calculation” tab.

Lo-Demand-Result [Proof -Test Interval = 10 Years]						
System / System Parts	**Architecture**	**PFH**	**SIL**	**SFF in %**	**MTTF in years**	**PFD in % for the overall result**
Pressure Sensor	1oo2	9,243 E-5	4	94,576	76,614y	71,60
F 3238	1oo2	4,627 E-7	4	99,917	52,298y	0,36
F 8650E	1oo2	3,077 E-6	4	99,769	27,396y	2,38
F 7553	1oo2	2,170 E-7	4	99,952	101,997y	0,17
F 3330	1oo2	5,807 E-7	4	99,767	69,888y	0,45
Valve	1oo2	3,232 E-5	4	94,759	206,056y	25,04
System without Sensors and Actuators		4,337 E-6	4	99,832	12,542y	100,00
System with Sensor and Actuator		1,291 E-4	3	98,459	10,242y	100,00
TÜV claimed SIL for Systems without Sensor and Actuator			**3**			

Table 8: "Lo-Demand Results" Calculated for the H51q-HRS System Loop

After the PFD calculation, the system is categorized in the SIL 3 class.

Hi-Demand-Result [Proof-Test Interval = 10 Years]						
System / System Parts	**Architecture**	**PFH**	**SIL**	**SFF in %**	**MTTF in years**	**PFH in % for the overall result**
Pressure Sensor	1oo2	1,982 E-8	**3**	94,576	76,614y	50,57
F 3238	1oo2	1,548 E-9	**4**	99,917	52,298y	3,95
F 8650E	1oo2	7,235 E-9	**4**	99,769	27,396y	18,47
F 7553	1oo2	2,275 E-9	**4**	99,952	101,997y	5,81
F 3330	1oo2	1,226 E-9	**4**	99,767	69,888y	3,13
Valve	1oo2	7,082 E-9	**4**	94,759	206,056y	18,07
System without Sensor and Actuator		1,228 E-8	**3**	99,832	12,542y	100,00
System with Sensor and Actuator		3,918 E-8	**3**	98,459	10,242y	100,00
TÜV claimed SIL for Systems without Sensor and Actuator			**3**			

Table 9: "Hi-Demand Results" Calculated for the H51q-HRS System Loop

After the PFH calculation, the system is categorized in the SIL 3 class.

SIL based on HFT and SFF (TÜV Approved)					
System / System Parts	**Architecture**	**Type A/B**	**SIL**	**SFF in %**	**MTTF in years**
Pressure Sensor	1oo2	B	**2**	94,576	76,614y
F 3238	1oo2	B	**3**	99,917	52,297y
F 8650E	1oo2	B	**3**	99,769	27,396y
F 7553	1oo2	B	**3**	99,952	101,997y
F 3330	1oo2	B	**3**	99,767	69,888y
Valve	1oo2	B	**2**	94,759	206,056y
System without Sensors and Actuators			**3**	99,832	12,541y
System with Sensor and Actuator			**2**	98,458	10,242y
TÜV claimed SIL for Systems without Sensor and Actuator			**2**		

Table 10: "SIL Based on HFT and SFF (TÜV Approved)" Calculated for the H51q-HRS System Loop

After the module certification, the system is categorized in the SIL 2 class.

Note The functional safety of every safety function's target SIL must be proven in accordance with the applicable norms.

The SIL specified in the manufacturer's documentation is a deciding factor for the SIL specification of a component. The documentation details the examination and certification of this SIL.

13.4 Configuring Systems using the Example of *HIMatrix*

13.4.1 General

The *HIMatrix* System contains a controller (resource), which can be extended using the decentral I/O module. The controller and the remote I/Os are linked via SafeEthernet.

If the I/O signals of the remote I/Os are used in a *HIMatrix* system loop,, the controller only requires the CPU components.

The I/O signals are processed in the controller's CPU component.

Only the controller's CPU component (i.e. not the complete controller) is considered in the SIL calculation.

This topic is explained in greater detail in the example of a *HIMatrix* system presented below. This ia a major difference between H41q/H51q and *HIMATRIX* systems.

Input	**Controller**	**Output**
F1 DI 16 01	**F30**	**F2 DO 16 01**

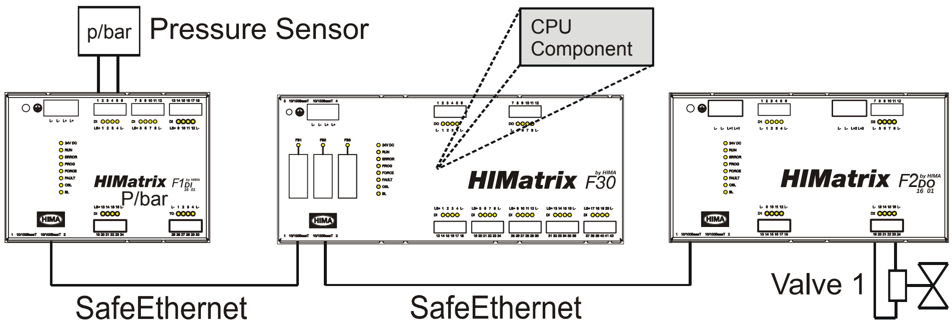


Fig. 41: Typical *HIMatrix* System Loop

- The input signal sent from the pressure sensor is received by the decentral I/O module "F1 DI 16 01" and then sent to the controller "F30".
- The input signal is processed in the controller CPU component, which creates an output signal.
- The controller "F30" sends the output signal to the decentral I/O module "F1 Do 16 01" via SafeEthernet, where it is then output in the valve.

13.4.2 Configuration of *SILence* Loops

In ***SILence***, *HIMatrix* system loops are freely defined systems. All single systems must be added and configured by the user.

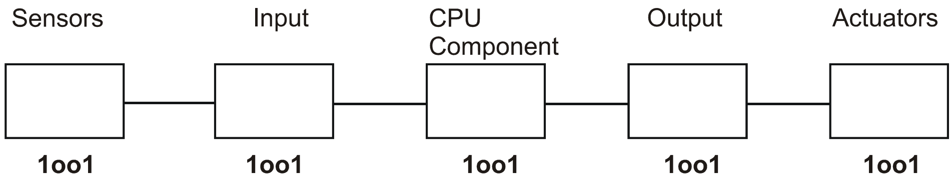


Fig. 42: A *HIMatrix* System Loop in *SILence*

Single system	Architecture	Module	Module Description
Sensor	1oo1	Pressure sensor	Standard Pressure Sensor
Input	1oo1	F1 DI 16 01	16 digital Inputs
CPU	1oo1	F30 – SiCPU	CPU Component
Output	1oo1	F2 DO 16 01	16 Digital Outputs
Actuator	1oo1	Valve	Standard Valve

Table 11: Single Systems and Modules Used in the *HIMatrix* System Loop

13.4.3 Configuring *SILence* Loops

Open the project in which the new system (loop) should be saved, or create a new project:

To create a "New System" in ***Silence***:
- Select *File → New System*. The "Select System" dialog box opens.

To create a free defined System:
- Activate the option *Create new System* window in the "Select System" dialog box.
- Click *Create*. The editor opens and the single system "CPU" is displayed in the "System" tab.

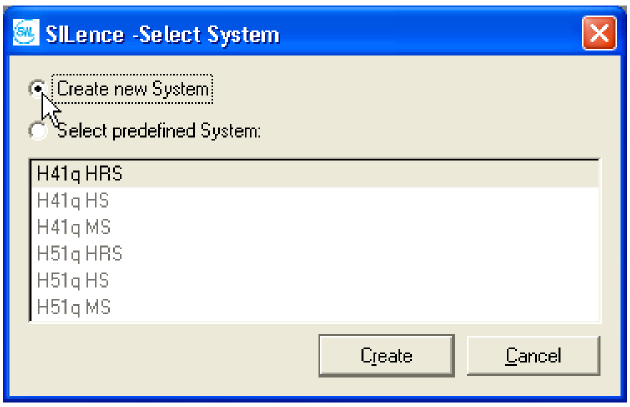


Fig. 43: "Select System" Dialog Box

To configure the single system “CPU“:

- Select an architecture (1oo1) for the single system “CPU“ in the drop-down list.

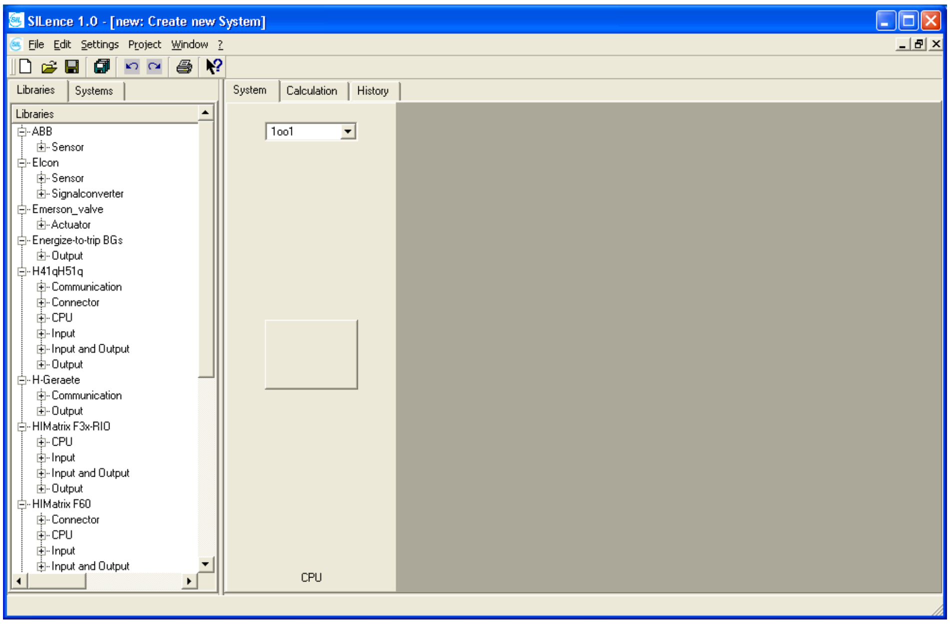


Fig. 44: A Newly Created “Free Defined System” Displayed in the Editor

To add the single system “Sensor“ to the single system “CPU“:

- Right-click on the single system “CPU“.
- Select *Add single system to the left* → *Sensor* using the context menu.
- Select an architecture for the new single system “Sensor“ (1oo1) in the drop-down list.

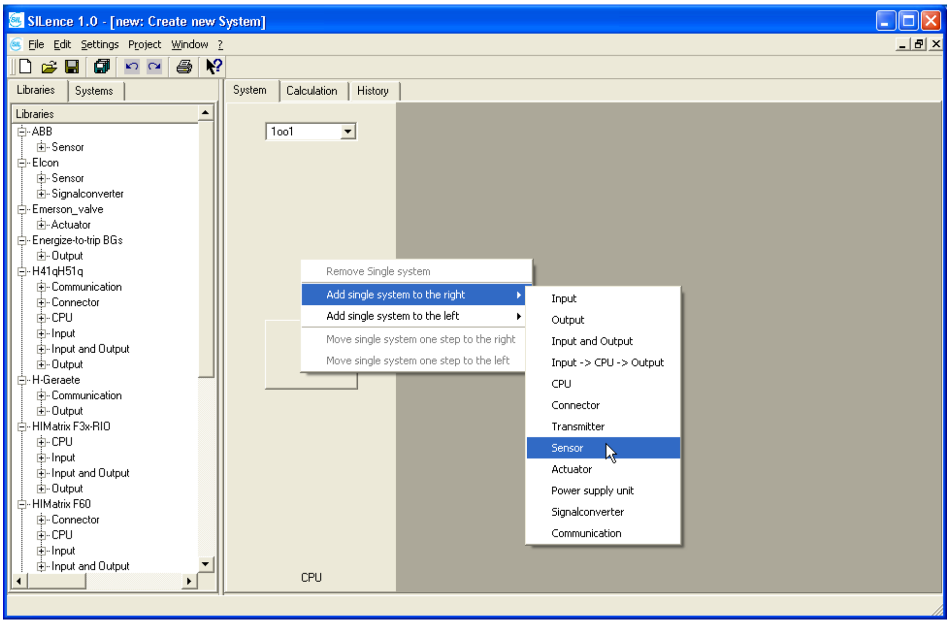


Fig. 45: Single System are Added Using the Context Menu

To add the single system “Input“ to the new system:

- Right-click on the single system “CPU“.
- Select *Add single system to the left → Input* using the context menu.
- Select an architecture (1oo1) for the new single system “Input“ in the drop-down list.

To the single system “CPU“, add the single system “Output“:

- Right-click on the single system “CPU“.
- Select *Add single system to the right → Output* using the context menu.
- Select an architecture (1oo1) for the new single system “Output“ in the drop-down list.

To add the single system “Actuator“ to the single system “Output“:

- Right-click on the single system “Output”.
- Select *Add single system to the right → Actuator* using the context menu.
- Select an architecture (1oo1) for the new single system “Actuator“ in the drop-down list.

To set the “Proof-Test-Interval-Configuration“:

- Select *Settings* → *Proof-Time-Interval-Configuration* to open the “Proof-Test-Interval-Configuration” dialog box.
- Set the proof-time intervals (by default: 3 and 10 years) using the arrows near the field.
- Click *OK* to confirm these actions.

Fig. 46: “Proof-Test-Interval-Configuration” Settings

To add modules to the free defined *HIMatrix* system:

- Right-click on a single system rectangle.
- Select one of the possible modules using the context menu.
- Add the following modules to the system:

Sensor	Input	CPU	Output	Actuator
Pressure sensor	F1 DI 16 01	F30 – SiCPU	F2 DO 16 01	Valve

Table 12: Modules Used for the Free Defined *HIMatrix* System

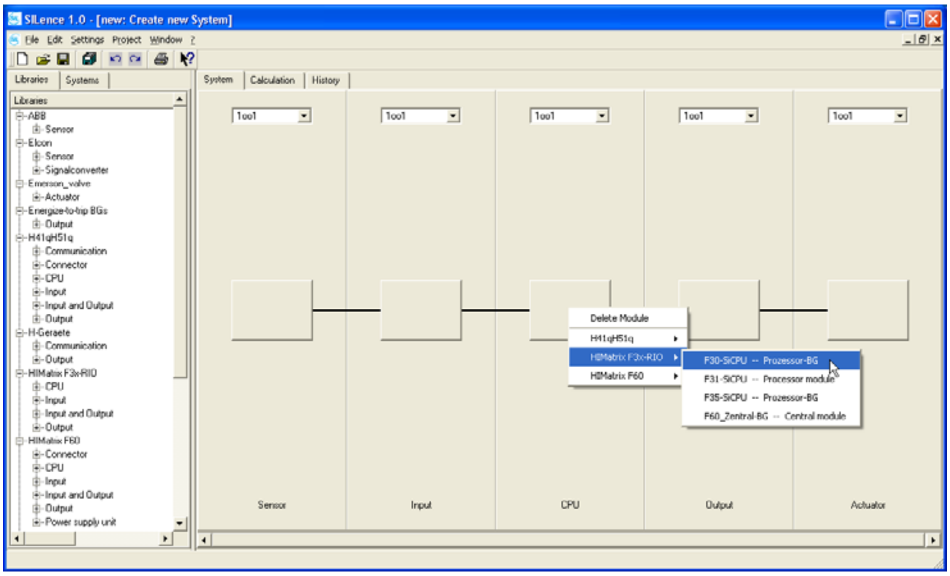


Fig. 47: Selection of Possible Modules in the Context Menu

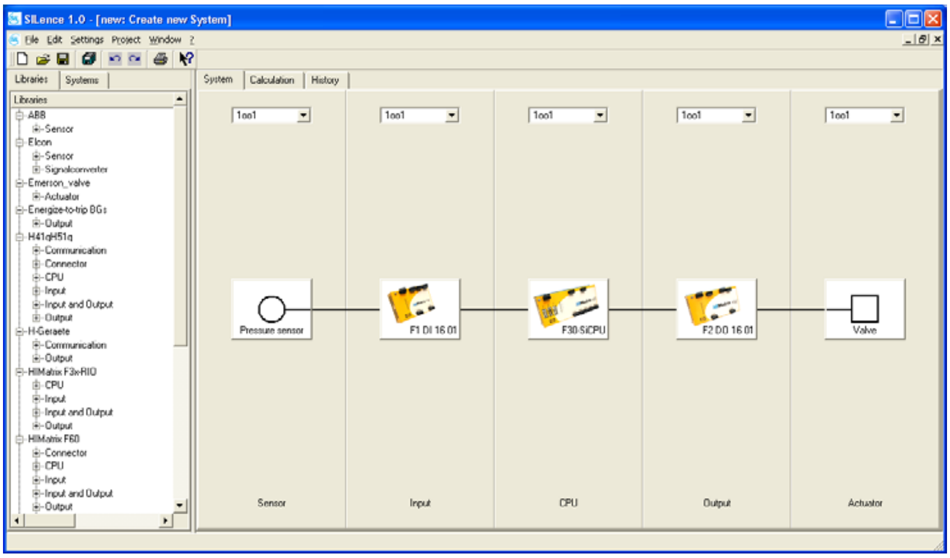


Fig. 48: Configured H51q-HRS System

To save the project and all created systems:

- Select *File* → *Project save as.. .*
- A standard dialog box opens.
- Select the directory in which the project should be saved.
- Enter the project name in the field “File Name”.
- Click *Save* to save the project

13.4.4 Results Calculated for the *HIMatrix* System Loop

After configuring the system, the results for the configured system are displayed in the “Calculation” tab.

Lo-Demand Result [Proof-Test Interval = 10 Years]						
System / System part	**Architecture**	**PFD**	**SIL**	**SFF in %**	**MTTF in years**	**PFD in % for the overall result**
Pressure Sensor	1oo1	1,773 E-3	**2**	94,576	153,229y	70,21
F1 DI 16 01	1oo1	3,684 E-5	**4**	99,795	45,019y	1,46
F30 – SiCPU	1oo1	4,246 E-5	**4**	99,851	50,362y	1,68
F2 DO 16 01	1oo1	3,626 E-5	**4**	99,773	15,220y	1,44
Valve	1oo1	6,367 E-4	**3**	94,759	412,113y	25,21
System without Sensor and Actuator		1,156 E-4	**3**	99,810	9,279y	100,00
System with Sensor and Actuator		2,525 E-3	**2**	98,875	8,567y	100,00
TÜV claimed SIL for Systems without Sensor and Actuator			**2**			

Table 13: "Lo-Demand Results" Calculated for the *HIMatrix* System Loop

After the PFD calculation, the system is categorized in the SIL 3 class.

Hi-Demand Result [Proof-Test Interval = 10 Years]						
System / System parts	**Architecture**	**PFH**	**SIL**	**SFF in %**	**MTTF in years**	**PFD in % for the overall result**
Pressure sensor	1oo1	4,041 E-8	**3**	94,576	153,229y	62,71
F1 DI 16 01	1oo1	2,773 E-9	**4**	99,795	45,019y	4,30
F30 – SiCPU	1oo1	2,842 E-9	**4**	99,851	50,362y	4,41
F2 DO 16 01	1oo1	3,903 E-9	**4**	99,773	15,220y	6,06
Valve	1oo1	1,451 E-8	**3**	94,759	412,113y	22,52
System without Sensor and Actuator		9,517 E-9	**4**	99,810	9,279y	100,00
System with Sensor and Actuator		6,443 E-8	**3**	98,875	8,567y	100,00
TÜV claimed SIL for Systems without Sensor and Actuator			**3**			

Table 14: "Hi-Demand Results" Calculated for the *HIMatrix* System Loop

After the PFH calculation, the system is categorized in the SIL 3 class.

SIL based on HFT and SFF (TÜV Approved)					
System / System parts	**Architecture**	**Type A/B**	**SIL**	**SFF in %**	**MTTF in years**
Pressure sensor	1oo1	B	**2**	94,875	8,567y
F1 DI 16 01	1oo1	B	**3**	99,795	45,019y
F30 – SiCPU	1oo1	B	**3**	99,851	50,362y
F2 DO 16 01	1oo1	B	**3**	99,773	15,220y
Valve	1oo1	B	**2**	94,759	412,113y
System without Sensors and Actuators			**3**	99,810	9,279y
System with Sensor and Actuator			**2**	98,875	8,567y
TÜV claimed SIL for Systems without Sensors and Actuators			**2**		

Tabelle 15: "SIL based on HFT and SFF (TÜV Approved)" Calculated for the *HIMatrix* System Loop

After the module certification, the system is categorized in the SIL 2 class.

Note The calculation of the functional safety is *one* condition for the SIL classification of a plant. Further conditions must be determined together with the responsible certification authority or with an expert.

13.4.5 Overview of HIMA Libraries for the *HIMatrix* Controllers

The following *HIMatrix* controllers are available in the HIMA library in ***SILence***.

Controller	Description
F30	20 Digital Inputs 8 Digital Outputs with Field Bus
F31	20 Digital Inputs 8 Digital Outputs without Field Bus
F35	24 Digital Inputs, 8 Digital Outputs 8 Analogue Outputs, 2 Counters
F60	Configurable with Various Modules

Table 16: *HIMatrix* Controllers Available in the HIMA Library

Important	If the controller's I/O channels (incl. CPU) are to be used in the loop, please use the entries above taken from the HIMA library.

The following decentral I/O modules are available in the HIMA library in ***SILence***:

Decentral I/O Modules	Description
F1 DI 16 01	16 Digital Inputs
F2 DO 4 01	4 Digital Outputs
F2 DO 8 01	8 Digital Relay Outputs
F2 DO 16 01	16 Digital Outputs
F3 AIO 8/4 01	8 Analogue Inputs, 4 Analogue Outputs
F3 DIO 20/8 01	20 Digital Inputs, 8 Digital Outputs

Table 17: Decentral I/O Modules Available in the HIMA Library

Important	If decentral I/O modules (incl. CPU) are to be used in the loop, please use the entries above taken from the HIMA library.

The safety-related, decentral I/O modules can only forward I/O signals.. I/O signals are processed in the user program running on the *HIMatrix* controller.

The following *HIMatrix* CPU components are available in ***SILence*** HIMA library:

Controller	CPU Component Name
F30	F30 – SiCPU
F31	F31 – SiCPU
F35	F35 – SiCPU
F60	F60_Central Module

Table 18: *HIMatrix* CPU Component Available in the HIMA Library

Important	If only controller's CPU components (no O/I channels) are to be used in the loop, please use the entries above taken from the HIMA library.

Note	If only the controller's CPU components are to be used in the system, but the library entries detailed in Table 16 are used for the calculation, a worst SIL category may result as the I/O channels are considered in the calculation even though they are not used.

14 Adding New Modules in *SILence*

For HIMA modules, only ***SILence*** module libraries authorised by HIMA may be used. The user may not change, add or delete the HIMA modules in HIMA libraries.

If a HIMA module is not available in the HIMA libraries check the HIMA homepage www.hima.com or contact HIMA support group.

HIMA provides the manufacturer module libraries for ***SILence*** selected manufacturer modules. The user may not change these libraries.

14.1 Adding New Modules

14.1.1 Adding New Modules Using the Module Editor

New modules are modules not available in the ***SILence*** module libraries (e.g. HIMA and manufacturer module libraries).

The user can add new modules and enter the parameters for the new modules using the module editor. Module's manufacturer must provide the λ and β values.

To configure a new manufacturer module in ***SILence***, follow these steps:

Configuring a Module Using the Example of a Valve

The valve manufacturer provides the following λ, β values.

β Values for the New Module „Valve“	
β Module	**0.02**
β_D Module	**0.01**
β Component1	**0.05**
β_D Component 1	**0.05**

Table 19: All β Values for the New Module

λ Values for the New Module „Valve“		
	Unit 1	**Unit 2**
Description	**FB 1**	**FB 2**
λ_S	**5.50313e-006**	**5.50313e-006**
λ_{DU}	**1.002301e-007**	**1.002301e-007**
λ_{DD}	**1.5313e-006**	**1.5313e-006**

Table 20: All λ Values for the New Module

If the new module's SIL is unknown, the SIL can be determined using the new module's λ values. To determine the SIL, the values SFF, HFT and type A/B must be known.

Note	***SILence*** examines the module's SIL as specified by the user and classifies it in a lower class, if the comparison with the SFF and HFT provides a worst SIL value. ***SILence*** does not improve the SIL, even if the SFF and HFT values would allow it.

All the calculations in the following example are based on the λ values presented in Table 19.

Determining SFF
In the following equation, all new module's λ values must be used (See chapter 6, equation 15).

$$SFF = \frac{\Sigma\lambda_S + \Sigma\lambda_{DD}}{\Sigma\lambda_S + \Sigma(\lambda_{DD} + \lambda_{DU})}$$

The following SFF value results from this equation:
SFF = 0,985952 (98,5952 %)

Determining the Hardware Failure Tolerance N
Each individual module is always a 1oo1 system.
Thus results an HFT value of N = 1 – 1 = 0.

Determining the Type A or Type B Classification
Because only insufficient experience has been acquired with the module, and no manufacturer specifications are available, the module is classified as Type B (in accordance with the definition provided in chapter 3).

Determining the SIL
Using the estimated values and Table 20 presented below, it is possible to determine the SIL for the new module.

	Subsystem Type A			Subsystem Type B		
Safe Failure Fraction (SFF)	Hardware Failure Tolerance N			Hardware Failure Tolerance N		
	0 Failures	1 Failure	2 Failures	0 Failures	1 Failure	2 Failures
< 60 %	SIL 1	SIL 2	SIL 3	Not allowed	SIL 1	SIL 2
60 % to < 90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 % to < 99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Table 21: Chapter 3 „Hardware Requirements“, Table 3

Using Table 20, a SIL 2 results for the new module.

Determining the MTTF/h

If the module's manufacturer has not provided the MTTF, it can be calculated from the sum of all λ values.

$$MTTF = \frac{1}{\Sigma(\lambda_S + \lambda_{DD} + \lambda_{DU})} \text{ h}$$

The following MTTF value results from this equation:
70080.424 hours or 8 years.

Note	If a module's λ value is not considered during the MTTF calculation, ***SILence*** calculates a MTTF that appears to be better than the actual MTTF value of the module.

To configure a new manufacturer module in ***SILence***, use the following:

- Select *Settings → Module Editor* to open the Module Editor.
- Click *Add* to create a new module.

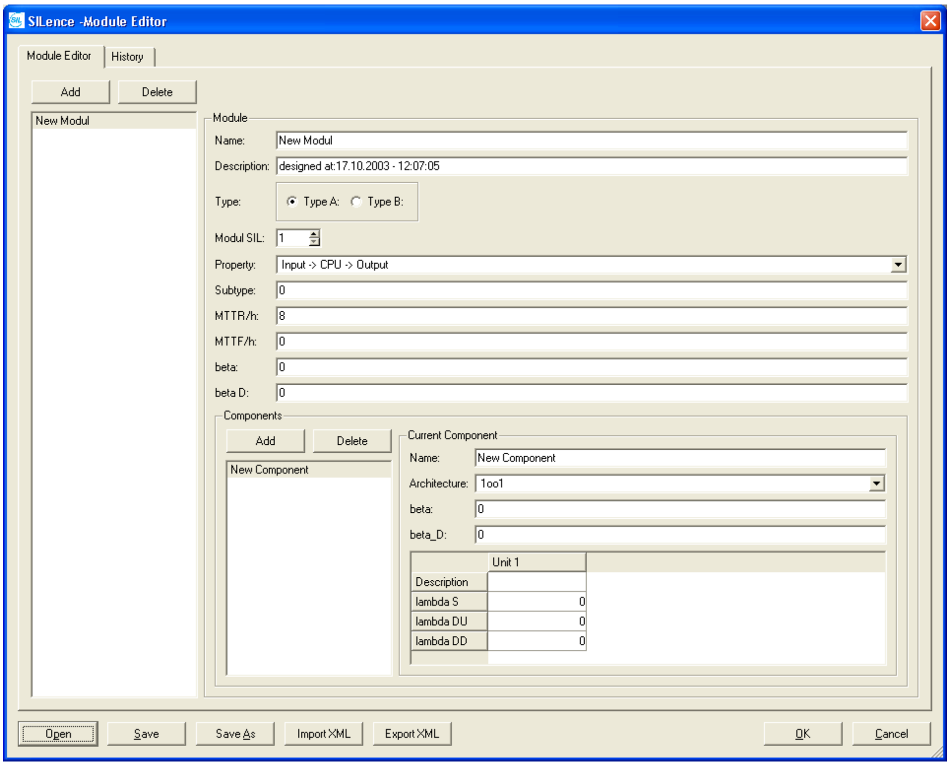


Fig. 49: Adding a New Module Using the Editor Module

To configure a new module:

- Configure the new module as described in this chapter. In the Module Editor, enter the parameters listed in the following tables.

Module Parameter	Input	Description
Name	**Valve**	Name of the new module (max. 15 characters)
Description	**Example for SIL 3**	Description of the new module
Type	**B**	Refer to previous section “Determining the classification as Type A or Type B“
Module SIL	**2**	Refer to previous section “Determining the SIL“ (1 to 4)
Property	**Actuator**	A valve is classified as “Actuator”
Subtype (0 bis 9999)	**1**	Only modules of the same subtype may be interconnected redundantly
MTTR/h	**8**	***SILence*** default value: 8h
MTTF/h	**70080**	Refer to previous section “Determining the MTTF/h“
β	**0.02**	Manufacturer’s default: see Table 19
β_D	**0.01**	Manufacturer’s default: see Table 19

Table 22: Module Parameter of the Valve

Component Parameter	Input	Description
Name	**Component 1**	Name of the current component
Architecture	**1oo2**	The determination of the current component’s architecture depends on the number of units
β	**0.05**	Manufacturer’s default: see Table 19
β_D	**0.05**	Manufacturer’s default: see Table 19

Table 23: Component Parameter of the Valve

Unit Parameter 1+2	Input	Input	Description
Description	**FB 1**	**FB 2**	Name of the unit
λ_S	**5.50313e-006**	**5.50313e-006**	Manufacturer’s default: see Table 20
λ_{DU}	**1.002301e-007**	**1.002301e-007**	
λ_{DD}	**1.5313e-006**	**1.5313e-006**	

Table 24: Unit Parameter of the Valve

Note The separator for decimal numbers in ***SILence*** is the point.

Note The user is responsible for ensuring the correctness of the parameters he entered. See also chapter 11.3.3 „Module Editor“.

After entering the parameters, the Module Editor should be configured as in Fig. 50.

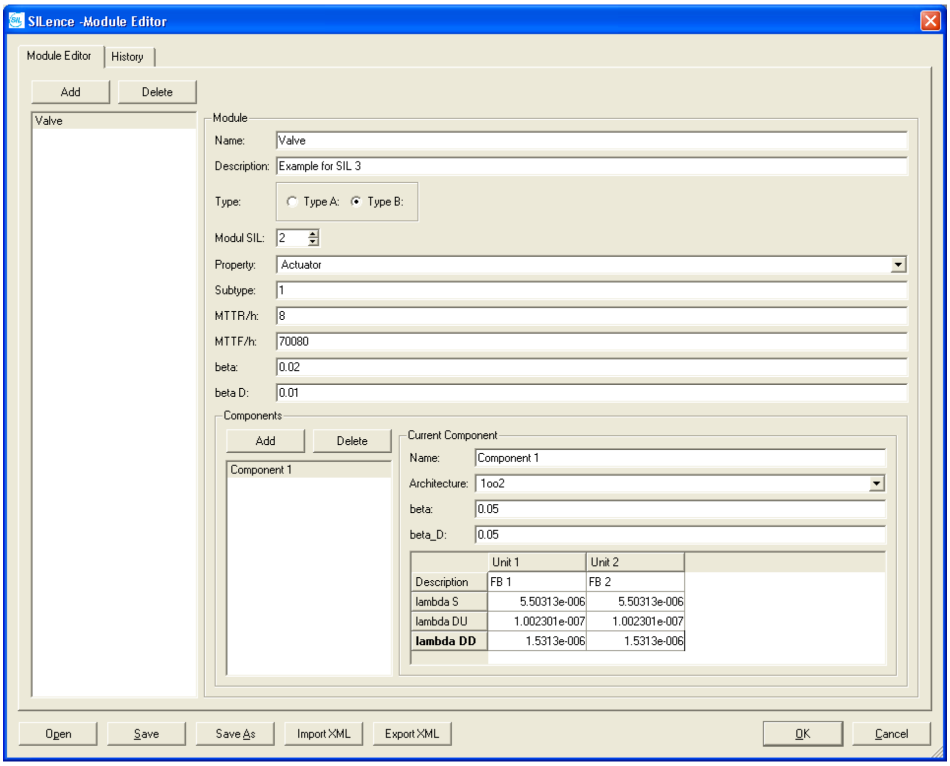


Fig. 50: Entered Parameters Displayed in the Module Editor

To save the new module in a new module library:

- Click *Save As* to open the standard dialog box.
- Select the path and enter the file name for the module library.
- Click the *Save* button.
- Click *OK* to close the Module Editor.

Note	Import the new module library using the “Libraries” dialog box. To move the new module from the module list into the provided module fields use the Drag & Drop function. See chapter 10 “Main Window” for more details.

To display the new module in the “Calculation” tab, the new module was "dragged and dropped" into the 1oo1 single system “Actuator”.

T1 [y, m]	System / Module	HIMA-Lib.	Type A/B	SIL	PFD	PFH	SFF	MTTF	PFx in % of the overall result
3 years	Lo-Demand result			3	2.435208e-004		98.595166%	8.000000y	100.00%
10 years	Actuator			3	2.435208e-004		98.595166%	8.000000y	100.00%
	Valve		B	3	2.435208e-004		98.595166%	8.000000y	100.00%
	Hi-Demand result			3		9.454334e-008	98.595166%	8.000000y	100.00%
	Actuator			3		9.454334e-008	98.595166%	8.000000y	100.00%
	Valve		B	3		9.454334e-008	98.595166%	8.000000y	100.00%
	SIL based on HFT and SFF (TÜV Approved)			2			98.595166%	8.000000y	
	Actuator			2			98.595166%	8.000000y	
	Valve		B	2			98.595166%	8.000000y	

Fig. 51: The New Module Displayed in the „Calculation“ Tab

After the PFH and PFD calculation, the new module is categorized in the SIL 3 class. After the SFF calculation and the classification as type B for HFT, it is re-categorized in the SIL 2 class.

Note For redundant interconnections of type A modules, the SIL X can be improved to SIL X+1. The prerequisite for such improvements is that the module software has already been certified for the higher SIL. Redundant interconnections only improve the hardware. A software failure would occur in both systems at the same time as the software, and consequently the probability of failure, is the same in both devices.

14.1.2 Adding New Modules Using the *Import XML* Option

SILence provides an XML interface to import and export module libraries in XML format.

The following example explains how to create a new module library in the module editor, and to export it using the *Export XML* option.

The new module library will be edited in XML format and can be imported into the Module Editor (MS-Notepad) using the *Import XML* option.

Follow these steps to create a new module library in the ***SILence***'s XML:

- Select *Settings* → *Module Editor* to open the Module Editor.

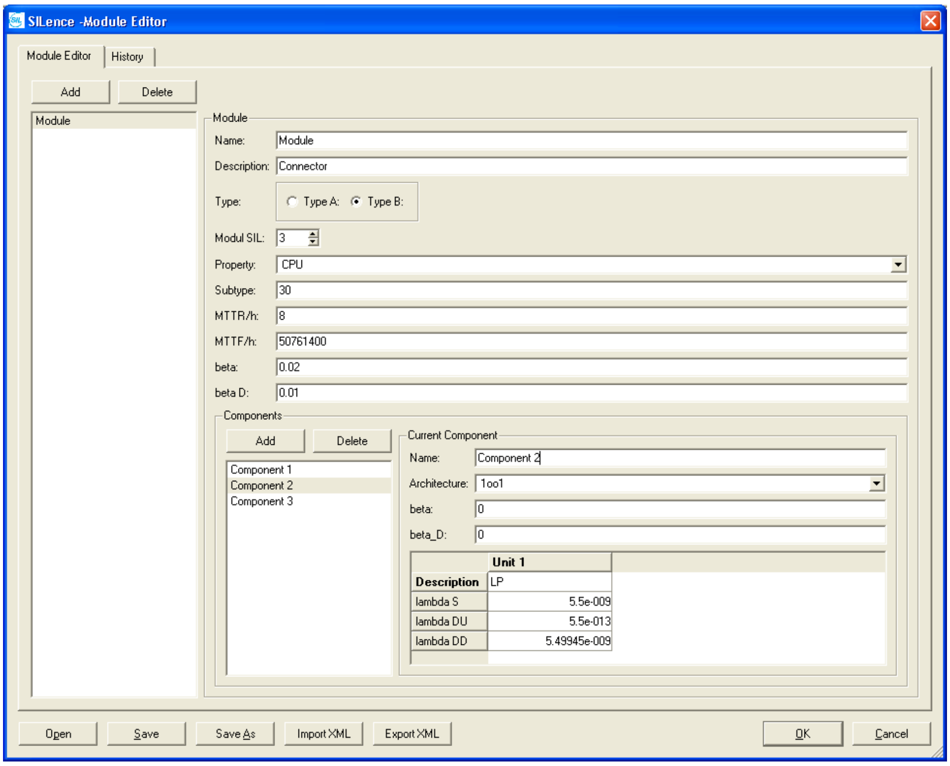


Fig. 52: A New Module in the Module Editor

To add a new module:

- Click the *Add* button to create a new module.

To export the new module as a XML module library:

- Click the *Export XML* button to open the standard dialog box.
- Enter the file name for the XML module library.
- Click the *Save* button.

Once the XML module library has been exported, it can be modified and extended using a suitable editor (XML editor or also MS notepad).

To re-import the XML module library into ***SILence***, make sure that it adheres to the ***SILence*** module library structure.

The following figure shows the new XML module library.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<?xml-stylesheet href="SILence.xsl" type="text/xsl"?>

<silence>
	<history>
		<changes>
		<date>02.10.2003 - 10:25:13</date>
		<version> </version>
		<comment> </comment
		><author> </author>

		</changes>
	</history>

	<devices>
		<device>
			<name> Module</name>
			<property>Connector</property>
			<MTTF>5.07614e+007</MTTF>
			<MTTR>8</MTTR>
			<beta_D>0.01</beta_D>
			<beta>0.02</beta>
			<type>CPU</type>
			<subtype>30</subtype>
			<type_ab>B</type_ab>
			<cert_sil>3</cert_sil>
			<architecture>
				<property>Component 1</property>
				<arch_type>1oo1</arch_type>
				<beta_D>0</beta_D>
				<beta>0</beta>
				<component>
					<property>PROFIBUS-ADAPTER</property>
					<lambda_S>1.3e-009</lambda_S>
					<lambda_DD>1.29987e-009</lambda_DD>
					<lambda_DU>1.3e-013</lambda_DU>
				</component>
			</architecture>
			<architecture>
				<property> Component 2</property>
				<arch_type>1oo1</arch_type>
				<beta_D>0</beta_D>
				<beta>0</beta>
				<component>
					<property>LP</property>
					<lambda_S>5.5e-009</lambda_S>
					<lambda_DD>5.49945e-009</lambda_DD>
					<lambda_DU>5.5e-013</lambda_DU>
				</component>
			</architecture>
			<architecture>
				<property> Component 3</property>
				<arch_type>1oo1</arch_type>
				<beta_D>0</beta_D>
				<beta>0</beta>
				<component>
					<property>Plug</property>
					<lambda_S>3.05e-009</lambda_S>
					<lambda_DD>3.0497e-009</lambda_DD>
					<lambda_DU>3.05e-013</lambda_DU>
					</component>
			</architecture>
		</device>
	</devices>
```

Fig. 53: The New Library in XML Format

To import the XML module library into the Module Editor:

- Click the *Import XML* button to open the standard dialog box.
- Select the path and enter the file name for the module library.
- Click the *Open* button.

To save the new XML module library with the “*.sdd” file extension:

- Click the *Save As* button to open the standard dialog box.
- Select the path and enter the file name for the module library.
- Click the *Save* the button.
- Click *OK* to close the Module Editor.

Note	Import the new module library with the dialog “Libraries”. To move the new module from the module list into the provided module fields, use the Drag & Drop function. See chapter 10 “Main Window” for more details.

15 Example Calculations of Selected Systems

In the example calculations, the following single systems are used in various configurations:

Module	Pressure sensor / Pressure switch	Temp.-sensor / Temp.-switch	DI: F 3238	AI: F 6214	Connector: F 7553	CPU: F 8650E	DO: F 3334	AO: F 6705	Actuator: Valve
lambda_b in [1/h]			1,09E-06	1,11E-06	5,60E-07	2,08E-06	6,21E-07	9,45E-07	
MTTF in [years]			104,60	102,80	203,99	54,79	183,91	120,79	
Proof-test interval T_1 in [years]	10	10	10	10	10	10	10	10	10
MTTR in [h]	8	8	8	8	8	8	8	8	8
β_D	0,05	0,05	0,01	0,01	0,01	0,01	0,01	0,01	0,05
β	0,05	0,05	0,02	0,02	0,02	0,02	0,02	0,02	0,05
PFD_{1oo1} in [1]			2,37077E-05	5,11873E-05	9,77747E-06	2,93355E-05	1,39346E-05	1,85694E-05	
PFH_{1oo1} in [1/h]			5,13220E-10	1,10675E-09	5,75579E-10	4,07407E-09	6,86279E-10	6,16433E-10	
PFD_{2oo3} in [1] *)	1,00E-04	1,56E-04							3,33E-05
PFH_{2oo3} in [1/h] *)	2,22E-08	3,47E-08							7,40E-09
TÜV claimed SIL			3	3	3	3	3	3	

*) assumed value

Table 25: Single Systems Used in the Example Calculations

Two points apply to all systems described below:

- Sensors in 2oo3 architecture
- Actuators in 1oo2 architecture

15.1 System 1 (Digital Loop 1)

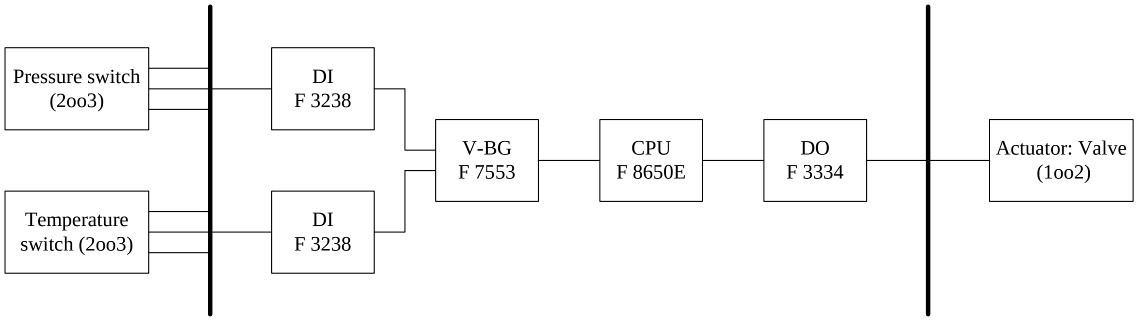


Fig. 54: System 1 (Digital Loop 1)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure switch	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature switch	2oo3	1,56000E-04	3,47000E-08	3	3
DI: F 3238	1oo2	4,62662E-07	1,54807E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo1	2,93355E-05	4,07407E-09	3	3
DO: F 3334	1oo1	1,39346E-05	6,86279E-10	4	4
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System without sensor and actuator		5,35103E-05	6,88400E-09	4	4
System with sensor and actuator		3,42810E-04	7,11840E-08	3	3
TÜV claimed SIL for systems without sensor and actuator				3	3

Table 26: Calculation Results for System 1 (Digital Loop 1)

15.2 System 2 (Digital Loop 2)

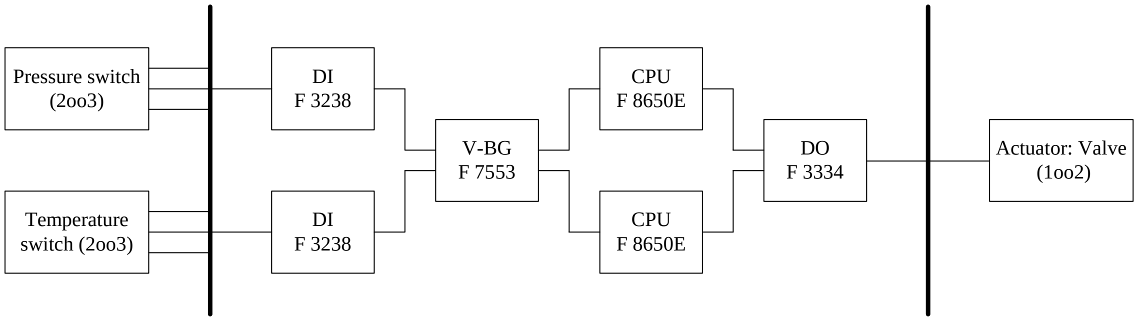


Fig. 55: System 2 (Digital Loop 2)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure switch	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature switch	2oo3	1,56000E-04	3,47000E-08	3	3
DI: F 3238	1oo2	4,62662E-07	1,54807E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo2	3,07711E-06	7,23550E-09	4	3
DO: F 3334	1oo1	1,39346E-05	6,86279E-10	4	4
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System without sensor and actuator		2,72518E-05	1,00454E-08	4	3
System with sensor and actuator		3,16552E-04	7,43454E-08	3	3
TÜV claimed SIL for systems without sensor and actuator				3	3

Table 27: Calculation Results for System 2 (Digital Loop 2)

15.3 System 3 (Digital Loop 3)

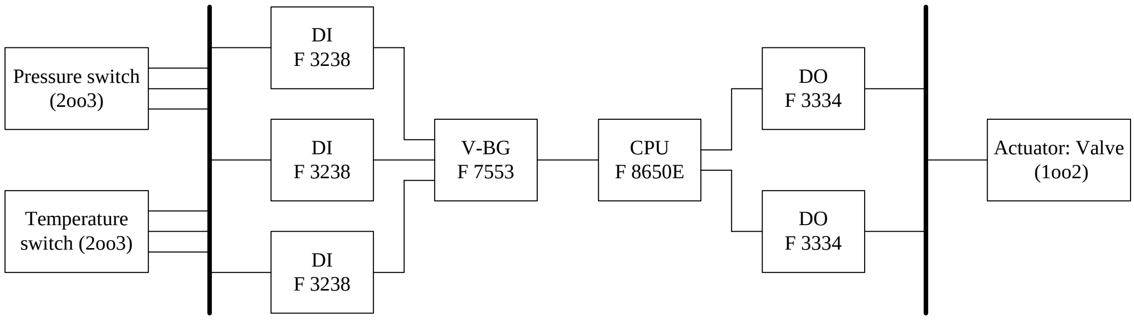


Fig. 56: System 3 (Digital Loop 3)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure switch	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature switch	2oo3	1,56000E-04	3,47000E-08	3	3
DI: F 3238	2oo3	4,64169E-07	1,56234E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo1	2,93355E-05	4,07407E-09	3	3
DO: F 3334	1oo2	6,08163E-07	1,28962E-09	4	4
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System without sensor and actuator		4,01853E-05	7,50161E-09	4	3
System with sensor and actuator		3,29485E-04	7,18016E-08	3	3
TÜV claimed SIL for systems without sensor and actuator				3	3

Table 28: Calculation Results for System 3 (Digital Loop 3)

15.4 System 4 (Digital Loop 4)

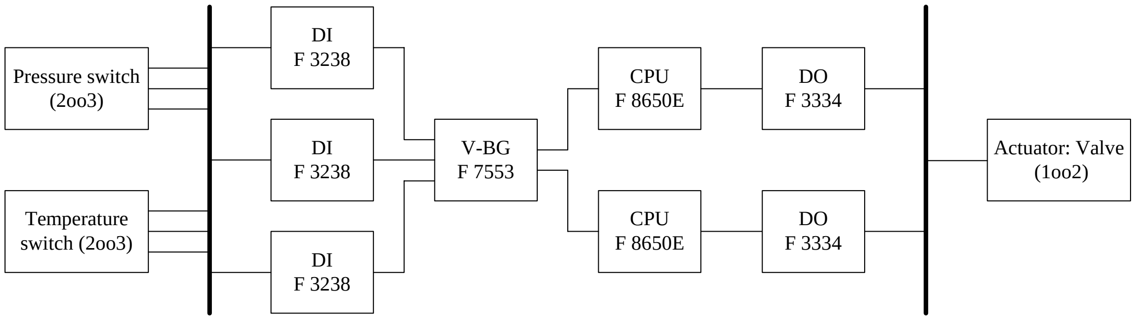


Fig. 57: System 4 (Digital Loop 4)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure switch	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature switch	2oo3	1,56000E-04	3,47000E-08	3	3
DI: F 3238	2oo3	4,64169E-07	1,56234E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo2	3,07711E-06	7,23550E-09	3	3
DO: F 3334	1oo2	6,08163E-07	1,28962E-09	4	4
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System without sensor and actuator		1,39269E-05	1,06630E-08	4	4
System with sensor and actuator		3,03227E-04	7,49630E-08	3	3
TÜV claimed SIL for systems without sensor and actuator				3	3

Table 29: Calculation Results for System 4 (Digital Loop 4)

15.5 System 5 (Analogue-Digital Loop 1)

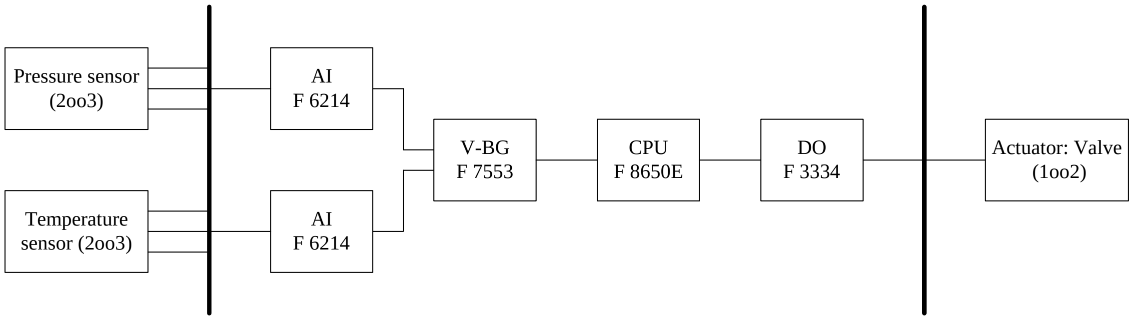


Fig. 58: System 5 (Analogue-Digital Loop 1)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature sensor	2oo3	1,56000E-04	3,47000E-08	3	3
AI: F 6214	1oo2	1,00023E-06	3,43468E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo1	2,93355E-05	4,07407E-09	3	3
DO: F 3334	1oo1	1,39346E-05	6,86279E-10	4	4
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System without sensor and actuator		5,40478E-05	8,77060E-09	4	4
System with sensor and actuator		3,43348E-04	7,30706E-08	3	3
TÜV claimed SIL for systems without sensor and actuator				3	3

Table 30: Calculation Results for System 5 (Analogue-Digital Loop 1)

15.6 System 6 (Analogue-Digital Loop 2)

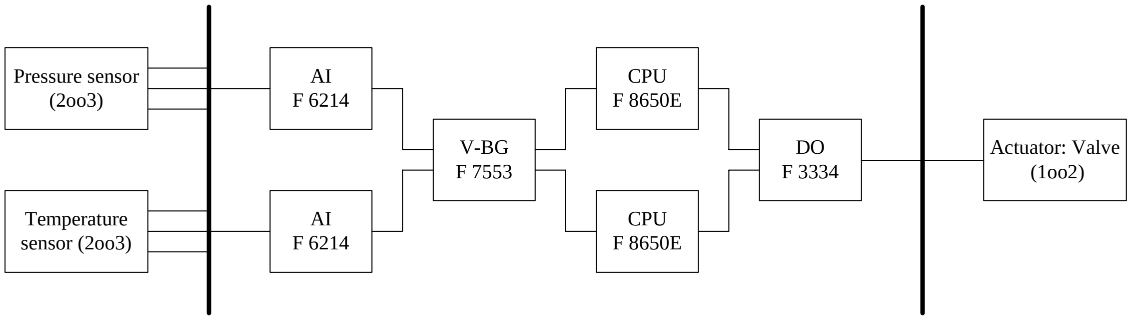


Fig. 59: System 6 (Analogue-Digital Loop 2)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature sensor	2oo3	1,56000E-04	3,47000E-08	3	3
AI: F 6214	1oo2	1,00023E-06	3,43468E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo2	3,07711E-06	7,23550E-09	3	3
DO: F 3334	1oo1	1,39346E-05	6,86279E-10	4	4
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System without sensor and actuator		2,77894E-05	1,19320E-08	4	4
System with sensor and actuator		3,17089E-04	7,62320E-08	3	3
TÜV claimed SIL for systems without sensor and actuator				3	3

Table 31: Calculation Results for System 6 (Analogue-Digital Loop 2)

15.7 System 7 (Analogue-Digital Loop 3)

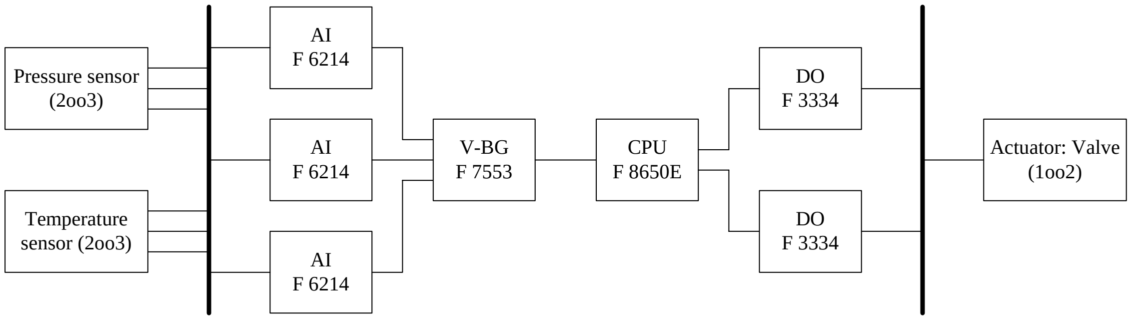


Fig. 60: System 7 (Analogue-Digital Loop 3)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature sensor	2oo3	1,56000E-04	3,47000E-08	3	3
AI: F 6214	2oo3	1,00726E-06	3,50269E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo1	2,93355E-05	4,07407E-09	3	3
DO: F 3334	1oo2	6,08163E-07	1,28962E-09	4	4
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System without sensor and actuator		4,07284E-05	9,44196E-09	4	4
System with sensor and actuator		3,30028E-04	7,37420E-08	3	3
TÜV claimed SIL for systems without sensor and actuator				3	3

Table 32: Calculation Results for System 7 (Analogue-Digital Loop 3)

15.8 System 8 (Analogue-Digital Loop 4)

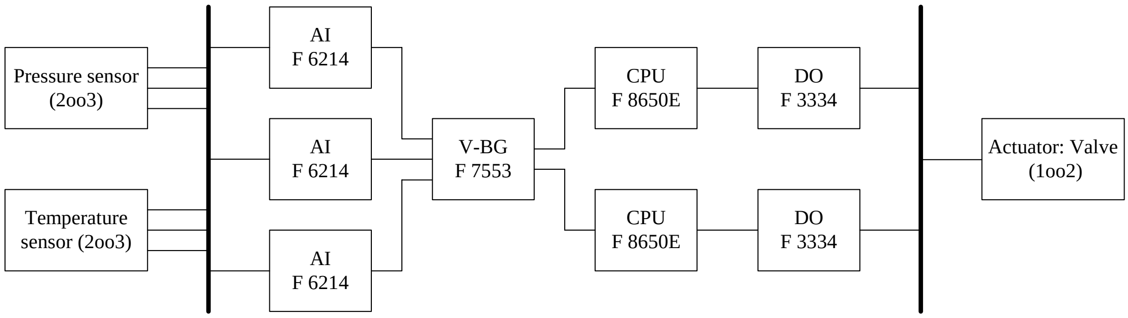


Fig. 61: System 8 (Analogue-Digital Loop 4)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature sensor	2oo3	1,56000E-04	3,47000E-08	3	3
AI: F 6214	2oo3	1,00726E-06	3,50269E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo2	3,07711E-06	7,23550E-09	3	3
DO: F 3334	1oo2	6,08163E-07	1,28962E-09	4	4
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System without sensor and actuator		1,44700E-05	1,26034E-08	4	3
System with sensor and actuator		3,03770E-04	7,69034E-08	3	3
TÜV claimed SIL for systems without sensor and actuator				3	3

Table 33: Calculation Results for System 8 (Analogue-Digital Loop 4)

15.9 System 9 (Analogue Loop 1)

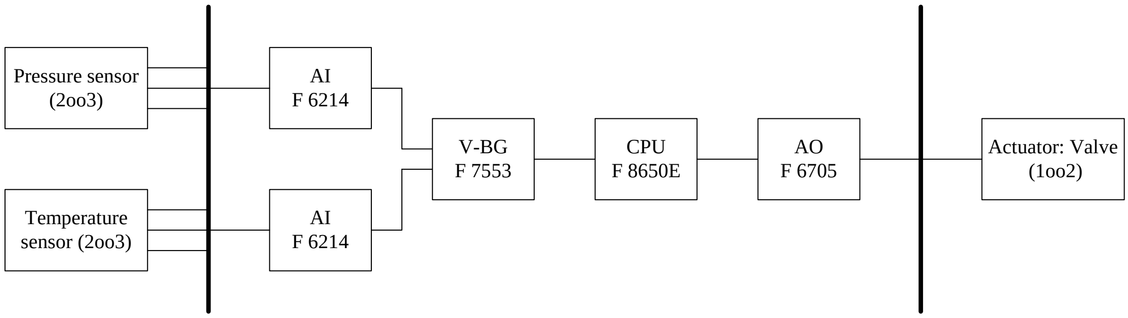


Fig. 62: System 9 (Analogue Loop 1)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature sensor	2oo3	1,56000E-04	3,47000E-08	3	3
AI: F 6214	1oo2	1,00023E-06	3,43468E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo1	2,93355E-05	4,07407E-09	3	3
AO: F 6705	1oo1	1,85694E-05	6,16433E-10	3	4
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System without sensor and actuator		5,86826E-05	8,70076E-09	4	4
System with sensor and actuator		3,47983E-04	7,30008E-08	3	3
TÜV claimed SIL for systems without sensor and actuator				3	3

Table 34: Calculation Results for System 9 (Analogue Loop 1)

15.10 System 10 (Analogue Loop 2)

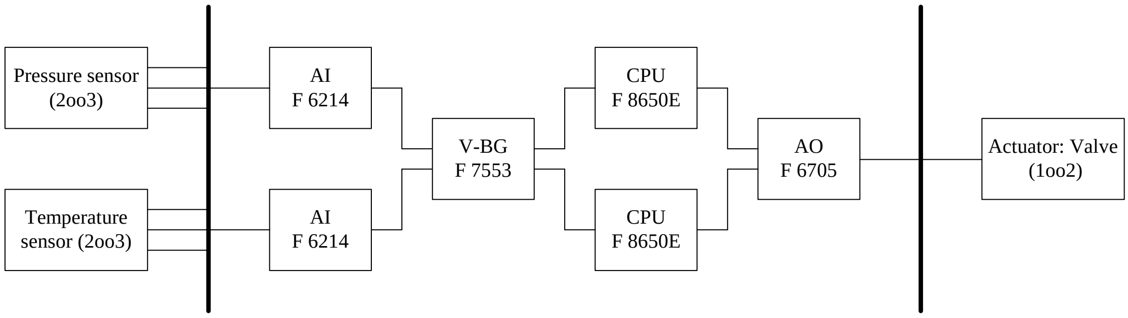


Fig. 63: System 10 (Analogue Loop 2)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature sensor	2oo3	1,56000E-04	3,47000E-08	3	3
AI: F 6214	1oo2	1,00023E-06	3,43468E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo2	3,07711E-06	7,23550E-09	4	3
AO: F 6705	1oo1	1,85694E-05	6,16433E-10	3	4
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System without sensor and actuator		3,24242E-05	1,18622E-08	4	3
System with sensor and actuator		3,21724E-04	7,61622E-08	3	3
TÜV claimed SIL for systems without sensor and actuator				3	3

Table 35: Calculation Results for System 10 (Analogue Loop 2)

15.11 System 11 (Analogue Loop 3)

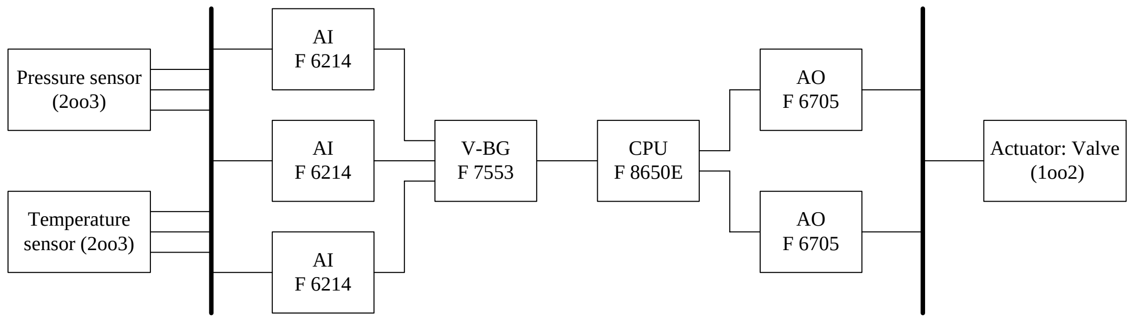


Fig. 64: System 11 (Analogue Loop 3)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature sensor	2oo3	1,56000E-04	3,47000E-08	3	3
AI: F 6214	2oo3	1,00726E-06	3,50269E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo1	2,93355E-05	4,07407E-09	3	3
AO: F 6705	1oo2	3,77332E-07	2,25748E-09	4	3
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System with sensor and actuator		4,04976E-05	1,04098E-08	4	3
System with sensor and actuator		3,29798E-04	7,47098E-08	3	3
TÜV claimed SIL for systems with sensor and actuator				3	3

Table 36: Calculation Results for System 11 (Analogue Loop 3)

15.12 System 12 (Analogue Loop 4)

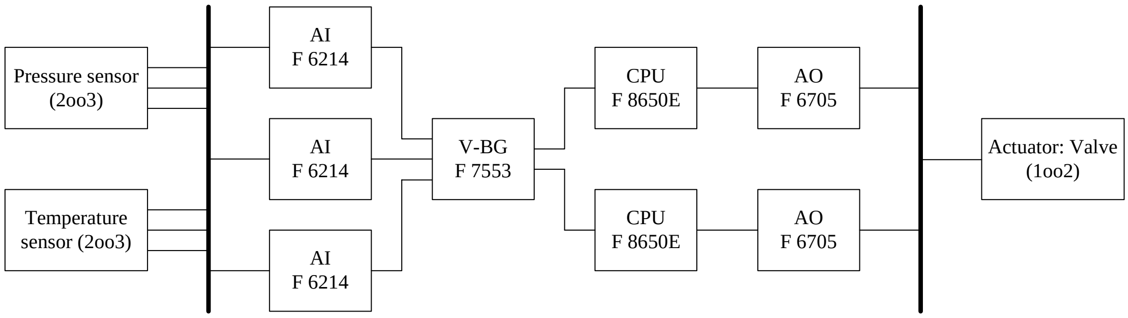


Fig. 65: System 12 (Analogue Loop 4)

	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1,00000E-04	2,22000E-08	3	3
Temperature sensor	2oo3	1,56000E-04	3,47000E-08	3	3
AI: F 6214	2oo3	1,00726E-06	3,50269E-09	4	3
Connector: F 7553	1oo1	9,77748E-06	5,75579E-10	4	4
CPU: F 8650E	1oo2	3,07711E-06	7,23550E-09	4	3
AO: F 6705	1oo2	3,77332E-07	2,25748E-09	4	3
Actuator: Valve	1oo2	3,33000E-05	7,40000E-09	4	3
System without sensor and actuator		1,42392E-05	1,35713E-08	4	3
System with sensor and actuator		3,03539E-04	7,78713E-08	3	3
TÜV claimed SIL for systems without sensor and actuator				3	3

Table 37: Calculation results of System 12 (Analogue Loop 4)

Appendix A

Printout of documentation

Appendix A contains the documentations for the systems H51q-HRS and *HIMatrix*, configured in chapter 13.

After configuration, the documentation was printed out using the menu option *print project.*

Table of contents	
Project summary	Lists all of the project's systems.
System configuration	Contains a copy of the project's systems and the list of modules used using their identification numbers (ID's).
Calculation- results for T1	Lists all the results calculated for the project, i.e. „Lo-Demand-result", „Hi-Demand-,result" and „SIL based on HFT and SFF (TÜV Approved)". The calculation results are printed out as they are displayed in the editor's "Computations" tab (see chapter 12.2).

Note	An identification number (ID: E96AC21-724038B9) corresponds to each module and predefined system. With this ID, HIMA can determine which ***SILence*** version and which module libraries have been used.

Note	In ***SILence***, the documentation printout is an important element. For this reason, it is a part of the TÜV approval process. If you use more than three fractional digits in the printout of the calculation results, set the printer to "Landscape", to prevent cropping.

Examples attached:

- H51q-HRS (8 pages)
- *HIMatrix* System (6 pages)

Contents

1 Project overview

1.1 Projectfiles

D:/SILence/H51q-HRS.ssy (ID:)

1.2 Project history

1.2.1 Change dated 27.10.2003 - 17:51:01

Version:
Author:
Comment:

2 System configuration:H51q-HRS.s

File: SILence -Editor [D:/SILence/H51q-HRS.ssy]
File-CRC: b53ac187

2.1 File History

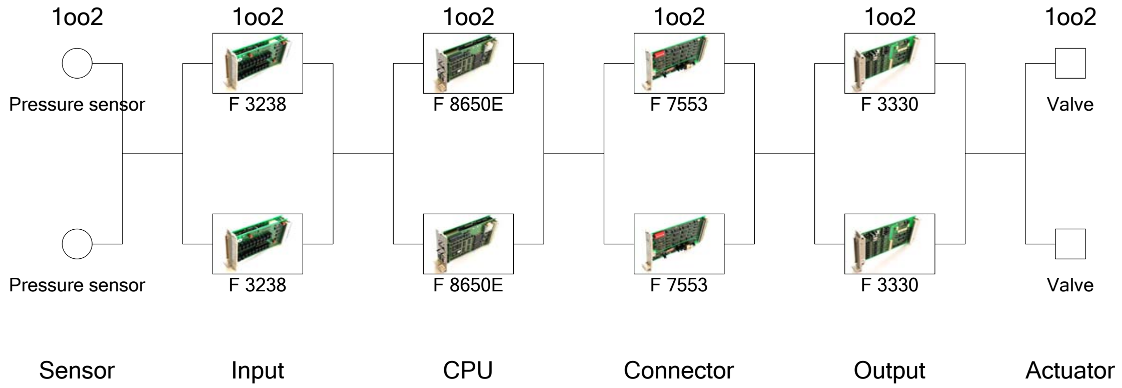
2.1.1 Change dated 27.10.2003 - 18:06:29

Version:
Author:
Comment:

2.1.2 Change dated 27.10.2003 - 18:06:30

Version:
Author:
Comment:

2.2 System configuration:



2.2.1 Libraries

Sensor: Architecture 1oo2

Pressure sensor (ID: 1A209F1E-AEDFA77F)	Pressure sensor / Pressure switch
Pressure sensor (ID: 1A209F1E-AEDFA77F)	Pressure sensor / Pressure switch

Input: Architecture 1oo2

F 3238 (ID: 68523389-15ED913E)	8-channel input module
F 3238 (ID: 68523389-15ED913E)	8-channel input module

CPU: Architecture 1oo2

F 8650E (ID: 68523389-6938ABB9)	Central module
F 8650E (ID: 68523389-6938ABB9)	Central module

Connector: Architecture 1oo2

F 7553 (ID: 68523389-F1C1933B)	Coupling module
F 7553 (ID: 68523389-F1C1933B)	Coupling module

Output: Architecture 1oo2

F 3330 (ID: 68523389-4AFA182A)	8-channel output module
F 3330 (ID: 68523389-4AFA182A)	8-channel output module

Actuator: Architecture 1oo2

Valve (ID: 1A209F1E-4EDB05A5)	Valve
Valve (ID: 1A209F1E-4EDB05A5)	Valve

2.3 Result for T1 =10 years

2.3.1 Lo-Demand-Result

System / Module	HIMA-Lib.	SIL	PFD	SFF	MTTF	Percent of PFx
Total result		3	1.290903e-004	98.458762%	10.241866y	**100.00%**
Sensor		4	9.242929e-005	94.575768%	76.617837y	**71.60%**
Pressure sensor		4	9.242929e-005	94.575768%	153.235675y	71.60%
Pressure sensor		4	9.242929e-005	94.575768%	153.235675y	71.60%
Input	HIMA	4	4.626617e-007	99.916874%	52.297623y	**0.36%**
F 3238	HIMA	4	4.626617e-007	99.916874%	104.595246y	0.36%
F 3238	HIMA	4	4.626617e-007	99.916874%	104.595246y	0.36%
CPU	HIMA	4	3.077107e-006	99.769363%	27.396384y	**2.38%**
F 8650E	HIMA	4	3.077107e-006	99.769363%	54.792767y	2.38%
F 8650E	HIMA	4	3.077107e-006	99.769363%	54.792767y	2.38%
Connector	HIMA	4	2.169758e-007	99.952465%	101.997187y	**0.17%**
F 7553	HIMA	4	2.169758e-007	99.952465%	203.994373y	0.17%
F 7553	HIMA	4	2.169758e-007	99.952465%	203.994373y	0.17%
Output	HIMA	4	5.807397e-007	99.767096%	69.888118y	**0.45%**
F 3330	HIMA	4	5.807397e-007	99.767096%	139.776235y	0.45%
F 3330	HIMA	4	5.807397e-007	99.767096%	139.776235y	0.45%
Actuator		4	3.232355e-005	94.759456%	206.126374y	**25.04%**
Valve		4	3.232355e-005	94.759456%	412.252748y	25.04%
Valve		4	3.232355e-005	94.759456%	412.252748y	25.04%

2.3.2 Hi-Demand-Result

System / Module	HIMA-Lib.	SIL	PFH	SFF	MTTF	Percent of PFx
Total result		3	3.918192e-008	98.458762%	10.241866y	**100.00%**
Sensor		3	1.981609e-008	94.575768%	76.617837y	**50.57%**
Pressure sensor		3	1.981609e-008	94.575768%	153.235675y	50.57%
Pressure sensor		3	1.981609e-008	94.575768%	153.235675y	50.57%
Input	HIMA	4	1.548069e-009	99.916874%	52.297623y	**3.95%**
F 3238	HIMA	4	1.548069e-009	99.916874%	104.595246y	3.95%
F 3238	HIMA	4	1.548069e-009	99.916874%	104.595246y	3.95%
CPU	HIMA	4	7.235500e-009	99.769363%	27.396384y	**18.47%**
F 8650E	HIMA	4	7.235500e-009	99.769363%	54.792767y	18.47%
F 8650E	HIMA	4	7.235500e-009	99.769363%	54.792767y	18.47%
Connector	HIMA	4	2.274887e-009	99.952465%	101.997187y	**5.81%**
F 7553	HIMA	4	2.274887e-009	99.952465%	203.994373y	5.81%
F 7553	HIMA	4	2.274887e-009	99.952465%	203.994373y	5.81%
Output	HIMA	4	1.225604e-009	99.767096%	69.888118y	**3.13%**
F 3330	HIMA	4	1.225604e-009	99.767096%	139.776235y	3.13%
F 3330	HIMA	4	1.225604e-009	99.767096%	139.776235y	3.13%
Actuator		4	7.081767e-009	94.759456%	206.126374y	**18.07%**
Valve		4	7.081767e-009	94.759456%	412.252748y	18.07%
Valve		4	7.081767e-009	94.759456%	412.252748y	18.07%

2.3.3 SIL by HFT and SFF (TÜV Approved)

System / Module	HIMA-Lib.	SIL	Type A/B	SFF	MTTF
Total result		2		98.458762%	10.241866y
Sensor		2		94.575768%	76.617837y
Pressure sensor		2	B	94.575768%	153.235675y
Pressure sensor		2	B	94.575768%	153.235675y
Input	HIMA	3		99.916874%	52.297623y
F 3238	HIMA	3	B	99.916874%	104.595246y
F 3238	HIMA	3	B	99.916874%	104.595246y
CPU	HIMA	3		99.769363%	27.396384y
F 8650E	HIMA	3	B	99.769363%	54.792767y
F 8650E	HIMA	3	B	99.769363%	54.792767y
Connector	HIMA	3		99.952465%	101.997187y
F 7553	HIMA	3	B	99.952465%	203.994373y

F 7553	3	B	99.952465%	203.994373y
Output	3		99.767096%	69.888118y
F 3330	3	B	99.767096%	139.776235y
F 3330	3	B	99.767096%	139.776235y
Actuator	2		94.759456%	206.126374y
Valve	2	B	94.759456%	412.252748y
Valve	2	B	94.759456%	412.252748y

2.4 Result for T1 =3 years

2.4.1 Lo-Demand-Result

System / Module	HIMA-Lib.	SIL	PFD	SFF	MTTF	Percent of PFx
Total result		4	3.803752e-005	98.458762%	10.241866y	**100.00%**
Sensor		4	2.704150e-005	94.575768%	76.617837y	**71.09%**
Pressure sensor		4	2.704150e-005	94.575768%	153.235675y	71.09%
Pressure sensor		4	2.704150e-005	94.575768%	153.235675y	71.09%
Input		4	1.472911e-007	99.916874%	52.297623y	**0.39%**
F 3238		4	1.472911e-007	99.916874%	104.595246y	0.39%
F 3238		4	1.472911e-007	99.916874%	104.595246y	0.39%
CPU		4	9.563758e-007	99.769363%	27.396384y	**2.51%**
F 8650E		4	9.563758e-007	99.769363%	54.792767y	2.51%
F 8650E		4	9.563758e-007	99.769363%	54.792767y	2.51%
Connector		4	7.778032e-008	99.952465%	101.997187y	**0.20%**
F 7553		4	7.778032e-008	99.952465%	203.994373y	0.20%
F 7553		4	7.778032e-008	99.952465%	203.994373y	0.20%
Output		4	1.808246e-007	99.767096%	69.888118y	**0.48%**
F 3330		4	1.808246e-007	99.767096%	139.776235y	0.48%
F 3330		4	1.808246e-007	99.767096%	139.776235y	0.48%
Actuator		4	9.633747e-006	94.759456%	206.126374y	**25.33%**
Valve		4	9.633747e-006	94.759456%	412.252748y	25.33%
Valve		4	9.633747e-006	94.759456%	412.252748y	25.33%

2.4.2 Hi-Demand-Result

System / Module	HIMA-Lib.	SIL	PFH	SFF	MTTF	Percent of PFx
Total result		3	3.808189e-008	98.458762%	10.241866y	**100.00%**
Sensor		3	1.898312e-008	94.575768%	76.617837y	**49.85%**
Pressure sensor		3	1.898312e-008	94.575768%	153.235675y	49.85%
Pressure sensor		3	1.898312e-008	94.575768%	153.235675y	49.85%
Input		4	1.543332e-009	99.916874%	52.297623y	**4.05%**
F 3238		4	1.543332e-009	99.916874%	104.595246y	4.05%
F 3238		4	1.543332e-009	99.916874%	104.595246y	4.05%
CPU		4	7.092196e-009	99.769363%	27.396384y	**18.62%**
F 8650E		4	7.092196e-009	99.769363%	54.792767y	18.62%
F 8650E		4	7.092196e-009	99.769363%	54.792767y	18.62%
Connector		4	2.271798e-009	99.952465%	101.997187y	**5.97%**
F 7553		4	2.271798e-009	99.952465%	203.994373y	5.97%
F 7553		4	2.271798e-009	99.952465%	203.994373y	5.97%
Output		4	1.220866e-009	99.767096%	69.888118y	**3.21%**
F 3330		4	1.220866e-009	99.767096%	139.776235y	3.21%
F 3330		4	1.220866e-009	99.767096%	139.776235y	3.21%
Actuator		4	6.970578e-009	94.759456%	206.126374y	**18.30%**
Valve		4	6.970578e-009	94.759456%	412.252748y	18.30%
Valve		4	6.970578e-009	94.759456%	412.252748y	18.30%

2.4.3 SIL by HFT and SFF (TÜV Approved)

System / Module	HIMA-Lib.	SIL	Type A/B	SFF	MTTF
Total result		2		98.458762%	10.241866y
Sensor		2		94.575768%	76.617837y
Pressure sensor		2	B	94.575768%	153.235675y
Pressure sensor		2	B	94.575768%	153.235675y
Input		3		99.916874%	52.297623y
F 3238		3	B	99.916874%	104.595246y
F 3238		3	B	99.916874%	104.595246y
CPU		3		99.769363%	27.396384y
F 8650E		3	B	99.769363%	54.792767y
F 8650E		3	B	99.769363%	54.792767y
Connector		3		99.952465%	101.997187y
F 7553		3	B	99.952465%	203.994373y

F 7553		3	B	99.952465%	203.994373y
Output		3		99.767096%	69.888118y
F 3330		3	B	99.767096%	139.776235y
F 3330		3	B	99.767096%	139.776235y
Actuator		2		94.759456%	206.126374y
Valve		2	B	94.759456%	412.252748y
Valve		2	B	94.759456%	412.252748y

Contents

1 Project overview

1.1 Projectfiles

D:/SILence/HIMatrix.ssy (ID:)

1.2 Project history

1.2.1 Change dated 27.10.2003 - 17:51:01

Version:
Author:
Comment:

2 System configuration:HIMatrix.s

File: SILence -Editor [D:/SILence/HIMatrix.ssy]
File-CRC: 3826824c

2.1 File History

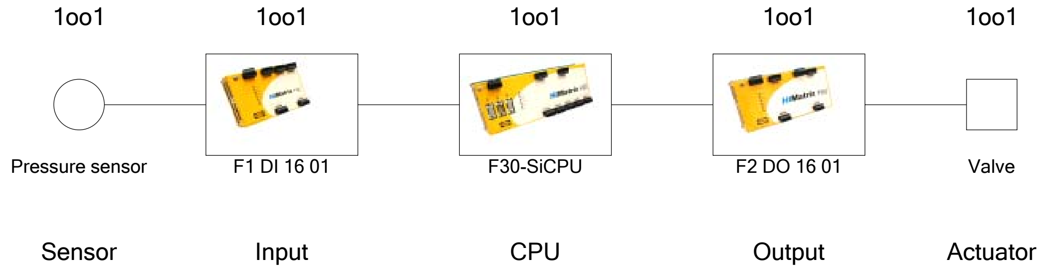
2.1.1 Change dated 27.10.2003 - 18:01:21

Version:
Author:
Comment:

2.1.2 Change dated 27.10.2003 - 18:01:21

Version:
Author:
Comment:

2.2 System configuration:



2.2.1 Libraries

Sensor: Architecture1oo1

Pressure sensor (ID: 1A209F1E-AEDFA77F) Pressure sensor / Pressure switch

Input: Architecture1oo1

F1 DI 16 01 (ID: 91841218-E6357FD0) RIO-NC input module

CPU: Architecture1oo1

F30-SiCPU (ID: 91841218-7B49D56E) Prozessor-BG

Output: Architecture1oo1

F2 DO 16 01 (ID: 91841218-32A4070D) RIO-NC output module

Actuator: Architecture1oo1

Valve (ID: 1A209F1E-4EDB05A5) Valve

2.3 Result for T1 =10 years

2.3.1 Lo-Demand-Result

System / Module	HIMA-Lib.	SIL	PFD	SFF	MTTF	Percent of PFx
Total result		2	2.525149e-003	98.875078%	8.567274y	**100.00%**
Sensor		2	1.772878e-003	94.575768%	153.235675y	**70.21%**
Pressure sensor		2	1.772878e-003	94.575768%	153.235675y	70.21%
Input	HIMA	4	3.684285e-005	99.794617%	45.019226y	**1.46%**
F1 DI 16 01	HIMA	4	3.684285e-005	99.794617%	45.019226y	1.46%
CPU	HIMA	4	4.246487e-005	99.850789%	50.361870y	**1.68%**
F30-SiCPU	HIMA	4	4.246487e-005	99.850789%	50.361870y	1.68%
Output	HIMA	4	3.625669e-005	99.773403%	15.220091y	**1.44%**
F2 DO 16 01	HIMA	4	3.625669e-005	99.773403%	15.220091y	1.44%
Actuator		3	6.367061e-004	94.759456%	412.252748y	**25.21%**
Valve		3	6.367061e-004	94.759456%	412.252748y	25.21%

2.3.2 Hi-Demand-Result

System / Module	HIMA-Lib.	SIL	PFH	SFF	MTTF	Percent of PFx
Total result		3	6.443690e-008	98.875078%	8.567274y	**100.00%**
Sensor		3	4.040864e-008	94.575768%	153.235675y	**62.71%**
Pressure sensor		3	4.040864e-008	94.575768%	153.235675y	62.71%
Input	HIMA	4	2.772602e-009	99.794617%	45.019226y	**4.30%**
F1 DI 16 01	HIMA	4	2.772602e-009	99.794617%	45.019226y	4.30%
CPU	HIMA	4	2.841588e-009	99.850789%	50.361870y	**4.41%**
F30-SiCPU	HIMA	4	2.841588e-009	99.850789%	50.361870y	4.41%
Output	HIMA	4	3.902687e-009	99.773403%	15.220091y	**6.06%**
F2 DO 16 01	HIMA	4	3.902687e-009	99.773403%	15.220091y	6.06%
Actuator		3	1.451138e-008	94.759456%	412.252748y	**22.52%**
Valve		3	1.451138e-008	94.759456%	412.252748y	22.52%

2.3.3 SIL by HFT and SFF (TÜV Approved)

System / Module	HIMA-Lib.	SIL	Type A/B	SFF	MTTF
Total result		2		98.875078%	8.567274y
Sensor		2		94.575768%	153.235675y
Pressure sensor		2	B	94.575768%	153.235675y
Input	HIMA	3		99.794617%	45.019226y
F1 DI 16 01	HIMA	3	B	99.794617%	45.019226y
CPU	HIMA	3		99.850789%	50.361870y
F30-SiCPU	HIMA	3	B	99.850789%	50.361870y
Output	HIMA	3		99.773403%	15.220091y
F2 DO 16 01	HIMA	3	B	99.773403%	15.220091y
Actuator		2		94.759456%	412.252748y
Valve		2	B	94.759456%	412.252748y

2.4 Result for T1 =3 years

2.4.1 Lo-Demand-Result

System / Module	HIMA-Lib.	SIL	PFD	SFF	MTTF	Percent of PFx
Total result		3	7.682571e-004	98.875078%	8.567274y	**100.00%**
Sensor		3	5.339494e-004	94.575768%	153.235675y	**69.50%**
Pressure sensor		3	5.339494e-004	94.575768%	153.235675y	69.50%
Input	HIMA	4	1.316872e-005	99.794617%	45.019226y	**1.71%**
F1 DI 16 01	HIMA	4	1.316872e-005	99.794617%	45.019226y	1.71%
CPU	HIMA	4	1.661682e-005	99.850789%	50.361870y	**2.16%**
F30-SiCPU	HIMA	4	1.661682e-005	99.850789%	50.361870y	2.16%
Output	HIMA	4	1.273505e-005	99.773403%	15.220091y	**1.66%**
F2 DO 16 01	HIMA	4	1.273505e-005	99.773403%	15.220091y	1.66%
Actuator		3	1.917872e-004	94.759456%	412.252748y	**24.96%**
Valve		3	1.917872e-004	94.759456%	412.252748y	24.96%

2.4.2 Hi-Demand-Result

System / Module	HIMA-Lib.	SIL	PFH	SFF	MTTF	Percent of PFx
Total result		3	6.437029e-008	98.875078%	8.567274y	**100.00%**
Sensor		3	4.040864e-008	94.575768%	153.235675y	**62.78%**
Pressure sensor		3	4.040864e-008	94.575768%	153.235675y	62.78%
Input	HIMA	4	2.751651e-009	99.794617%	45.019226y	**4.27%**
F1 DI 16 01	HIMA	4	2.751651e-009	99.794617%	45.019226y	4.27%
CPU	HIMA	4	2.818622e-009	99.850789%	50.361870y	**4.38%**
F30-SiCPU	HIMA	4	2.818622e-009	99.850789%	50.361870y	4.38%
Output	HIMA	4	3.879992e-009	99.773403%	15.220091y	**6.03%**
F2 DO 16 01	HIMA	4	3.879992e-009	99.773403%	15.220091y	6.03%
Actuator		3	1.451138e-008	94.759456%	412.252748y	**22.54%**
Valve		3	1.451138e-008	94.759456%	412.252748y	22.54%

2.4.3 SIL by HFT and SFF (TÜV Approved)

System / Module	HIMA-Lib.	SIL	Type A/B	SFF	MTTF
Total result		2		98.875078%	8.567274y
Sensor		2		94.575768%	153.235675y
Pressure sensor		2	B	94.575768%	153.235675y
Input	HIMA	3		99.794617%	45.019226y
F1 DI 16 01	HIMA	3	B	99.794617%	45.019226y
CPU	HIMA	3		99.850789%	50.361870y
F30-SiCPU	HIMA	3	B	99.850789%	50.361870y
Output	HIMA	3		99.773403%	15.220091y
F2 DO 16 01	HIMA	3	B	99.773403%	15.220091y
Actuator		2		94.759456%	412.252748y
Valve		2	B	94.759456%	412.252748y

Appendix B

Installing and Registering *SILence*

PC Requirements

- Pentium III (600 MHz or higher)
- 256 MB RAM
- 500 MB free hard disk capacity
- Resolution: 1024 x 768 pixel or higher (required: 1280 x 1024 pixel)
- Microsoft Windows NT®, 2000® or XP®

Note	Make sure that the network interface card is correctly installed and activated. In Windows XP switch off the energy saver mode for the network interface card.

Installing of *SILence*

Install ***SILence*** on the PC, on which you would like to work later with ***SILence***.

Important	Make sure that ***SILence*** will be used on this PC. After registration, ***SILence*** can only be used on this PC. For each additional PC, a new license must be acquired.

Installing notes

Insert the CD into the CD drive. A few seconds later, set-up will start automatically. With certain settings, for example if the CD drive's auto run function of the CD drive has been deactivated deactivated, start the set-up program manually. In this case, double click the "setup.exe" file in the CD's root directory. When set-up has been started, the CD's operator interface will be displayed with various options . Follow the program's instructions.

Hotline +49 (0)62 02 709-255/-258

Registering *SILence*

Important	The Access Code for ***SILence*** is determined from the license number and the PC specifications. The Access Code can only be used on this PC! Make sure that ***SILence*** will be used on this PC. For each additional PC, a new license must be acquired.

To complete the registration of ***SILence***

- Start ***SILence*** to open the „Registration“ dialog box.

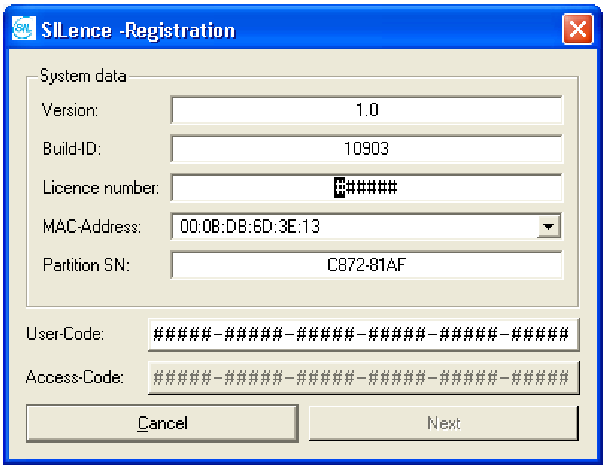


Fig. 66: „Registration“ Dialog Box after First Starting *SILence*

The “Registration” dialog box contains following data:

Data	Description
Version	Version of ***SILence***.
BuildID	Identity number of ***SILence***.
License	License number (on the CD cover)
MAC address	MAC address of the network module in the PC (automatically recognized).
Partition SN	Serial number of the PC’s hard disk (automatically recognized)
User Code	Code determined from the license number and the PC specifications
Access Code	Code determined from the User Code. The Access Code is provided by HIMA support group.

To determine the User Code:

- Enter the license number in the *Licence number* field. The license number is located on the CD cover.

After entering the licence number, the “User Code” is displayed in the identically named field.

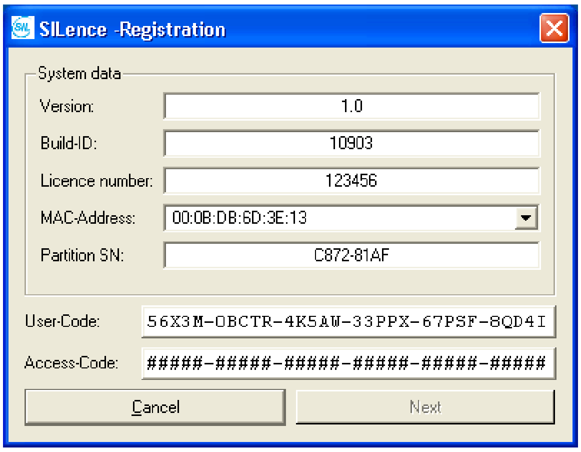


Fig. 67: Determined User Code after Entering the License Number

To determine the Access Code:

- Go to the ***SILence*** registration page on the HIMA Homepage www.hima.com
- Follow the instructions from the registration

Note	Note down or print out the Access-Code for ***SILence***.

To register ***SILence*** using the Access Code:

- Enter the Access Code into the *Access-Code* field.
- Click *Next* to confirm the registration.

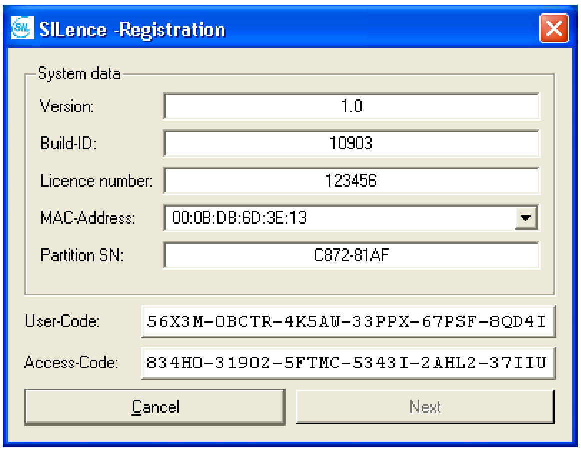


Fig. 68: Access Code Determined by HIMA

If you have problems with the registration or installation, please contact the HIMA-Support.

Hotline +49 (0) 6202 709-255/ -258

or

Phone : **+49 (0)6202 709-0**
FAX : **+49 (0)6202 709 107**
E-mail : **info@hima.com**

Please keep the following costumer data at hand:

- Adress,
- Costumer number,
- Licence number,
- Access Code from ***SILence***.

The HIMA Support engineer needs this data to generate the Access code for your ***SILence*** registration.

References of literature

[1] IEC/EN 61508: International Standard 61508 Functional Safety: Safety-Related System. Geneva, International Electrotechnical Commission, IEC Verlag Genf 1999

[2] *Börcsök, J.*: IEC/EN 61508 – eine Norm für viele Fälle, 2002

[3] *Börcsök, J.*: Sicherheitsbetrachtungen, 2003

[4] *Börcsök, J.*: Konzepte zur methodischen Untersuchung von Hardwarearchitekturen in sicherheitsgerichteten Anwendungen, 2002

[5] DIN V VDE 0801: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (E/E/PES), (IEC 65A/255/CDV:1998), S. 27f, Beuth Verlag Berlin August 1998

[6] DIN V 19250: Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen, Beuth Verlag Berlin 1998

[7] DIN V VDE 0801/A1: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben, Beuth Verlag Berlin 1990 und 1994

[8] IEC 60880-2: Software für Rechner mit sicherheitskritischer Bedeutung, 12/2001

HIMA
...the safe decision.

HIMA Paul Hildebrandt GmbH + Co KG
Industrial Automation
Postfach 1261 • D - 68777 Bruehl
Phone: (+49) 6202 709-0 • Fax: (+49) 6202 709-107
E-mail: info@hima.com • Internet: www.hima.com

(0342)