Department responsible: EN-ED-PC/BGH
Owner: Konrad Estermaier, EN-ED-PC / Approver: Peter Schöler, EN-ED

Supersedes version: 2019-11'

Suitability Range

This plant standard is mandatory, without limitation, for all regions of the Wacker group. Additionally, Service Center guidance is that adherence be maintained by all Wacker sites, regardless of location, as a best practice. This standard shall be reviewed by the responsible party on a case-by-case basis.

Supplements to This Plant Standard

Supplement 3	Safety Instrumented System Classification Analysis – Template of WF AS1075
Supplement 4	List of process-control EI&C equipment relevant to the quality, environmental, safety and energy-management system – template of WF ET1030
Supplement 5	Pre-commissioning testing certificate of safety-related PCE locations – template of WF ET1086
Supplement 6	Report on initial inspection – template of WF ET1526
Supplement 7	EI&C – Preventive maintenance – template of WF ET1386
Supplement 8	Step-by-step documentation
Supplement 10	Documents for Inspecting PCE Protective Equipment
Supplement 11	Procedure for SIL calculation and typicals
Supplement 12	Modification of safety instrumented systems
Supplement 13	Comparison of safety-related control systems

Contents

1 Aim

This plant standard shall be used for the planning, design, commissioning, testing and operating of safety instrumented systems (SIS). It also aims to bring about a coherent strategy for the installation and maintenance of this type of system.

This standard covers safety instrumented systems that safeguard processing plants in the chemical industry. It is based on IEC 61511-1 to 3 / ANSI/ISA 84.00.01-1 to 3 (hereafter referred to as IEC 61511).

The purpose of this plant standard is to draw attention to the existing rules, regulations, standards and provisions, to point out the key passages and to draw up a set of rules which will facilitate efficient, harmonized implementation across the plant.

2 Definitions

To facilitate the consistent use of key terms, the following definitions are binding.

2.1 Diversity

Diversity, or diverse redundancy, i.e. redundancy using dissimilar means

Note: When diversity is required, a physically different measurement should be used whenever possible (e.g. pressure and temperature measurements for safeguarding a vessel). If this is not possible, the same physical parameter may be used but it must be measured by different methods (e.g. 2 pressure measurements obtained using different makes of equipment and different measuring principles).

2.2 Process Fault Tolerance Time or Process Safety Time

The process safety time is also known as the process fault tolerance time and is defined as the period of time between a failure occurring in the process or in the BPCS and the occurrence of the hazardous event if the safety function has not been activated. (IEC 61511-2 Section 11.9.2)

2.3 Response Time

The period of time from the detection of the unsafe condition to the activation of the countermeasure is described as the response time. Typically, the response time should be ≤ ½ process safety time. Possible post-reactions and tailings must be observed.

2.4 Basic Process Control Systems

Basic process control systems (BPCS) ensure the correct operation of a plant. This includes all controllers and normal process switches and measurements which operate the plant in its normal operating range (e.g. switching point of a vessel's filling-level measurement (LSH)).

2.5 SIS Classification Analysis

The SIS Classification Analysis team shall include the safety engineer (or safety representative), the plant EI&C engineer, the plant process engineer, the production manager, the chemical process expert (chemical safety/process owner) and, in the cases of new design, the design process engineer and design electrical engineer. During the analysis, the hazardous event identified by the Wacker Analysis is further analyzed and evaluated via the WF AS 1075 or in COMOS via the PQBB.

2.6 Controlled Shutdown (Plant Off)

To prevent economic losses, a controlled shutdown can be used.
The determination of the possible consequence severity and the necessity of a plant shutdown may be made in the context of the Wacker safety analysis. The detailed description will be made within the requirements of the specification. It's not for emergency. Realization in the BPCS.

For example to avoid damage to equipment.

2.7 Emergency Stop / Emergency Shutdown

An Emergency Stop for process plants can be useful as an additional manual intervention for other protective measures and is necessary:

- to avoid imminent personnel injury
- to avoid environmental impact
- to address a Loss of Primary Containment of a hazardous chemical that is either active or imminent (i.e., a leak is occurring or will occur if action is not taken immediately)

It serves to prevent / limit a (further) damage, especially in case of unspecific events, if detection / intervention is only possible by employees or cannot be secured by EI&C technology alone. (e.g., leakage with unknown exit or heavy smoke).

The determination of the possible extent of damage and the necessity of an Emergency Stop are carried out by the analysis team for carrying out systematic safety assessments (see section 4.4, A 07-04-04).

Realization:

- no SIL calculation is required
- proven in used devices
- closed-circuit principle
- programmable controllers must meet at least SIL2 requirements or hardwired logic
- initial test and regular proof test

2.8 EI&C Systems for Plant Safety

2.8.1 Process control monitoring systems

These help to ensure that the plant operates as specified. In safety terms, their role is to indicate when process variables (e.g. pressure) are no longer within the normal operating range but are still within the tolerable risk range, and/or to automatically restore these parameters to the normal range; i.e. such systems are triggered at the transition between the normal operating range and the permitted fault range.

The plant can still continue operating when the process control monitoring system responds.

Process control monitoring systems particularly include process control systems that are upstream of the direct-acting protective devices (e.g. safety valves, rupture discs) or safety instrumented systems in order to prevent them, if possible, from being triggered.

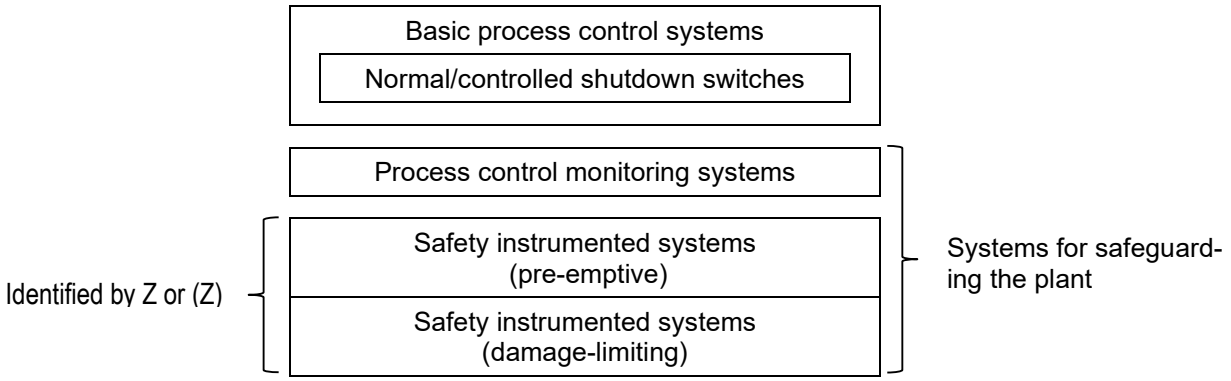


Figure 1 – Explanation on the definition under 2.7

2.8.2 Safety Instrumented Systems (SIS)

Unlike the basic process control system and the process control monitoring system, the function of the safety instrumented system is to prevent a process excursion in the plant.
A safety instrumented system mitigates the residual risk of the failure of administrative controls, all upstream and operational measures, and all EI&C operational and monitoring equipment.

In the absence of a safety instrumented system (that is deemed necessary on the basis of a safety review), it must be anticipated that conditions in the plant could arise that could cause personal injury and serious environmental or equipment damage or provoke a “serious risk” within the context of the governing body’s functional safety management standards.

2.8.3 Safety Integrity Level (SIL)

Discrete level (SIL level 1-4) for specifying the safety integrity requirements of the safety instrumented functions (SIFs). Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest. The SIL level 4 is not achievable with electronic systems alone. They are rare in the process industry and shall be avoided where reasonably practicable.

2.8.4 Safety Instrumented Function (SIF)

Safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function.

2.9 Safety requirements Specification (SRS)

The Safety Requirements Specification specify the requirements for the SIS, including any application programs and the architecture of the SIS.

The SIS requirements shall be expressed and structured in such a way that they are

- clear, precise, verifiable, maintainable and feasible;
- written to aid comprehension and interpretation by those who will utilize the information at

any phase of the safety life-cycle.

2.9.1 Safety Instrumented Systems for Explosion Damage Protection

If safety instrumented systems are used to reduce explosion zones, they become active protective measures in explosion damage protection.

2.10 Damage Limitation Systems

Damage limitation systems serve to limit the possible effects in the event of a major accident. These systems differ from prevention systems in that it is assumed the event has already occurred. They may be implemented via BPCS or via the SIS, as determined by the risk analysis team.

2.11 Tolerable Risk

Tolerable risk is the maximum acceptable risk of a specific technical process or condition. It is usually described indirectly in terms of safety requirements.

The tolerable risk is determined by subjective and objective influences and may vary considerably from application to application.

Subjective influences include:

- Personal perceptions of danger, which may depend, for instance, on whether a hazard is visible or not, or whether the persons at risk have any influence on the process; Social acceptance of dangers.

2.12 Active Fault

Active (function-initiating) fault, which triggers the safety function without the specified conditions being fulfilled (i.e. unnecessary, spurious trip).

2.13 Passive Fault

Passive (function-inhibiting) fault, which blocks the safety function (of the relevant channel) although all the specified conditions have been met (i.e. the requisite protective function would not have been fulfilled).

2.14 Validation

Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled. This means demonstrating that the SIF and SIS after installation meet the SRS in all respects. Validation encompasses checking the safety-relevant system against the specifications of the safety requirements as a whole, which include the stipulations outlined in this standard, the WF AS1075, and any relevant functional descriptions of associated loops/equipment.

2.15 Verification

Theoretical or practical demonstration - for each phase of the safety life cycle in question – that for specified inputs, the deliverables meet the requirements and objectives for the phase concerned.

2.16 Competent Person/Qualified Personnel (IEC61511-1 5.2.2.2)

Persons involved in SIS safety life-cycle activities shall be competent to carry out the activities for which they are accountable.

- engineering knowledge, training and experience appropriate to the process application
- engineering knowledge, training and experience appropriate to the applicable technology used (e.g., electrical, electronic or programmable electronic)
- engineering knowledge, training and experience appropriate to the sensors and final elements
- safety engineering knowledge (e.g., process safety analysis)
- knowledge of the legal and regulatory functional safety requirements
- adequate management and leadership skills appropriate to their role in the SIS safety lifecycle activities
- understanding of the potential consequence of an event
- the SIL of the SIF

  the novelty and complexity of the application and the technology

3 Management of Functional Safety

In accordance with IEC 61511-1, management activities shall be described as those activities necessary to ensure that functional safety objectives are met.

These management measures – including the adherence to the regulations referred to in Section **Fehler! Verweisquelle konnte nicht gefunden werden.** – are generally required when implementing or modifying safety instrumented systems.

The following on-going management activities are required during the course of the project and shall be documented.

3.1 Defining Responsibilities

As part of EI&C project planning, personnel shall be specified, and their responsibilities defined (form WF 10-0003).

3.2 Safety Life Cycle

Safety planning requires the definition of a safety life cycle, and it must be structured according to the following phases (see IEC 61511-1 Section 6):

- Hazard and risk assessment
- Allocation of safety functions to protection layers (Risk Graph Analysis)
- Safety requirements specification for the SIS
- Basic engineering and Design planning
- Installation, commissioning and validation

- Operation and maintenance
- Change/modification
- Decommissioning

The documentation required for each life cycle phase is specified in Plant Standard G-WN 08-26-01 WGER Bbl 8.

3.3 Verification

The aim of verification is to show that the results from each phase of the safety life cycle meet the defined objectives and requirements of the phase, in every respect.

Table 1 – Verification Plan Requirements and Activities (as per **IEC 61511**-1, Section 7.1.1)

Requirements	Measures
List of verification tasks	Test ▪ hardware design ▪ software design (if available) ▪ installation and maintenance using Form WF 10-0009
Timescale for described tasks	The inspection dates shall be entered in the project schedule
Naming the persons responsible	The persons responsible for the tasks shall be specified using Form WF 10-0003
List of the equipment to be verified	All equipment to be verified (safety instrumented systems) shall be listed using Form WF ET1030
List of the documentation required for carrying out the verification	Records required for verification shall be compiled using the following Forms: ▪ WF ET1086 ▪ WF ET1526 or WF 10-0010 ▪ WF 10-0003 ▪ WF 10-0009
Modification	WF ET 1786 Site-specific management of change procedure
Decommissioning	WF ET 1786 Decommissioning shall be reasoned and documented

3.4 Validation

The objective of validation is inspection and testing of the installed and commissioned SIS and its associated SIF(s) against the requirements as stated in the SRS.

3.5 Assessment

The assessment:

- includes checking if everything is listed as planned
- is performed for each phase of the life cycle
- is carried out with sufficient independence and expertise.

Assessment shall be based on WF 10-0009.

The assessment team shall include at least one experienced person who was not involved in the project design (or planning measures).

SIL 1: competent person from the same department

SIL 2: competent person from another department

SIL 3: Competent internal functional safety expert or competent external functional safety expert (if deemed necessary by internal expert) technical office responsible for functional safety, or inspection authority

Note: Changes based strictly in software may be assessed via desktop review (or remote desktop witness). Introduction of new field sensors or actors into SIF loops require additional on-site field verifications by the qualified person. New SIF devices include both new installations and incorporation of existing installations repurposed for use in the SIS.

4 Hazard and Risk Analysis

The groupwide uniform procedures for the development, documentation, update and review of the plant engineering safety plan and the role of the involved functions are regulated in the directive A 07-04-04.

The risk shall always be reduced at least to the tolerable risk level, either by non-process control measures and/or by SIS measures. These measures may be of a technical and/or organizational nature and may complement each other or be used in place of each other.

A systematic safety analysis must be performed for all plants and processes. This documented analysis must be made available and always kept up to date.

The following tools are applied for the systematic safety assessment:

- Plausibility check WF AS1460
- WACKER analysis WF AS1065B

5 Classification of Safety Instrumented Systems

When safety instrumented systems are required for risk reduction, they shall be in accordance with IEC 61511-1 to 3.

5.1 Hazard Analysis and Risk Assessment

A hazard analysis and risk assessment must be conducted for each safety instrumented function during the safety review so that suitable measures relating to the protective function can be determined and specified.

The safety review shall be convened by the project manager and concluded before planning for the actual engineering even begins (WF AS1075).

The result of this review, which operators, the safety department, the technical department (process engineers and responsible EI&C engineer) shall attend, shall be recorded using WF AS1075 and signed by the participants.

The primary objective of this safety review is to identify and specify suitable mechanical protective equipment and safeguards (i.e. safety relief valves and rupture discs). If adequate protective function cannot be achieved using direct-acting devices (e.g. safety valves and bursting discs), safety instrumented systems shall be specified to compliment the protective function.

In cases where no other non-SIS independent protective systems (e.g. rupture disks, pressure safety valves, etc.) are installed or they do not have adequate relief capacity, the SIF acts as the sole safety protective system to prevent an impermissible operating condition with respect to equipment design pressure or temperature.

In accordance with the hazard analysis and risk assessment (see IEC 61511-1, Section 8), the following points and requirements shall be considered and documented in AS1075:

- Description of all essential safety-relevant functions for the requisite functional safety
- Definition of safe state
- Specification of the trigger for a demand and its estimated demand frequency (probability of occurrence)
- Preferred interval between retests
- Response times of the safety-relevant system to bring the process to a safe state
- Determining the SIL
- Signal inputs and their trip points
- Signal outputs and their mode of action (e.g. close on trip)
- Functional correlation between signal inputs and outputs (see also functional description)
- Requirements for shutting down the plant by manual operation (if applicable)
- Requirements for resetting the safety-relevant system (if applicable)
- Commissioning requirements (if applicable)
- Any exceptional interfaces between the safety-relevant system and other systems
- Description of the plant operating modes and a list of the safety-relevant functions required to operate the plant in each of these operating modes
- Safety requirements of the user software
- Bypass requirements
- Consideration of environmental conditions and product characteristics

5.2 Risk Parameters

From the wide range of factors potentially influencing both, safety requirements and measures, four key parameters shall be considered; these permit a qualitative appraisal of the risks involved:

a) Consequence severity
   - S1: Minor injury, minor environmental impact, limited or no potential for a severe incident *)
   - S2: Serious permanent injury to one or more persons, one fatality; temporary, significant environmental impacts, major incident*)
   - S3: Major injuries, fatalities; severe, long-lasting environmental impact, major incident *)
   - S4: Multiples fatalities, catastrophic environmental effects, significant asset loss or business interruption, major incident *)

b) Exposure Frequency to hazard (of persons)
   - F1: Rare to fairly often
   - F2: Frequent to permanent

c) Opportunity to Prevent
   - P1: Possible under limited conditions
   - P2: None

d) Likelihood of Consequence Occurrence
   - L1: Very low
   - L2: Low
   - L3: Relatively high

Caution: IEC 61511-1 9.3.2 states that the risk reduction claimed for a BPCS protection layer shall be ≤10. As such, for S2, P1 and L1 must not both be selected unless there is an administrative control or technical measure completely independent from the BPCS. For example, one safeguard or control acting hardwired, with a separate PLC or a safety system or with a separate process unit.

For explanations of the risk parameters see the completion instructions in WF AS1075.

These risk parameters are used to determine the **S**afety **I**ntegrity **L**evel (SIL) as per IEC 61511-3 – represented in the risk graph in WF AS1075.

If a SIL greater than or equal to 1 is obtained, the code letter Z shall be used to identify the switching function at the appropriate process control location (as per IEC 62424).

SIL 4 cannot be covered by safety instrumented systems alone. Measures additional to PCE are essential to reduce the risk to at least SIL 3. Organizational measures shall also be implemented.

The SIL is derived from the graded risk parameters as shown in the risk graph (Figure 2).

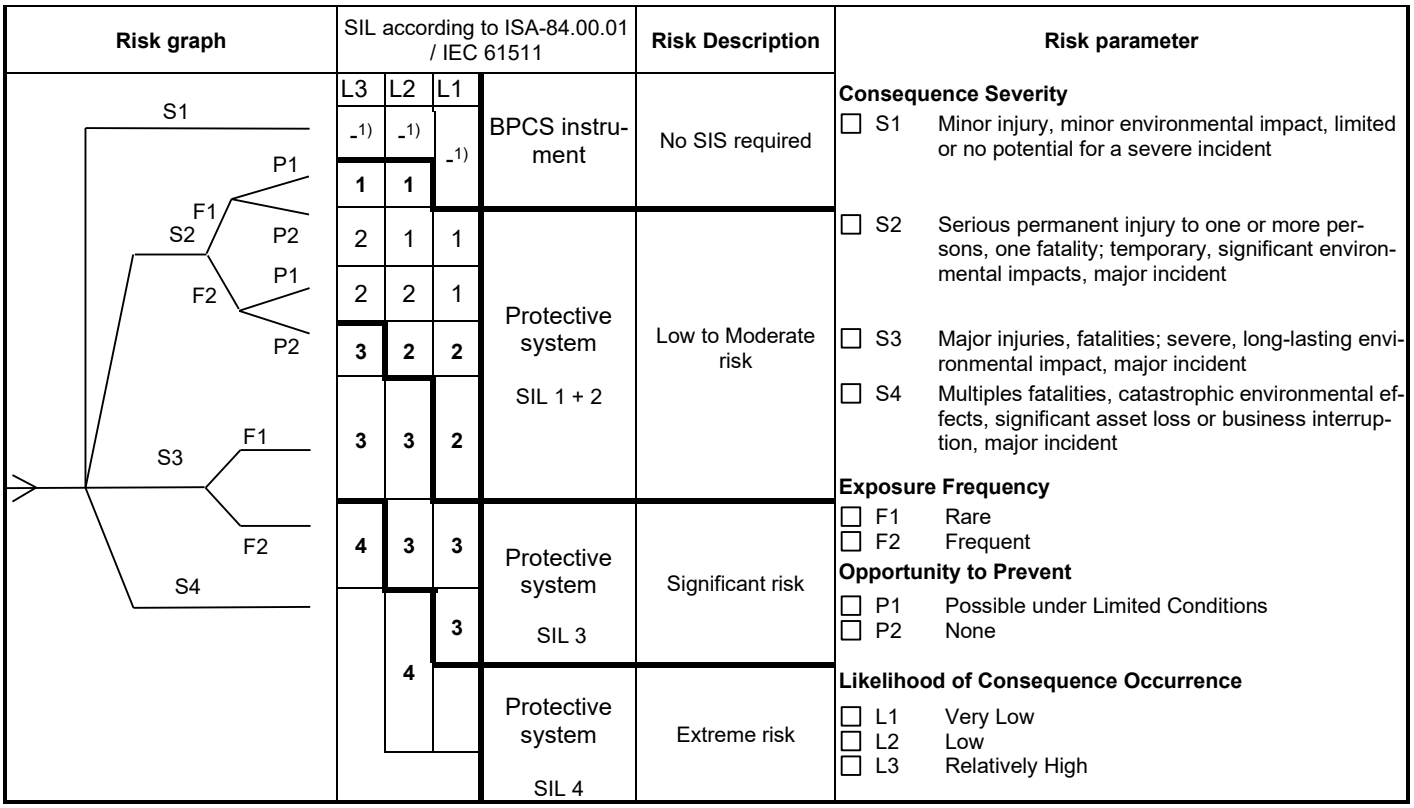


Figure 2 – Risk Graph as per WF AS1075

6 Engineering and Design

The following points should be observed when planning the safety instrumented system:

- There must be a description of the safety function and the requirements must be specified.
- The safe state or the safe intermediate state shall be defined.
- Consideration must be given to factors that influence the safety function (mutual influence on safety functions, e.g. emergency pressure relief on combined vessels, reaction times and environmental conditions).
- Retests must be performed.
- Consideration must be given to demand rates (typically low demand mode in process plants).
- The behavior of the safety instrumented system outside of normal operation.
- If online testing will be required, then bypass facilities shall be included in the design to allow for such testing (i.e. bypass valves, redundant devices, etc.) (IEC 61511 11.8.2)
    - Note: Special software programming should also be considered to facilitate such testing

6.1 Protection Design Requirements and Best Practices

The design requirements and best practices specify the general requirements of the safety instrumented system. These should be treated as general rules, with explicit direction denoted by “shall.”

6.1.1 Architecture Design

6.1.1.1 Basic Measures

- Use proven, dependable installation techniques.
- The safety instrumented system must be clear and simple in design. Suitable mechanisms should be in place to minimize any further effects of a possible failure. Examples of such mechanisms are:

– High-resistance decoupling
– Short-circuit resistance
– Galvanic isolation

[1] No SIS required

- preferably use de-energize to trip
- design the safety function in such a way that device failures bring the system to a safe state.
- Take steps to prevent unauthorized persons from changing the threshold limits.
- Ensure that deviations in energy supplies (such as the control air, electrical power, etc.) exceeding the acceptable tolerances of the equipment never lead to a shutdown of the safety instrumented system. This type of shutdown can be prevented by:

– The equipment's properties
– Using redundancy, etc. to ensure a continuous energy supply
– Implementing the functionality necessary to automatically monitor the auxiliary power supply and trigger the necessary protective function

- When implementing redundancy for the SIS, common cause failures shall be minimized between redundant channels as much as possible.
- If the SIS's process connections are equipped with means of isolation from the process, their current status must be easily recognizable and have a mechanism to prevent accidental closure. Inadvertent isolation can be prevented by installing a locking sleeve, adding a padlocked chain, or removing the handwheel.
- Prevent automatic reengagement after the protective function has been triggered so that the reengagement can only be done in a controlled manner. Usually, reset functions are activated using a key-operated pushbutton or process control system buttons as defined in the safety requirements specification (SRS).

6.1.1.2 Hardware Fault Tolerance (HFT) – Sensors, Final Elements, and Non-PE Logic Solvers

A hardware error tolerance of *n* means that *n*+1 errors could cause the loss of the safety function.

Table 2 – Hardware Fault Tolerance HFT

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (high demand mode)	1
3 (any mode)	1

Reference IEC 61511-1 1.4

6.1.2 Shared Use Devices between SIFs and BPCS

A device used by the SIF shall not be used by the BPCS where a failure of that device may result in both a demand on the SIF and a dangerous failure of the SIF, unless an analysis has been carried out to confirm that the overall risk is acceptable. When a part of the SIS is also used for control purposes and a dangerous failure of the common equipment would cause a demand on the function performed by the SIS, then a new risk is introduced. The additional risk is dependent on the dangerous failure rate of the shared device because if the shared device fails, a demand will be created immediately to which the SIS may not be capable of responding. (IEC61511, 11.2.10)

If the device has special requirements for internal leak-tightness, e.g. block and bleed, shared use is not permitted. Shared use in SIL 1 or SIL 2 is also not permitted in new plant designs. In SIL 3 the shared use is allowed in new plant design due to the multi-channel design (HFT>0).

6.1.2.1 Requirements for Shared Use Devices in SIFs

In assessing overall risk of shared use devices, the following conditions must be considered:

- The risk graph analysis does not take additional credit for the multipurpose nature of the shared device (i.e. the added BPCS function of the SIS device does not equate to moving from L2 to L1 likelihood, or moving from S2 to S1 consequence severity etc.).
- The SIF is only used operationally for a short time in start-up/shutdown, purging or emptying conditions.
- Special monitoring (e.g. local personnel) can be provided
- A failure on the shared component could be detected (e.g. PST, setpoint / actual difference, etc.)
- Adequate reaction time for preventative measures is available (actual time will vary depending on system specific variables, e.g. the speed of a process change, hazard attempting to prevent, etc.)
- An opportunity for prevention exists (The measure, e.g. manual intervention, is clearly described in the PQBB/AS1075 and the employees are trained. Thus, only for P1 in the risk graph)
- In case of abnormal conditions (i.e. bad control quality due to defective positioner) a prompt repair can be performed (< 8h)

6.1.3 SIS/BPCS Relationship

6.1.3.1 SIS Structure

When designing SIS, the following aspects should be observed in addition to ensuring functional safety and the necessary availability of the production plants:

- Safety instrumented systems need to be structured according to independent, stand-alone plant sections.
- Care should be taken to separate the safety logic solver of minimally-influential systems from central/highly-impactful systems (i.e. to discourage the failure of any given system's SIS from causing widespread shut-downs).
- Implementing exclusively SIFs in the SIS
- The isolation of the systems (SIS, BPCS) must be all-encompassing (software, power supply, relays, I/O cards, etc.)
- Hardware switches/configurable control systems are a good alternative for specific applications.

6.1.3.2 Safety Systems Integrated into a BPCS

Fully integrated SIS in a PBCS offer advantages in terms of uniform technology, project planning and engineering. Due to the required separation of SIS and BPCS as well as cyber security requirements their use is no longer considered good practice. And the dependency on the BPCS version upgrade cycle also leads to a reduction in availability. The use of an integrated SIS is therefore not recommended and strongly discouraged.

6.1.3.3 Safety Systems Separate to the BPCS

The preferred practice is to separate safety systems from BPCS functions. The SIS shall be designed to be separate and independent from the BPCS to the extent that the safety integrity of the SIS is not compromised.

Advantages:

- Systems can be easily assigned to the plant structure
- Clear separation/distinction of the safety circuits from “normal” control loops possible – less risk of unintentionally deactivating safety circuits
- Possibility of operating independently of the standard BPCS (no restrictions in the standard PCS or in the SIS).
- Enhanced access control promotes a rigorous change control process, lessening opportunity for flawed modifications/unplanned downtime
- PESs with single, dedicated use (i.e. SIS only) may yield faster cycle times/shorter time to respond to SIF demand
- Highly robust in terms of cyber security (it is generally impossible to access externally)

Disadvantages:

- Separate hardware required
- Additional hardware engineering required
- Higher costs than for an integrated system (depends on the application)
- Troubleshooting for errors in two systems

6.1.3.4 Safety System partially integrated into a BPCS

- Engineering workstations can access/modify both BPCS and SIS
- BPCS and SIS can pass information and commands directly between one another (note: this requires careful design review with appropriate running requirements for control, integrity of SIS, and scrutiny of BPCS influence over SIS—i.e. reset functionality from BPCS)

6.1.3.5 Hardwired Solutions or Standalone Configurable Logic Solver

- Hardwired solutions (i.e. relays or current switches) should be used in a few, simple circuits with purely digital and few analog signals and little need for modification. These systems have limitations as online changes are not possible.
- Configurable control systems (i.e. PNOZmulti) are suitable for managing up to 30 in/outputs. Analog value processing is possible. The configurable control systems are connected to the BPCS with a Profibus or ethernet. Thanks to favorable acquisition costs and simple engineering, configurable control systems are an optimum solution for the decentralized protection of individual plant components (kneaders, reactors, agitators).

6.1.3.6 Decision Matrix for Separate, Integrated and Hardware Solution

The decision matrix provides support when selecting the most appropriate SIS, irrespective of the plant type, and also for setting up and operating key criteria.

For a comparison of different systems and manufacturers see G-WN 08-26-01 WGER Bbl 13.

Table 3 – Decision Matrix

	SIS integrated into a BPCS[3]	SIS partially integrated into a BPCS[1]	SIS separate to the BPCS	Hardware circuit/config. Control system
Proportion of safety engineering in relation to total PCS positions is very high	++	++	+	--
Proportion of safety engineering in relation to total PCS positions is very low and simple	-	-	-	++
Plant shutdown possible at any time	+	+	+	+
No/few plant shutdowns possible	-	+	++	+
Safety signals require networking	+	++	++	--
High level of software modification	-	+	+	--
Production plant expansion is possible in stages (plant extensions)	-	+	++	+
Cyber security robustness[2]	--	--	+	++

Explanation of symbols:
-- requirements not met, replacement/complementary measures required, use not recommended
- requirements part met, observe potential restrictions during use
+ requirements met
++ requirements met in full, highly suited to the described application
[1] separate controller and engineering tools for SIS and PCS in a combined engineering environment
[2] detailed explanation in section 6.1.2.7. below
[3] highly discouraged

6.1.3.7 Cyber Security Requirements

Due to the higher level of networking and use of standard BPCS components, integrated systems are more susceptible to cyber security attacks and therefore strongly inadvisable. Separate SIS including the associated engineering station are only more robust than integrated SIS to cyber security attacks if they are operated as standalone systems. When using these systems, it is important to exercise rigorous compliance with the manufacturers' specifications and the requirements of A 08-01-09 on protection against malicious software. (See also A 08-01-15 and IEC 61511-1 8.2.4)

6.1.3.8 Life Cycle Factors

When using integrated systems, the SIS must be upgraded with the standard BPCS (usually every 5 years). SIS upgrades can be very expensive (e.g. renewed acceptance by an authorized inspection party). Often, the SIS needs to be available during plant or BPCS shutdowns.

6.1.3.9 Recommended Uses

The engineering benefits of integrated SIS are often offset by performance losses due to complex testing algorithms. Separate systems avoid complex structures or intermeshing, which are difficult to manage in the event of plant expansions and disruptions (for the advantages/disadvantages see 6.1.2.2 and 6.1.2.3). The decision matrix (Table 3) can provide valuable information on SIS selection. For the majority of applications, the use of separate SIS is recommended.

6.1.4 Testing Considerations

6.1.4.1 Proof Test

Recurrent function tests are essential to identify and remedy undetected failures.

The test cycle and other important information relating to the tests, e.g. switch limit values, are determined in the risk graph analysis. In the absence of any comparable experience, the test interval shall initially be reasonably short. If the tests indicate suitable safety-related availability, the test interval can be gradually extended over time. This approach must be documented.

Test cycles shall first be determined jointly by the plant management, the EI&C engineer and the safety department and modified by this working party as required.

Test cycles can be extended so that the interval is longer than one year. Provided plant experience deems appropriate and PFD calculations are met.

When extending the test cycle, the following points must be checked:

- Are there any restrictions in terms of maintenance regulations?
- Consider the environmental conditions (e.g. housing, cooling, installation situation)
- Process connections (redundancy with partial inspection, partial stroke test etc.
- Does the EI&C and process engineering operating experience permit an extension?

A testing concept should be created as early as the planning stage:

- Maintenance and testing equipment for retesting
- Automation or PCS-based retesting (e.g. start-up of an initial setting of valves for push of a button).

6.1.4.2 Partial Stroke Test

The partial stroke test is performed during continuous plant operation. This involves the actuator moving approx. 10–15 % towards the safety position. By doing this it is possible to identify whether the actuator could, in principle, occupy the safety position. The results shall be documented.

6.1.4.2.1 Design Variants

a) Mechanical Blockade

The actuator is mechanically blocked to restrict movement to 10–15 %. By means of a manual demand (e.g. key switch), the valve is then moved in the direction of the safety position until it stops at the mechanical blockade. After the test the actuator is returned to the initial setting and the mechanical blockade removed.

b) Solenoid Valve Deactivation Signal

Using a safety control system or a special switching box, the solenoid valve is deactivated until the desired position of the actuator (10–15 % of its path) has been achieved. The drive and the actuator then return to the starting position.

c) Positioner

An intelligent positioner can independently perform and evaluate the partial stroke test in a time-controlled manner. The positioner itself is therefore a device in a safety circuit and must satisfy functional safety requirements. It may be possible to do without a solenoid valve.

6.1.4.2.2 Time Interval of the Partial Stroke Test

The PST should be performed ten times more frequently than the retest (typically once a month) and can be initiated manually or automatically.

6.1.4.2.3 Proof Test Coverage of the Partial Stroke Test

The required proof test coverage of the PST must be defined. If required for internal leak-tightness verification, the proof test coverage can be measured at a max. 50 %, otherwise it is approx. 70 %.

6.1.4.3 Online Testing

Industry best practice suggests offline testing. If this approach will not suit the design in question, additional discussion and design considerations are required. Online testing typically has an adverse effect on PFD calculations/loop integrity.

For online testing, retesting takes place during continuous operation without shutting down the plant. This needs to be taken into consideration during SIL calculations, and corresponding maintenance and testing equipment needs to be designed:

- Redundancies (e.g. 2oo3)
- Bypasses

6.1.5 BPCS Monitoring Systems

Process control monitoring systems are usually realized in the BPCS, and here too, care must be taken to ensure that proven-in-use hardware is used. These systems are usually single-channel.

6.1.5.1 BPCS Monitoring Systems having influence on Risk Parameters

It may be useful to include certain process control monitoring systems in the safety analysis (WF AS1075) for determining the SIL, since they can influence the risk parameters (predominantly the “probability of occurrence”).

6.1.5.2 Testing Monitoring Systems

Process control monitoring systems are not subject to obligatory testing or documentation unless they influence the SIL rating derived in “WF AS1075”. In a case-by-case basis they must undergo initial testing, retesting and an inspection. By default, such systems must be tested and maintained unless Operations and Engineering determine that the device is used in a continuous operational mode and any failure would be readily apparent (i.e. failure of a controller results in abnormal process conditions).

6.1.5.3 BPCS Monitoring System as the Result from the Risk Graph

If the result of the SIS classification analysis (WF AS1075) is a process control monitoring system (SIL not needed), then this must undergo regular testing and inspection, unless there is a minor consequence from device failure, then regular testing and inspection can be implemented using area discretion.

6.1.5.4 BPCS for Preventing Serious Economic Losses

Process control systems for preventing serious economic losses are designed purely from an economic point of view. If periodic inspection, testing and servicing is necessary, the plant management and the EI&C engineers can decide on the appropriate type and scope.

6.1.5.5 Monitoring the Space Between the Safety Valve and the Rupture Disc Component

If a combination of safety valve and a rupture disc is used, the space between them shall be monitored for pressure build-up. A BPCS monitoring system must be used to alert personnel to an unacceptable pressure increase in this space. The BPCS monitoring system is subjected to a full proof test. The inspection periods shall be determined and defined in a hazard analysis. Documentation in WF ET1030.

6.1.6 Human-SIS Interface

The following information should be shown within the operator interface:

- Current values of the process parameters
- Visual indicator that the safety function has been activated
- Status of the sensors and actuators
- Indication that a protective function is bypassed
- Power-loss messages, when these affect safety (for example, when using the open-circuit principle)

6.1.6.1 Safety Instrumented Functions Without a Switching Function

In this situation, operator response is part of the safety plan (as defined in IEC 61511 11.3), and must therefore be clearly defined in a standard operating procedure. The safety plan must therefore include an audible/optical alarm that is clearly recognizable as different from the operational signals.

6.1.6.2 Safety Instrumented Systems Without Sensor Technology

In this situation, the operator’s awareness of the danger and subsequent response is part of the SIS, and must therefore be clearly defined in a standard operating procedure. The action (remote operation of the actuators) must ensure safety.

Example: Emergency Stop or Emergency Shutdown

6.2 Equipment Selection

All SIS components shall either:

- have SIL certification
- be established via prior use
- be type-tested by a Wacker-approved 3rd party

6.2.1 Equipment with SIL Certification

A component may be used in safeguards if the manufacturer declares in writing that the equipment conforms to the requirements of the IEC 61508 series of standards.

If the same components are used redundantly for SIL 3, the equipment software must satisfy the requirements according to SIL 3. Hardware diversity is preferred but at discretion of EI&C engineer.

6.2.2 Type-tested Equipment by a Wacker-approved 3rd party

To accomplish this, the device(s) in question are supplied to an approved testing body who will run them through a stringent testing protocol. This results in a declaration of type-testing, with a statement on what SIL level the device/device combination is suitable for (given HFT stipulations). This will not provide a specific failure rate value, but rather allow for utilization of the values set forth in NAMUR NE130.

Type testing provides evidence that a product meets the requirements of the relevant product standards and is suitable, in principle, for its intended field of application.

6.2.3 Proven-in-use Equipment

The end user can issue a declaration to state safety application suitability for those components used in their plant lacking a SIL certificate (WF ET1775).

Prerequisite:

- Use in large numbers over a long period of time in applicable service and conditions (approx. 100,000 service hours)
- Incident statistics on the failures of this component over the entire period being certified
- Documentation of the component requirements for this use.

6.2.4 Sensor

Field devices should be selected and installed such that errors based on process or environmental conditions are prevented.

Intelligent sensors must be write-protected to prevent uncontrolled modification of parameters.

Any manually operated flaps as process shut-off devices must be mechanically secured against adjustment or sealed in the ”off” position.

6.2.5 Logic

6.2.5.1 Hardware Components

Hardware-based signal processing with fail-safe components, e.g. emergency–shutdown switching devices

6.2.5.2 Safety Control System

Programmable safety control systems must undergo certification. An end user declaration will not suffice.

6.2.6 Final Element

6.2.6.1 Valves

Pneumatic actuator with defined safety position (e.g. spring power) controlled by solenoid valve.

It is essential that the pneumatic connection between the solenoid valve and the drive is not buckled. (e.g. pipework with stainless steel piping).

For control valves, the solenoid valve should generally be positioned between the positioner and the drive.

The valve may also be shared for non-SIS purposes, though the valve suitability for the required switching operations must be considered and a risk assessment performed as necessary.

Leak-tightness of Valves

The internal leak-tightness of valves shall be ensured in accordance with the hazard potential. The hazard potential shall be identified at the Wacker Analysis Report using WF AS1065B, Number 1.7.

If specific requirements relating to the internal leak-tightness of valves are necessary, these shall be recorded using WF AS1075. The leak-tightness may be checked in the following ways:

- If there is a block and bleed system, with a failsafe control system
- When carrying out the function test (during retesting), plausibility tests can be used to check the leak-tightness of the valve (e.g. level check after closing the feed valve during overfill prevention or pressure increase)
- Equipment and control procedures in place (e.g. automatic leak-tightness control), which automatically check the leak-tightness of the valve

  Testing the leak quantity. See *API STD 598* for valve ratings and valve leakage
- Removal of valve and examination in a suitable workshop.

The test record for the repeat testing shall specify which of the above options are used (see for example, SAP ZIEMR). The test interval is specified in WF AS1075.

The test result shall be recorded and the report filed.

The same applies when the open valve guarantees the safe state. In this case it shall be demonstrated that, in the event of a failure, the valve actually opens fully.

Notes on Test Intervals for final actors (different intervals compared to the remaining equipment of the corresponding SIF):

- Valves which always come into contact with “clean” media (e.g. H_2, N_2, air, exhaust gas, steam, deionized water) which have no caulking, caking or corrosive effect: removal and overhaul (i.e. valve rebuild) approximately on a 4-5 year frequency.
- Valves which come into contact with the “product” or are in an extraordinary atmosphere (e.g. high temperatures): removal and overhaul (i.e. valve rebuild) approximately on a 1-3 year frequency.

6.2.6.2 Contactors / Motor Starters (motor, heating etc.)

The utilization category must be observed when specifying the protection. (AC-1 for resistive loads, AC-3 for motors). Reference to IEC 60947-4-1.

SIL 1 Single-channel design using standard switching and minimum 15 % oversizing

SIL 2 Single-channel design using standard switching and minimum 100 % oversizing

SIL 3 Two-channel (redundant) in series design using standard switching and minimum 100 % oversizing

6.2.7 Interface

Passive equipment, for example for explosion isolation, have no functional safety requirement.

Relays and protections for control voltage signals must be designed to be forcibly actuated and the contact load observed as for line protections (see 6.2.6.2).

6.3 Hardware Planning

6.3.1 Design

- Closed-circuit principle
- Fail-safe properties of operating material shall be utilized (e.g. actuator with spring return to the safe position)
- Installation that is as simple and easy to perform as possible
- Non-safety functions combined with safety functions shall be verified for noninterference with the safety functions.
- The preparation and testing of the hardware planning shall be documented using form WF ET1528 or WF 10-0009

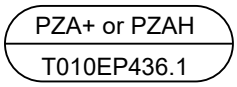
6.3.2 Proper Identification/Labeling

6.3.2.1 Identification in Flow Diagrams

Information with examples can be found in WN 40-1001 WGER.

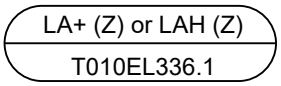
6.3.2.1.1 Safety Instrumented Systems with Z Switching Function

A “Z” shall be used for safety instrumented systems for the switching function as per IEC 62424;
e.g. overfill protection:



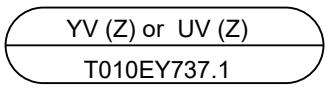
6.3.2.1.2 Safety Instrumented Systems without Z Switching Function

Safety instrumented systems without switching functions (e.g. leak indicators) shall be labeled with “(Z)”;
e.g. leak indicator:



6.3.2.1.3 SIS Actuator

The actuator of a safety instrumented system shall be labeled with “(Z)”;
e.g. ON/OFF valve:



6.3.2.1.4 Further Tagging (not relevant, only WGER)

6.3.2.2 Tags in Circuit Diagrams

In circuit diagrams the devices shall be labeled as a SIS device.
e.g. transducer for gage pressure: V0700T066EP402.1 (PIZA+) or (PIZAH)

6.3.2.3 Tags for Safety Instrumented Systems Equipment

The SIS devices in the field or in a cabinet shall be tagged with “(Z)”.

6.4 Software Planning

If a programmable safety control system is used, the requirements stipulated in the functional description and the “Risk Graph Analysis meeting on the Classification of PCS Equipment” WF AS1075 must be incorporated in the user program.

Observe the following:

- The user software programmers shall be suitably qualified:
  - Training in functional safety
  - System training for the safety system employed
  - Verification of work or completed projects in the field of functional safety
- A software structure shall be installed, which complements the hardware structure, i.e. distribution according to process control functions
- Care shall be taken to create a clear and intelligible user software program, i.e. the program design shall be as simple as possible, comments, etc.
- Use certified or standardized function modules and libraries
- Access to the programming environment shall be protected, for example by password
- For the strict separation of safety instrumented systems and **non** safety-relevant equipment, no basic process control system (BPCS) equipment and process control monitoring functions are implemented in the software function units of the SIS equipment.

The preparation and testing of the user software shall be documented in WF 10-0009.

6.5 SIL calculation

At the Risk Graph Analysis meeting the risk graph is used as the basis for determining the SIL level which reduces the existing hazard potential of the plant and hence the residual risk to a tolerable level.

Choose safety system equipment (such as sensors, controls and actuators) that will help achieve this SIL.

The reliability of a safety instrumented system must be demonstrated by a PFD calculation (**P**robability of **F**ailure on **D**emand) and consideration of the architecture limitations taking into account, for example, the redundancy structure and test intervals.

Even when an SIL certificate or manufacturer's declaration is available for component, if there is no operating experience for the specific application condition, there must be a field-testing phase.

6.5.1 Information Necessary for Calculating the SIL

- Desired SIL: SIL 1, 2 or 3
- Mission time: typ. 15 yrs
  (Period of time between the start-up of a plant and the replacement of a device or its restoration to an as-new condition.)
- Repair, MTTR: typ. 8 h
- Test interval: typ. 1 year (to be coordinated with the equipment’s operator)
- Operating mode: typ. demand or low-demand mode
- Testing mode: typ. offline (offline vs online)

A SIL calculation should contain the following information in addition to the data and documents normally needed for the calculations:

- Information on the coverage of hazardous and unidentified faults in the PTC retest (**P**roof **T**est **C**overage) it is dependent upon the completeness of checking being performed:

Typical proof test coverage while performing the minimum requirements of a proof test (see section 7.3 for full testing requirements):

- Sensor: 90–95 %
- Logic: 99 %
- Actuator: 80–90 %

- Data on the service life of all the components in use (with information and plan of action if the target service life is not achieved)
- Data substantiating the “proven-in-use” qualification; for example, manufacturer’s certificate, production records, etc.
- SIL certificates (certificates are not needed for equipment whose failure rates are included in the database of certified calculation programs).

6.6 Installation

Safety instrumented systems shall be set up according to specifications and plans and commissioned such that they are ready for initial testing.

All components must be precisely installed according to the installation schedules and commissioned in consultation with planning.

Before commissioning, testing for proper installation and correct function of the SIS must be performed and confirmed and recorded using the form WF ET1086.

An installation certificate should be prepared. Use WF ET1305 or WF 10-0029

6.7 Initial Test/Validation

The initial test includes a complete functionality test. Testing under operating conditions (e.g. filling a vessel to test the overfill protection) generally requires the presence of the operator.

The inspection schedule shall be described in detail. The following inspection and testing activities should be included:

- Start-up, standard operations and shutdown of the plant
- Absence of interference with operating equipment and monitoring equipment
- Protective functions in the case of measured values outside of the measurement range
- Proper sequence of the switching function
- Alarms and operating conditions are properly displayed
- Reset function
- Bypassing (if necessary)
  - Bypasses must be reported
  - A bypass procedure must be defined in operational documentation
  - details see 7.4
- Diagnostic equipment must function as stipulated
- Response in the event of loss of auxiliary power
  - After auxiliary power has been restored, manual approval is required so that the safety instrumented system can revert to its proper operational status.

Special care must be taken that the required circuit has actually been triggered by the SIS, as in many cases the safety-relevant signals are also activated in the PCS and the same switching function is triggered in the PCS. This generally creates the need to temporarily bypass relevant BPCS interlocks.

The initial test shall be recorded and kept for the life of the loop and documented via WF ET1526 or WF 10-0010.

6.8 Final Documentation

The planning, installation and commissioning of a safety instrumented system shall be documented. This shall be available upon completion of commissioning and prior to handover for operation. Depending on the scope of the protective loop this can cover:

- Flow diagram (as per IEC 62424)
- Specifications and records of results from the Risk Graph Analysis meeting (for example, WF AS1075)
- Process-control location sheets
- Computation documents
- Function-specific description (operating instructions)
- Wiring diagrams
- Logic diagrams or functionality plans
- Test instructions
- Proof test checklist
- If necessary, programs of safety-relevant, programmable control systems
- Data sheets from the manufacturer of the operating material
- Test report
- Hazard assessment
- Any test certificate required shall also be included in the documentation.

See WN 08-26-01 Bbl 10 and A-WN 08-10-02.

7 In Operation

The objective is to operate and maintain a safety instrumented system so as to preserve the necessary functional safety.

7.1 Training/Instruction

7.1.1 Operating Personnel

The operating personnel must be instructed in the function and operation of the SIS in their area:

- Understanding of the function (switching points and their effect)
- Information on hazards against which the SIS protects
- Effect of a bypass (WF 10-0100)
- Response to PCS messages.

7.1.2 Maintenance Staff

Maintenance staff must be instructed in the SIS function:

- Test procedure
- Understanding of the function (switching points and their effect)
- Information on hazards against which the SIS protects
- Effect of a bypass (WF 10-0100)
  Response to diagnostic messages (e.g. displays for safety control systems and transducers).

7.2 Repair

A SIS must be maintained so that the required functional safety is ensured.

- Repair work must be carried out only by qualified personnel who have been properly trained
- Devices may only be repaired by qualified personnel who have been properly trained or the manufacturer
- Equipment should generally be replaced 1:1. If this is not possible it is considered a modification (see 7.5)

A maintenance order shall be opened in SAP with maintenance instructions for each repair to a safety instrumented system. The safety circuit shall be tested and the root cause completed in full for every component with a fault.

The result of the fault analysis shall be entered in the feedback text for the SAP order.

7.3 Prooftest

Regular retests must be performed based on written instructions to detect hidden faults. Tests shall be written in adherence with the national functional safety authority.

Content of the instructions:

- Description of the correct functionality of each sensor and actuator
- Description of the logical link or limit values
- Description of the alarms and displays
- Description of retest performance

Any discrepancies found during testing shall be noted and verified with area EI&C engineer for correction.

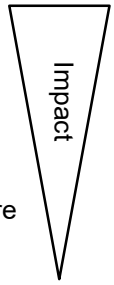
The retest is processed via scheduled maintenance orders with maintenance instructions in SAP.

(see IEC 61511-1, Section 16)

Requirements on a proof test:

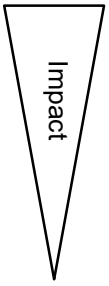
Pressure / level / flow / temperature transmitter

- Check response to both under-range (< 4mA) and over-range (> 20mA)
- Check zero, span, trip and trim against a traceable standard
- Check HART diagnostics and ramp the electronics through the 4-20mA range
- Confirm the logic solver is reading values properly
- Visual inspection, check for plugging, and that housing is within specified temperature
- Checking response in situ



Shutoff valve

- Stroke valve closed
- Test seat leakage against the specification
- Check timing against the specification
- Checking response in situ under actual process conditions (e.g., flow and pressure)
- Check repeatability
- Check hysteresis, smoothness of operation, and position feedback
- Record as-found condition



For detailed determination of the Proof Test Coverage, see NAMUR NA106.

7.4 Bypassing Safety Instrumented Systems (de- and re-commissioning)

A SIS can be bypassed if required if certain alternative measures are taken and said bypass is temporary.

When bypassing safety instrumented systems, the following points should be documented:

- Statement of the consequence mitigated by the interlock in question
- Reason for bypass and definition of alternative measures
- Written confirmation of the alternative measures provided
- Duration of the bypass
- Confirmation of the bypassing of the SIS
- Approval for re-commissioning
- Re-commissioning and function test
- Handover to shift leader
- Archive of the original document for the life of the loop
- Additional site-specific requirements may apply

Documentation shall be performed using WF10-0100.

Bypassing for Plant Operation

Individual passwords, chip cards or keys shall be used to bypass SIS, for example to start-up or clean the plant. This should not overlap with other authorization groups.

The users must be given specific instructions by EI&C Engineer Plant and Production Manager.

7.5 Modification

Changes to the SIS shall follow the plant site's management of change procedure.

Modifying safeguards bears the risk of implementing systematic faults, which prevent or impair the desired operation of this or another safeguard. For this reason, it must be ensured that all modifications are carried out using the same systems and care that were used when planning and installing the safety system. The involved and responsible operators and maintenance staff must be advised of the modification and if necessary, trained in accordance with the modification. As a rule, modifications to safety systems require new consideration, the type and scope of which depends on the modifications (see G-WN 08-26-01 WGER Bbl 12).

Examples:

- The risk has changed (for example, new feedstocks or process conditions)
- The protective function (functional plan) has changed
- The process conditions affecting the reliability of the safety instrumented system have changed (for example, the sensors or actuators are no longer suitable)
- The process engineering has changed (for example, because the equipment has changed)
- Legal conditions have changed. For example, new environmental legislation requires that the safety valve be replaced to comply with laws governing permissible emissions.
- Changes to limit values.

7.6 Grandfathering

For existing SIS designed and constructed in accordance with code, standards, or practices prior to the issue of this standard the user shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.

WCC/WPNA: ISA-TR84.00.04-2015, PART 1

7.6.1 Modernization or Repair of an existing Safety Instrumented System (not relevant, only WGER)

7.7 Useful Lifetime

The useful lifetime is a period in which the devices have a constant probability of failures according to the manufacturer. After this time, a device must not be operated in a safety instrumented function (unless proper extension assessment is performed). However, there is nothing to prevent the removed devices from continuing to be operated in the BPCS.

Devices in SIS should be able to be operated until they have to be replaced due to increased failure rates or for reasons of wear and tear, as the safety reliability is no longer sufficiently ensured. The point in time for this is essentially application-dependent and subject to systematic influences.

In SIL certificates and, in some cases, in operating or instruction manuals, manufacturers specify a maximum useful lifetime or an "expiration date" for the failure rates of their devices. This establishes a period in which the devices have a constant probability of failure according to the manufacturer. Certificates recommend that devices be replaced after a certain number of years. Under certain circumstances, variations are possible due to previous years of storage or extensions by proving that the safety parameters have not changed.

As a reference, IEC 61508.2: 2011, Chapter 7.4.9.5, Note 3 is often quoted in SIL certificates a useful lifetime of 8 to 12 years.

7.7.1 Extend the Useful Lifetime

To extend the useful lifetime of devices in a SIF, practical measures of the manufacturer and the operator are specified in IEC 61508-02:2011 and in AK-Praxis NAMUR AK4.5 Functional Safety.

As long as no abnormalities on devices are identified and measures according to 7.7.1.1.1 and/or 7.7.1.1.2 have been taken, no restrictions to the useful service life of devices used in SIS are to be expected. Based on broad operational experience, and from a practical point of view, there is nothing to prevent the use of such a device in a SIS be-yond the time of the stated "expiration date".

In case of abnormalities that are traced back to operation itself or specific operating conditions of the devices under consideration, these abnormalities must be analyzed and appropriate measures maintenance (for example, replace electronic devices such as pressure transmitters or maintain mechanical components such as valves) must be initiated.

7.7.1.1 Measures

Preparation of an assessment based on the required measures from IEC 61508-02:2011 to the manufacturer and the operator of devices in SIS following the AK-Praxis of the NAMUR working group AK4.5.

The assessment shall specify the purpose, scope of validity and measures taken by the manufacturer and the operator. For documentation purposes, the WF ET3350 is available.

7.7.1.1.1 Measures taken by the manufacturer

The following measures should be investigated in cooperation with the equipment vendor:

- Appropriate device design (e.g. avoid usage of age-critical components).
- Active error behavior, i.e. errors should be detectable, or the device should fail safe.
- Device-specific maintenance recommendations.[1]
- The device was developed according to IEC 61508.
- Detailed description in SIL-certificates or safety manuals enabling extension of useful lifetime. (not absolutely). [2]
- If the above measures are not possible or only possible to a limited extent, then the manufacturer should inform the customer of components that limit the useful lifetime.

7.7.1.1.2 Measures taken by the end user

Possible examples of operator actions to extend and monitor the useful lifetime:

- Use of devices based on prior use over a period of 10.000h including application-specific maintenance measures.
- Reduction of critical operating conditions, e.g. by protection against environmental influences [2] (validate against AS-1075, Materials of Construction in contact with product).
- Consideration of the process conditions e.g. abrasion, vibration, corrosion e.g. based on plant-specific empirical values to determine suitable maintenance measures.
- Design of the safety function in such a way that faults lead to a safe state (e.g. closed-circuit current principle, fail-safe properties).
- Validation of device reliability by fault data acquisition, e.g. by applying NAMUR.smart cause determination in case of faults, evaluation and derivation of measures. The evaluation of the fault data acquisition is carried out by EN-ED-PC Competence Centre Functional Safety. Operators are actively informed in the event of anomalies.
- Monitor components that are subject to wear or have been designed by the manufacturer as components limiting the service life and replace them as a preventive measure, e.g. during plant shutdowns, regular proof tests (e.g. seals, final control element, diaphragm ...).
- Use of automatic diagnostics. [3]
- Use of the same type of device in SIS and BPCS service as additional evidence of detectable failures outside of useful life.
- Use of maintenance experience, exchange of experience between end user. [3]

8 Auditing

Audits of functional safety shall be performed at periodic intervals.

Each audit is conducted by the individual business divisions; this relates both to the organization and the mutual auditing by EI&C production engineers.

[1] if necessary

[2] not absolutely

(The checklist for auditing functional safety (ET1871) is stored in Docunize.)

The members of the audit team are the Auditor and the I&C Engineer Plant.

Normative References

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

A 07-04-04	Safety of Plants and Processes – Design and Changes
A 08-01-09	Safeguarding Systems in Enhanced Security Networks
A 08-01-15	OT Security
A-WN 08-10-02 ADR	Technical Documentation for Plant
A-WN 08-10-02 CHA	Technical Documentation for Plant
ANSI/ISA-84.00.01	Functional Safety: Safety Instrumented Systems for the Process Industry Sector
API STD 598	Valve Inspection and Testing
IEC 61508-02	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
IEC62424	Representation of process control engineering - Request in P&I diagrams and data exchange between P&ID tools and PCE-CAE tools
IEC 61511	Functional safety – Safety instrumented systems for the process industry sector
ISA-TR84.00.04, Part1	Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)
NAMUR NE 93	Verification of the safety-related reliability of SIS
NAMUR NE 106	Test intervals of safety instrumented systems
AK-Praxis NAMUR WG4.5	Useful Lifetime of Devices - Handling of Manufacturer Data
WF AS1065BE	WACKER Analysis Report
WF AS1075	Safety Instrumented System Classification Analysis
WF AS1460	Plausibility Check, Equipment Loads, Basic Safety Plans
WF ET1030	List of Quality-, Environment- Safety and Energy Management System Relevant I&C Devices for Process Management
WF ET1086	Pre-Commissioning Testing Certificate of Safety Integrated Functions
WF ET1526	Safety Instrumented Function initial testing report
WF ET1775	Prior Use Declaration for SIF
WF ET1871	Checklist Functional Safety Audit
WF ET3350	Assessment for extending the useful life of devices in Safety Instrumented Systems
WF 10-0003	Log of Functional Safety Management
WF 10-0009	SIF-Release for Construction
WF 10-0010	Safety Instrumented Function(SIF) Report on Initial Inspection
WF 10-0029	EIC Installation Verification
WF 10-0100	Safety Interlock Bypass-24 Hour Permit
WN 27-1001	Labeling EI&C Devices
WN 40-1001	Labeling and Depiction of Process Control Engineering in P&I Diagrams

Changes

The following changes have been made with respect to version 2019-011:

- Complete revision of chapter 7.7 Useful Lifetime with a scope of extending.