


KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions	 Engineering Solutions www.klmtechgroup.com	Page : 1 of 74
		Rev: 01
		October 2011
KLM Technology Group P. O. Box 281 Bandar Johor Bahru, 80000 Johor Bahru, Johor, West Malaysia	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Co Author: Rev 01 Aprilia Jaya
		Editor / Author Karl Kolmetz

TABLE OF CONTENT

INTRODUCTION

Scope	3
General Design Considerations	4

DEFINITIONS

25

THEORY OF THE DESIGN

27

Relief system	30
Pressure Relief Devices	31
A. Heat Exchanger Split Tube and Tube Leakage	41
B. Pumps and Downstream Equipment	43
C. Compressor and Downstream Equipment	45
D. Fired Heaters (Furnace) and Boilers	47
E. Pressurized Storage (Offsites)	50

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 2 of 74
		Rev: 01
		October 2011

F. Piping	51
G. Pressure Relief Valve for Liquid Thermal Expansion	52

High Integrity Protection Systems (HIPS)	54
---	-----------

REFERENCES	75
-------------------	-----------

LIST OF TABLE

Table 1: SIL Level and Related Measure	9
Table 2: Possible (simplified) format for Safety Requirement Specification	22
Table 3: Comparisons of conventional, bellow and pilot pressure relief valve	38

LIST OF FIGURE

Figure 1: Safety layers	7
Figure 2: Example SIL 1 SIF (a) and High Reliability SIL 1 SIF (b).	9
Figure 3: Example SIL 2 SIF (a) and High Reliability SIL 2 SIF (b).	10
Figure 4: Example SIL 3 SIF (a) and High Reliability SIL 3 SIF (b).	11
Figure 5: Flowchart – SIL development and allocation	12
Figure 6: Example of allocation of safety function to protection layers for overpressure protection	13
Figure 7: Basic SIS layout	16
Figure 8: The relationship between SIS, SIF and SIL	20

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 3 of 74
		Rev: 01
		October 2011

Figure 9: SIS safety life-cycle phases	23
Figure 10: Conventional pressure relief valve	32
Figure 11: Balanced pressure relief valve	33
Figure 12: Pilot Operated Relief Valve	36
Figure 13: Forward-Acting Solid Metal Rupture Disk Assembly	37
Figure 14: Heat exchanger with pressure relief valve to protect form overpressure	42
Figure 15: Piston pumps with pressure compensation	44
Figure 16: Gas compressor	46
Figure 17: Fire heaters	49
Figure 18: Pressure storage tank	51
Figure 19: Two-out-of-three Voting	55
Figure 20: Field Input Devices	56
Figure 21: Installation Illustration for Final elements Showing 1oo2 Valves and 1oo2 Solenoids	57
Picture 22: HIPS Schematic Diagram	61
Figure 23: Simplified Decision Tree	62

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 4 of 74
		Rev: 01
		October 2011

INTRODUCTION

Scope

This design guideline covers the process safety issues in overpressure relieving system including chemical, petrochemical, and hydrocarbon processing facilities. It helps engineers understand the basic design of process safety and increase their knowledge in prevention and restrain the accidents caused by overpressure that might happen.

All the important parameters used in this guideline are well explained in the definition section which helps the reader understand the meaning of the parameters and the terms used.

The design consideration is discuss about method of safety layers like Safety Instrumented System (SIS), Safety Integrity Level (SIL), Safety Instrumented Function (SIF), High Integrity Protective System (HIPS), and Pressure Relief Valve (PRV) in some equipment such flare, furnaces, pressure storage, piping and pump.

In an increasingly multi-disciplinary engineering environment, and in the face of ever increasing system complexity, there is a growing need for all engineers and technicians involved in process engineering to be aware of the implications of designing and operating safety-related systems.

This guideline includes knowledge of the relevant safety standards. Safety Instrumented Systems play a vital role in providing the protective layer functionality in many industrial process and automation systems. This guideline describes the purpose of process safety-related systems in general and highlights best engineering practice in the design and implementation of typical safety instrumented systems, underpinned by the relevant standards.

The design of safety in overpressure relieving system may be influenced by factors, including process requirements, environmental regulations, location, process materials involved, user friendly and economic.

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 5 of 74
		Rev: 01
		October 2011

General Design Considerations

Nothing is more important than safety to the process control industries. High temperature and pressure, flammable and toxic materials are just some of the issues faced on a daily basis. Reliability is a key component of safety; the more reliable the device, the safer the critical process. Compliance with the industrial standards, ANSI/ISA 84.01-1996 and IEC 61508, requires four essential elements:

1. Identification of safety functions required for safe shutdown;
2. Assignment of a safety integrity level (SIL) for each safety function;
3. Use of the safety lifecycle for the SIS design; and
4. Verification of the SIL achieved for each safety function.

Safety Methods employed to protect against or mitigate harm/damage to personnel, plant and the environment, and reduce risk include:

1. Changing the process or engineering design
2. Increasing mechanical integrity of the system
3. Improving the Basic Process Control System (BPCS)
4. Developing detailed training and operational procedures
5. Increasing the frequency of testing of critical system components
6. Using a safety Instrumented System (SIS)
7. Installing mitigating equipment

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 6 of 74
		Rev: 01
		October 2011

Simplified steps in developing the Safety-related System

1. Formulate the conceptual design of the process and define the overall scope
2. Identify process hazards and risks via a hazard analysis and risk assessment
3. Identity non-SIS layers of protection
4. Determine the need for additional protection i.e. a SIS

Where a SIS is identified as being required...

1. Determine the target SIL (using qualitative and/or quantitative methods)
2. Develop safety requirement specification (SRS)
3. Develop SIS conceptual designs to meet SRS
4. Develop detailed SIS design
5. Install the SIS
6. Perform Commissioning and pre-startup testing
7. Develop operation and maintenance procedures
8. Conduct pre-startup safety review
9. Carry out operation and maintenance of SIS
10. Record and re-assess any modification to SIS
11. Carry out decommissioning procedures at the end of the life of the SIS.

No single safety measure can eliminate risk and protect a plant and its personnel against harm or mitigate the spread of harm if a hazardous incident occurs. For this reason, safety exists in protective layers: a sequence of mechanical devices, process controls, shutdown systems and external response measures which prevent or mitigate a hazardous event.

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 7 of 74
		Rev: 01
		October 2011

If one protection layer fails, successive layers will be available to take the process to a safe state. If one of the protection layers is a safety instrumented function (SIF), the risk reduction allocated to it determines its safety integrity level (SIL). As the number of protection layers and their reliabilities increase, the safety of the process increases.

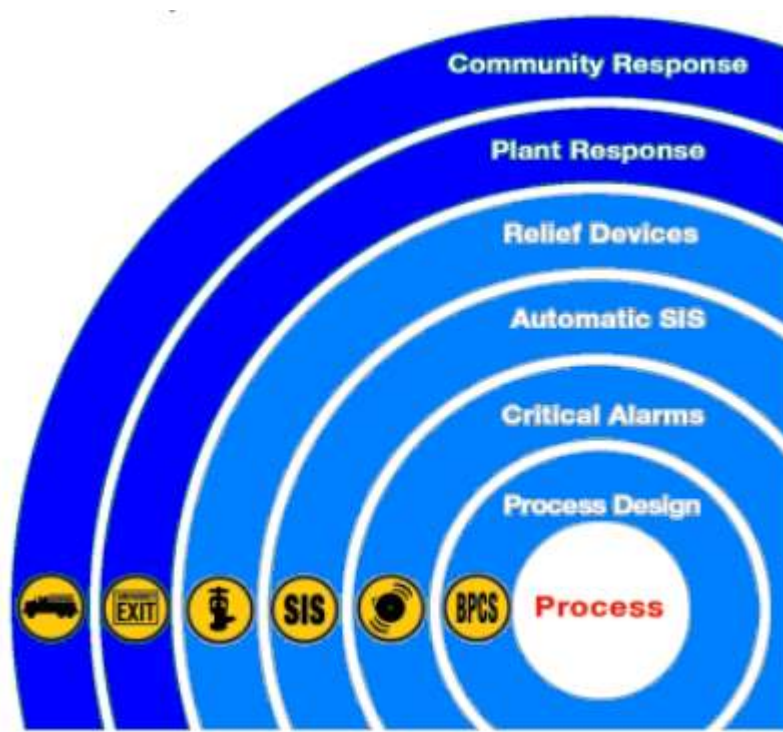


Figure 1: Safety layers

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 8 of 74
		Rev: 01
		October 2011

Safety Integrity Level (SIL)

Safety Integrity Level (SIL) is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. Safety Integrity Level is a way to indicate the tolerable failure rate of a particular safety function. Standards require the assignment of a target SIL for any new or retrofitted Safety Instrumented Function (SIF) within the Safety instrumented system (SIS).

The assignment of the target SIL is a decision requiring the extension of the Hazards Analysis. The SIL assignment is based on the amount of risk reduction that is necessary to maintain the risk at an acceptable level. All of the SIS design, operation and maintenance choices must then be verified against the target SIL. This ensures that the SIS can mitigate the assigned process risk. It is at the heart of acceptable SIS design and includes the following factors:

1. Device integrity
2. Diagnostics
3. Systematic and common cause failures
4. Testing
5. Operation
6. Maintenance

SIL is defined as four discrete levels of safety (1-4). Each level represents an order of magnitude of risk reduction. The higher SIL level, the greater the impact of a failure and the lower the failure rate that is acceptable. Standards require the assignment of a target SIL for any new or retrofitted SIF within the SIS.

The claimed SIL is limited by the calculated Probability of Failure on Demand (PFD) and Risk Reduction Factor (RRF). When the hazards identification and risk assessment phase concludes that a SIS is required, the level of risk reduction afforded by the SIS and the target SIL have to be assigned.

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 9 of 74
		Rev: 01
		October 2011

Various methodologies are used for assignment of target SILs. The determination must involve people with the relevant expertise and experience. Methodologies used for determining SIL include Simplified Calculations, Fault Tree Analysis, Layer of Protection Analysis (LOPA) and Markov Analysis.

There are several problems inherent in the use of Safety Integrity Levels. These can be summarized as follows.

- Poor harmonization of definition across the different standards bodies which utilize SIL
- Process-oriented metrics for derivation of SIL
- Estimation of SIL based on reliability estimates
- System complexity, particularly in software systems, making SIL estimation difficult to impossible

Table 1: SIL Level and Related Measure

SIL	Availability	Range of Average PFD	Range of RRF	Qualitative Consequence
4	>99.99%	10^{-5} to 10^{-4}	100,000 to 10,000	Potential for fatalities in the community
3	99.9%	10^{-4} to 10^{-3}	10,000 to 1,000	Potential for multiple on-site fatalities
2	99 to 99.9%	10^{-3} to 10^{-2}	1,000 to 100	Potential for major on-site injuries or a fatality
1	90 to 99%	10^{-2} to 10^{-1}	100 to 10	Potential for minor on-site injuries

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 10 of 74
		Rev: 01
		October 2011

SIL 1

In a simple independent SIL 1 SIF (figure 2a), a single sensor is used to detect the pressure. The logic solver de-energizes a solenoid operated valve (SOV) removing air from the valve actuator, allowing the valve to go to its specified failed closed (FC) position. A higher reliability (low spurious trip rate) SIL 1 design (Figure 2b) by implementing 2oo2 voting for the sensor and SOV. 2oo2 voting SOVs have been proven through decades of use to achieve high integrity and reliability when instrument air quality is good and the SOVs are properly maintained.

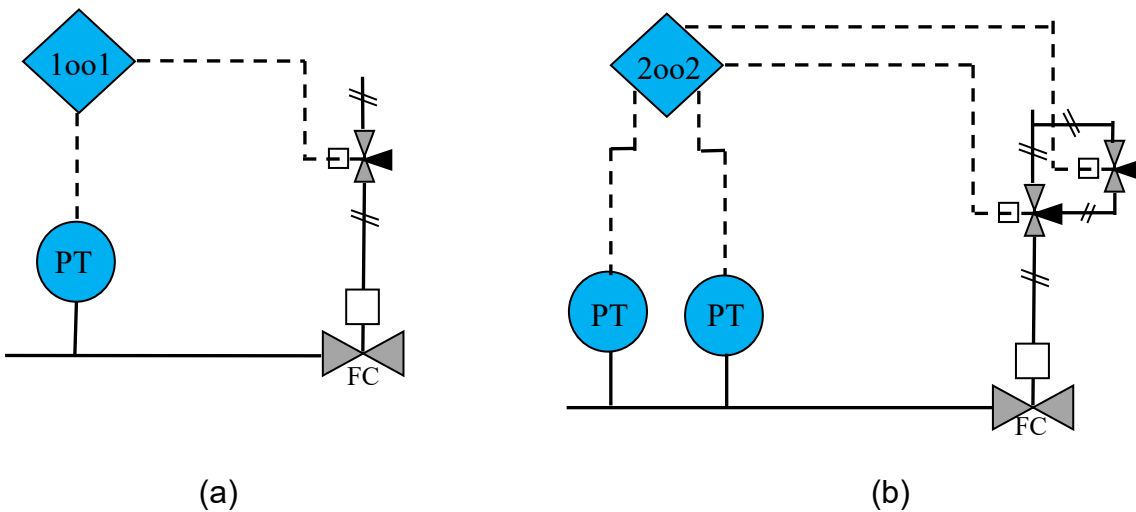


Figure 2: Example SIL 1 SIF (a) and High Reliability SIL 1 SIF (b).

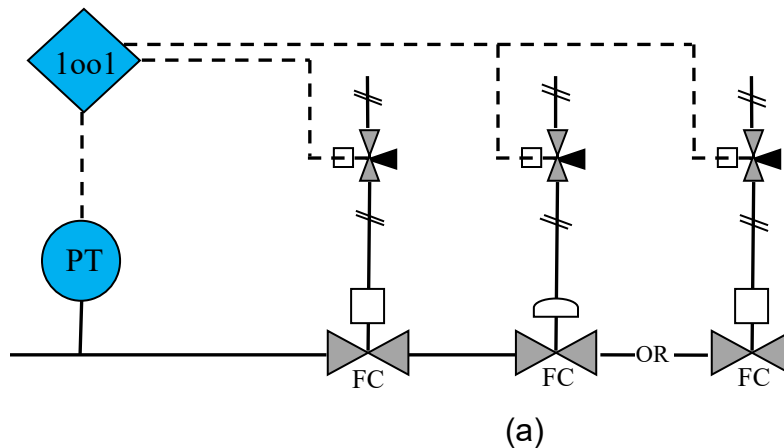
These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design	Page 11 of 74
	SAFETY IN OVERPRESSURE RELIEVING SYSTEMS	Rev: 01
	(ENGINEERING DESIGN GUIDELINES)	October 2011

SIL 2

Simplex pressure transmitters can be used in SIL 2, given a reasonable test interval and the use of good quality equipment. Figure 3a provides an SIL 2 SIF with an option to use an additional block valve or to share the control valve as a second means of process isolation. The control valve cannot be used, unless it fully meets the SIS design basis (e.g., integrity, independence, leak tightness, response time, etc.). Figure 3b provides a higher reliability SIL 2 design using 2oo2 voting sensors and SOVs.



These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 12 of 74
		Rev: 01
		October 2011

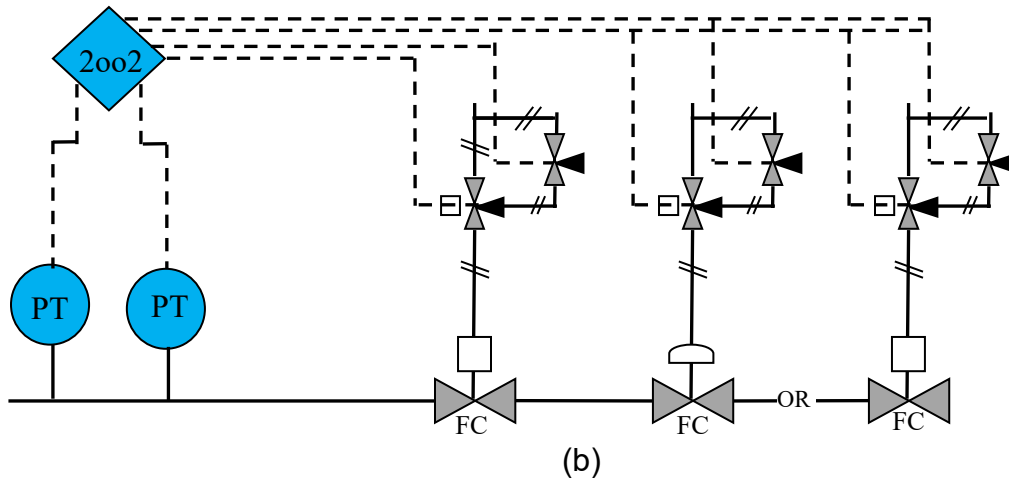


Figure 3: Example SIL 2 SIF (a) and High Reliability SIL 2 SIF (b).

SIL 3

SIL 3 is the highest level of performance typically expected from an SIF in the process industry. For SIL 3, systematic errors must be minimized through the use of fault tolerance. Fault tolerance must be provided in the sensors, logic solver, final elements, and any required support systems. Figure 4a provides an SIL 3 architecture that is fault tolerant against dangerous failures using 1oo2 voting sensors and dedicated block valves. Figure 4b provides a high reliability SIL 3 architecture using 2oo3 voting sensors and 2oo2 SOVs.

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

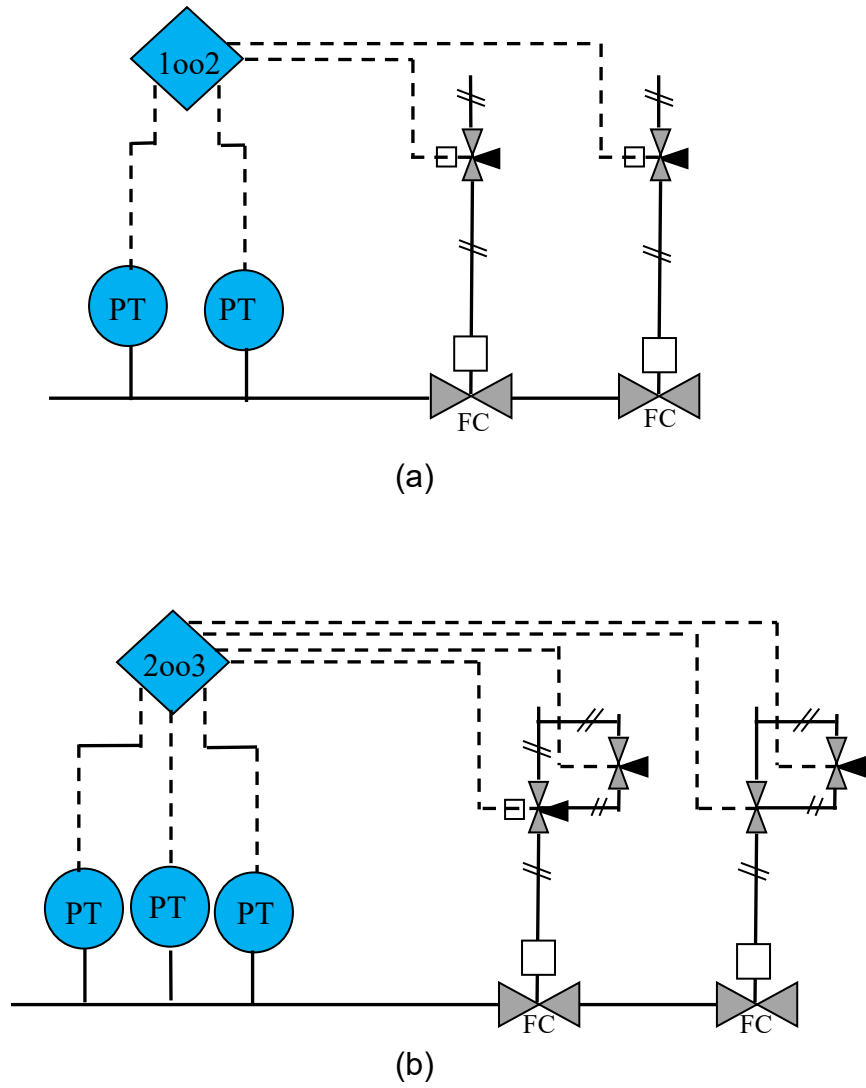
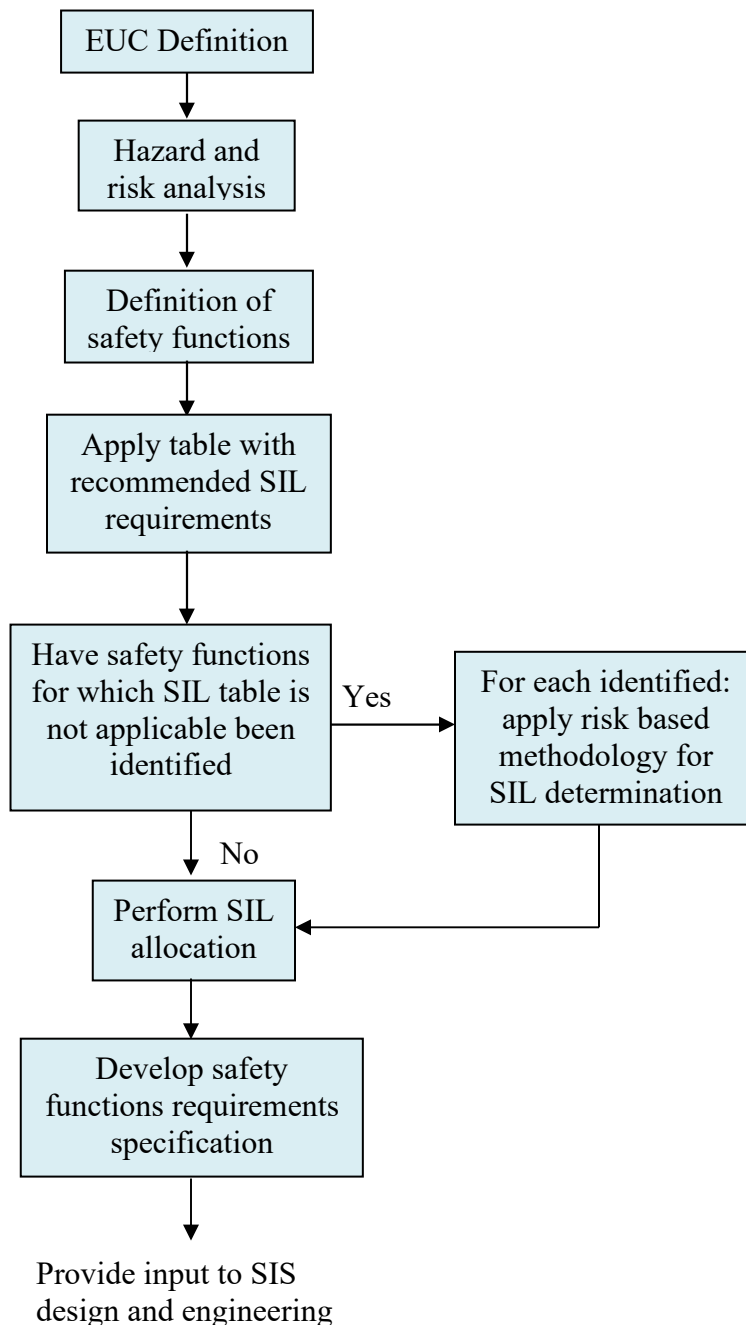


Figure 4: Example SIL 3 SIF (a) and High Reliability SIL 3 SIF (b).

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design	Page 14 of 74
	SAFETY IN OVERPRESSURE RELIEVING SYSTEMS	Rev: 01
	(ENGINEERING DESIGN GUIDELINES)	October 2011



These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 15 of 74
		Rev: 01
		October 2011

Figure 5: Flowchart – SIL development and allocation

If the required SIL cannot be achieved with the initial design, some options are:

1. More frequent proof testing
2. Add redundancy (i.e., initiating device, control system, final element)
3. Install “smarter” device (i.e., HART smart transmitter or transmitter vs. switch or relay, smart control valve with diagnostics and feedback and position indication vs. basic control valve)
4. Add protection layers (independent)

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

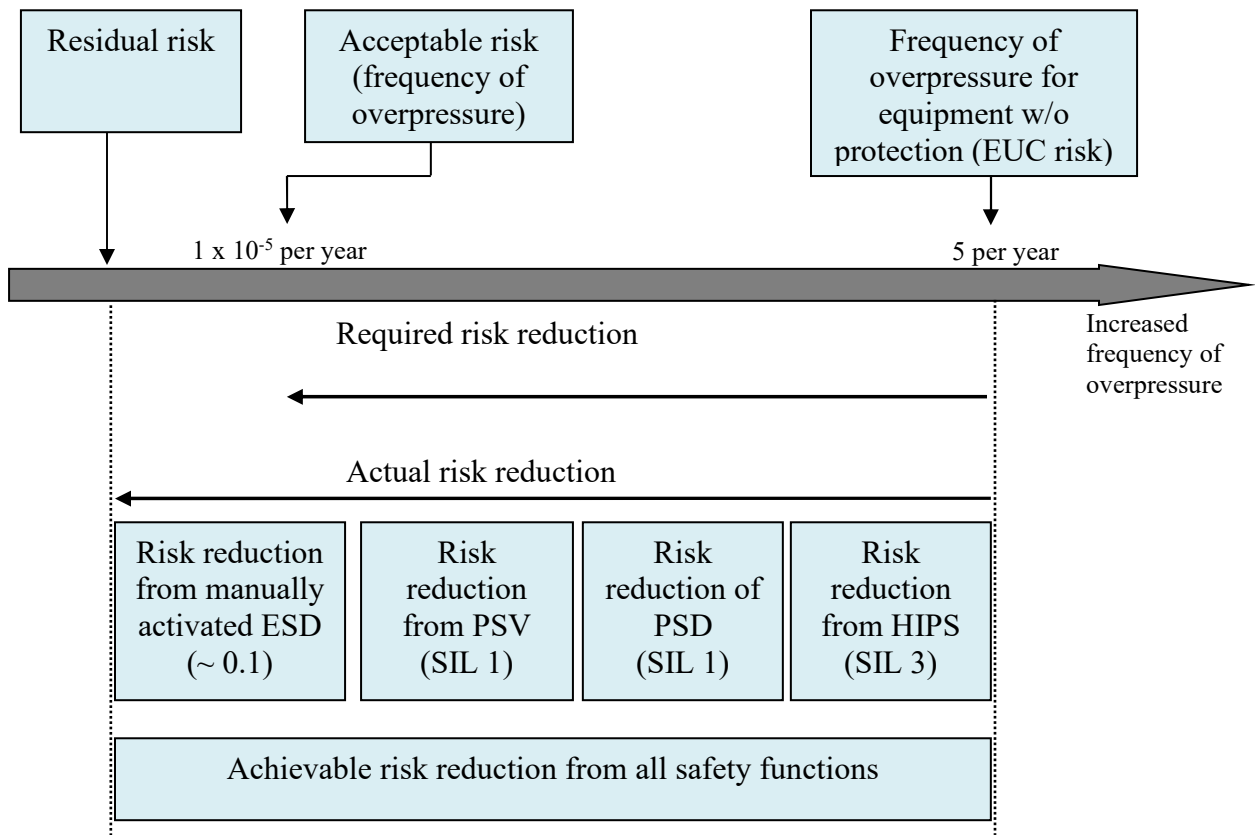


Figure 6: Example of allocation of safety function to protection layers for overpressure protection

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 17 of 74
		Rev: 01
		October 2011

The SIL is affected by the following:

1. Device integrity determined by documented and supportable failure rates;
2. Redundancy and voting using multiple devices to ensure fault tolerance;
3. Functional testing at specific intervals to determine that the device can achieve the fail safe condition;
4. Diagnostic coverage using automatic or on-line methods to detect device failure;
5. Other common causes including those related to the device, design, systematic faults, installation, and human error.

Safety Instrumented System (SIS)

A safety instrumented system (SIS) is a system comprising sensors, logic solvers and actuators for the purposes of taking a process to a safe state when normal predetermined set points are exceeded, or safe operating conditions are violated such as set points for pressure, temperature, level, etc. in other words, they trip the process when they out of limit condition. SIS are also called emergency shutdown (ESD) systems, safety shutdown (SSD) systems, and safety interlock systems.

The scope of a SIS encompasses all instrumentation and controls that are responsible for bringing a process to a safe state in the event of an unacceptable deviation or failure. SIS provides a layer of protection to help protect the process against accidents. The basic SIS layout comprises:

1. Sensor(s) for signal input and power
2. Input signal interfacing and processing
3. Logic solver with associated communications and power. The safety firmware constitutes the basic logic solver equipment from which the safety applications are built:
 - a. Framework, racks, cabinets;
 - b. Processor/memory boards;
 - c. Communication boards;

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 18 of 74
		Rev: 01
		October 2011

- d. I/O boards;
- e. Termination units;
- f. Power supplies;
- g. System software;
- h. Application software libraries;
- i. Application programming tools;
- j. Communication protocols;
- k. Human/system interfaces.

When designing the logic solver hardware, the following should be taken into account:

- a. A safety user design manual should exist which describes how non-certified equipment shall be used in safety critical applications. For certified equipment this is normally available as part of the certification;
- b. Appropriate designated architecture must be selected for the central processing unit. As a minimum, the selected architecture shall meet the highest SIL level of the relevant safety functions;
- c. If possible, the architecture of the I/O and interface modules should be selected individually for each safety function;
- d. When working with certified equipment, the difference between certified components and components certified for non-interference should be noted:
- e. Certified components: for use in safety critical functions;
- f. Components certified for non-interference: may be used but not in safety critical functions.
- g. For non-certified equipment PFD calculations shall be performed to show that the contribution from the logic solver is within acceptable limits;
- h. For certified equipment the maximum contribution to the PFD figure is normally part of the certification report and is therefore available as pre-calculated and verified parameters;

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 19 of 74
		Rev: 01
		October 2011

- i. For non-certified equipment the maximum time in degraded mode should be calculated;
 - j. For certified equipment the maximum time in degraded mode is normally part of the certification report and is therefore available as pre-calculated and verified parameters.
4. Output signal processing, interfacing and power
 5. Actuators and valve(s) or switching devices to provide the final control element function.

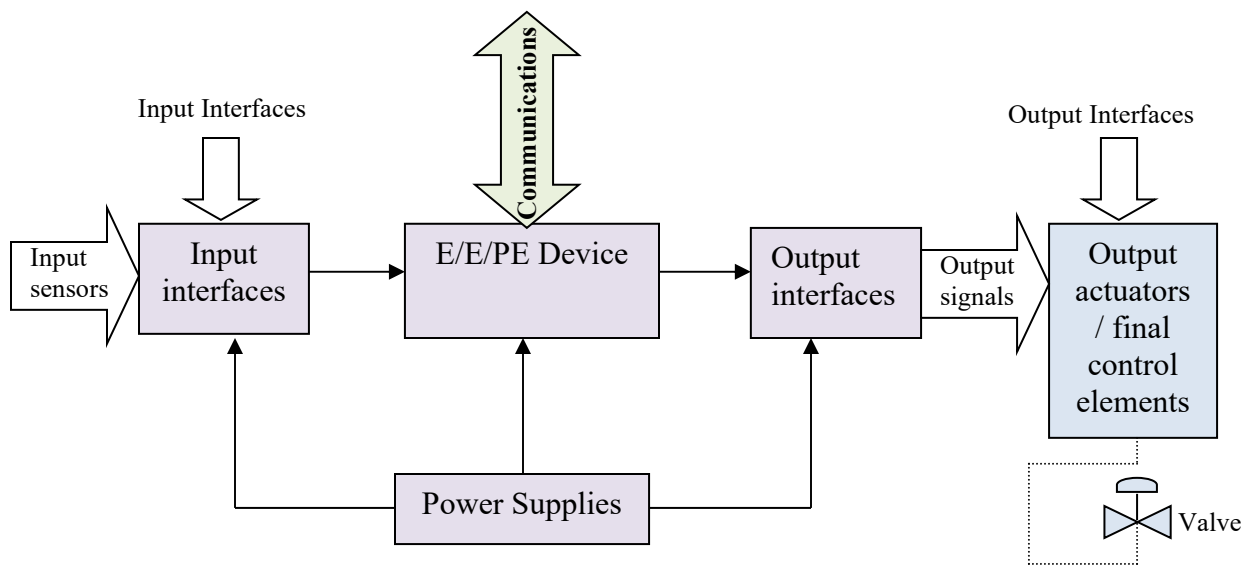


Figure 7: Basic SIS layout

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 20 of 74
		Rev: 01
		October 2011

Safety Instrumented System (SIS) is an alternative for conventional relief device to eliminate the source of overpressure, thereby making relief capacity unnecessary. They are typically used where the provision of relief capacity is inappropriate. This is typically (but not always) due to one of the following factors:

1. The fluid which would be discharged via a relieving device is toxic or extremely hazardous
2. Realistic evaluation of the overpressure scenario and quantification of the relief load is difficult or impossible (e.g. explosive reaction)
3. The cost of providing the necessary capacity in the disposal system or the relief valves is prohibitive.
4. The vessel is not exclusively in air, water, or steam service.
5. The user must ensure the MAWP of the vessel is higher than the highest pressure that can reasonably be achieved by the system.
6. A quantitative or qualitative risk analysis of the proposed system must be made addressing: credible overpressure scenarios, demonstrating the proposed system is independent of the potential causes for overpressure; is as reliable as the pressure relief device it replaces; and is capable of completely mitigating the overpressure event.

Lifecycle of SIS is based on IEC 61511. IEC 61511 covers a wide range of chemical process operations. Due to its broad scope, the standard has many general requirements addressing the complete lifecycle of the SIS, starting with the identification of SIS requirements in the risk assessment and ending when the SIS is decommissioned. While there are many different ways of representing the lifecycle, a simple four step approach can be followed:

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 21 of 74
		Rev: 01
		October 2011

1. Define a risk-management strategy - establish a facility management system for how SISs are identified, designed, inspected, maintained, tested, and operated to achieve safe operation and perform a hazard and risk analysis to identify where SISs are needed and their target SIL
2. Implement the strategy - develop a design basis to achieve the target SIL and execute the detailed design to meet the requirements. The SIS design basis should address the following:
 - a. Detection of and response to potential hazardous events
 - b. Selection of equipment based on prior history
 - c. Fault detection, such as diagnostics and proof testing
 - d. Fault tolerance against dangerous failures
 - e. Procedures for maintenance and test, including the use of bypasses
 - f. Operation and maintenance procedures required when SIS equipment is out of service
 - g. Emergency shutdown capability if the SIS fails to take action as expected
 - h. Start-up and shutdown of the process equipment
3. Validate, start-up, operate and maintain the strategy - implement the SIS following the design basis and detailed design documentation and define what is required of operation and maintenance personnel to sustain the SIL
4. Manage changes to the strategy - ensure the SIS meets the target SIL by monitoring operation, inspection, test, and maintenance records and making changes as necessary to improve its performance

Validation planning of the SIS should define all activities required for validation. The following items shall be included:

1. The validation activities, including validation of the SIS with respect to the safety requirements specification and implementation and resolution of resulting recommendations;
2. Validation of all relevant modes of operation of the process and its associated equipment including:

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 22 of 74
		Rev: 01
		October 2011

- a. Preparation for use including setting and adjustment;
 - b. Start-up, teach, automatic, manual, semi-automatic and steady state of operation;
 - c. Re-setting, shut down and maintenance;
 - d. Reasonably foreseeable abnormal conditions.
3. The procedures, measures and techniques to be used for validation;
 4. Reference to information against which the validation shall be carried out (e.g., cause and effect chart, system control diagrams).
 5. When the activities shall take place;
 6. The persons, departments and organizations responsible for the activities and levels of independence for validation activities;

SIS safety validation shall mean all necessary activities to validate that the installed and mechanical completed SIS and its associated instrumented functions, meets the requirements as stated in the Safety Requirement Specification (SRS). The validation of the safety instrumented system and its associated safety instrumented functions shall be carried out in accordance with the safety instrumented system validation planning. Validation activities shall as a minimum confirm that:

1. The safety instrumented system performs under normal and abnormal operating modes (e.g., start-up, shutdown, etc.) as identified in the Safety Requirement Specification;
2. Adverse interaction of the basic process control system and other connected systems do not affect the proper operation of the safety instrumented system;
3. The safety instrumented system properly communicates (where required) with the basic process control system or any other system or network;
4. Sensors, logic solver, and final elements perform in accordance with the safety requirement specification, including all redundant channels;
5. Safety instrumented system documentation reflects the installed system;
6. The safety instrumented function performs as specified on bad (e.g., out of range) process variables;

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 23 of 74
		Rev: 01
		October 2011

7. The proper shutdown sequence is activated;
8. The safety instrumented system provides the proper annunciation and proper operation display;
9. Computations that are included in the safety instrumented system are correct;
10. The safety instrumented system reset functions perform as defined in the safety requirement specification;
11. Bypass functions operate correctly;
12. Manual shutdown systems operate correctly;
13. The proof test intervals are documented in the maintenance procedures;
14. Diagnostic alarm functions perform as required;
15. The safety instrumented system performs as required on loss of power or a failure of a power supply and confirm that when power is restored, the safety instrumented system returns to the desired state.

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

<p>KLM Technology Group</p> <p>Practical Engineering Guidelines for Processing Plant Solutions</p> <p>www.klmtechgroup.com</p>	<p>Kolmetz Handbook of Process Equipment Design</p> <p>SAFETY IN OVERPRESSURE RELIEVING SYSTEMS</p> <p>(ENGINEERING DESIGN GUIDELINES)</p>	Page 24 of 74
		Rev: 01
		October 2011

DEFINITIONS

Availability - The probability that equipment will perform its task

Back Pressure - The pressure on the discharge side of a pressure relief valve. Total back pressure is the sum of superimposed and built-up back pressures.

Balanced Pressure Relief Valve- Is a spring loaded pressure relief valve that incorporates a bellows or other means for minimizing the effect of back pressure on the operational characteristics of the valve.

Closed Discharge System - The discharge piping for a pressure relief valve which releases to a collection system, such as a blowdown drum and flare header. However, a closed system can also be a process vessel or other equipment at a pressure lower than the set pressure of the pressure relief valve.

Common Cause Failure Mode - A coincident failure in two or more similar elements of a system caused by a single event. An example of a common cause failure mode is the simultaneous failure of two independent level instruments due to freezing of the process fluid in the instrument leads when exposed to low ambient temperatures

Conventional Pressure Relief Valve- Is a spring loaded pressure relief valve which directly affected by changes in back pressure.

Design Contingency - An abnormal condition including maloperation, equipment malfunction, or other event which is not planned, but is foreseen to the extent that the situations involved are considered in establishing equipment design conditions.

Disc – Movable element in the pressure relief valve which effects closure.

High Integrity Protective System (HIPS) - An arrangement of instruments and other equipment, including sensors, logic controllers and final control elements used to isolate or remove a source of pressure from a system or to trip a shutdown or depressuring device such that the design pressure and/or temperature of the protected system will not be exceeded.

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

<p>KLM Technology Group</p> <p>Practical Engineering Guidelines for Processing Plant Solutions</p> <p>www.klmtechgroup.com</p>	<p>Kolmetz Handbook of Process Equipment Design</p> <p>SAFETY IN OVERPRESSURE RELIEVING SYSTEMS</p> <p>(ENGINEERING DESIGN GUIDELINES)</p>	Page 25 of 74
		Rev: 01
		October 2011

Maximum Allowable Working Pressure (MAWP) - the maximum (gauge) pressure permissible at the top of a vessel in its normal operating position at the designated coincident temperature and liquid level specified for that pressure.

Open Disposal System - Discharge piping of a PR valve, which releases to the atmosphere either directly or via a collection system

Operating pressure - The gauge pressure to which the equipment is normally subjected in service.

Overpressure - The pressure increase over the set pressure of the relieving device during discharge. It is also used as a generic term to describe an emergency which may cause the pressure to exceed the maximum allowable working pressure.

PHA (Process Hazards Analysis) - An analysis of the process that may range from a simplified screening to a rigorous Hazard and Operability (HAZOP) engineering study. PHA will determine the need for a SIS.

Pilot Operated Pressure Relief Valve- Is a pressure relief valve in which the major relieving device or main valve is combined with and controlled by a self actuated auxiliary pressure relief valve (called pilot). This type of valve does not utilize an external source of energy and is balanced if the auxiliary pressure relief valve is vented to the atmosphere.

PFD_{avg} - The average PFD used in calculating safety system reliability

PFD Probability of Failure on Demand - The probability of a system failing to respond to a demand for a fraction arising from a potentially hazardous condition

Pressure Relief Device - A device actuated by inlet static pressure and designed to open during an emergency or abnormal condition to prevent the rise of internal fluid pressure in excess of a specified value. The device may also be designed to prevent excessive vacuum. The device may be a pressure relief valve, a non-reclosing pressure relief device or a vacuum relief valve.

These design guidelines are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 26 of 74
		Rev: 01
		October 2011

Pressure Relief Valve – This is a generic term applying to relief valves, safety valves or safety relief valves. Is designed to relief the excess pressure and to recluse and prevent the further flow of fluid after normal conditions have been restored.

Relief Valve - Is a spring loaded pressure relief valve actuated by the static pressure upstream of the valve. Opening of the valve is proportion to the pressure increase over the opening pressure. Relief valve is used for incompressible fluids / liquid services.

Relieving Pressure- The pressure obtains by adding the set pressure plus overpressure/accumulation.

Remote Contingency - An abnormal condition which could result in exceeding design pressure at the coincident temperature, but whose probability of occurrence is so low it is not considered as a design contingency.

Safety Requirements Specification - specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems.

Safety Valve- Pressure relief valve with spring loaded and actuated by the static pressure upstream of the valve and characterized by rapid opening or pop action. A safety valve is normally used for compressible fluids /gas services.

Safety Relief Valve- Is a spring loaded pressure relief valve. Can be used either as a safety or relief valve depending of application.

Set Pressure- Is the inlet pressure at which the pressure relief valve is adjusted to open under service conditions.

SIF (Safety Instrumented Function) - One loop within the SIS which is designed to achieve or maintain a safe state. A SIF's sensors, logic solver, and final control elements act in concert to detect a hazard and bring the process to a safe state.

SIL (Safety Integrity Level) - A way to indicate the tolerable failure rate of a particular safety function

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.

KLM Technology Group Practical Engineering Guidelines for Processing Plant Solutions www.klmtechgroup.com	Kolmetz Handbook of Process Equipment Design SAFETY IN OVERPRESSURE RELIEVING SYSTEMS (ENGINEERING DESIGN GUIDELINES)	Page 27 of 74
		Rev: 01
		October 2011

SIS (Safety Instrumented System) - Its purpose is to take process to a “safe state” when pre-determined set points have been exceeded or when safe operating conditions have been transgressed

SIS lifecycle - Both standards chose to rely on the establishment of a design process, throughout which the performance of the instrumented systems must be maintained.

These design guideline are believed to be as accurate as possible, but are very general and not for specific design cases. They were designed for engineers to do preliminary designs and process specification sheets. The final design must always be guaranteed for the service selected by the manufacturing vendor, but these guidelines will greatly reduce the amount of up front engineering hours that are required to develop the final design. The guidelines are a training tool for young engineers or a resource for engineers with experience.

This document is entrusted to the recipient personally, but the copyright remains with us. It must not be copied, reproduced or in any way communicated or made accessible to third parties without our written consent.