CHEMICAL ENGINEERING TRANSACTIONS
VOL. 48, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Eddy de Rademaeker, Peter Schmelzer

ISBN 978-88-95608-39-6; **ISSN** 2283-9216
DOI: 10.3303/CET1648095

The Use of Pressure Relief Systems as Single-Channel, Highly Reliable Safety Devices

Udo Dünger*[a], Ernst Molter[b], Volker Stellmacher[a], Thomas Gabriel[b]

[a]Covestro Deutschland AG, 51365 Leverkusen
[b]Bayer Technology Services GmbH, 51368 Leverkusen
udo.duenger@covestro.com

An evaluation of the impact of random and systematic errors on a pressure relief system was carried out according to DIN EN 61508-2. It is shown how systematic errors can be prevented by means of a management system that covers the entire life cycle of a pressure relief system. Avoiding systematic errors by using this method leads to pressure relief systems which can be classified as highly reliable.

1. Introduction

The assessment of the safety of a plant, especially chemical plant, is nowadays generally carried out on a risk basis. The level of risk is described by the assumed frequency of occurrence of the initiating event and the assumed extent of damage. The risk is typically determined by using a risk matrix, see Figure 1.

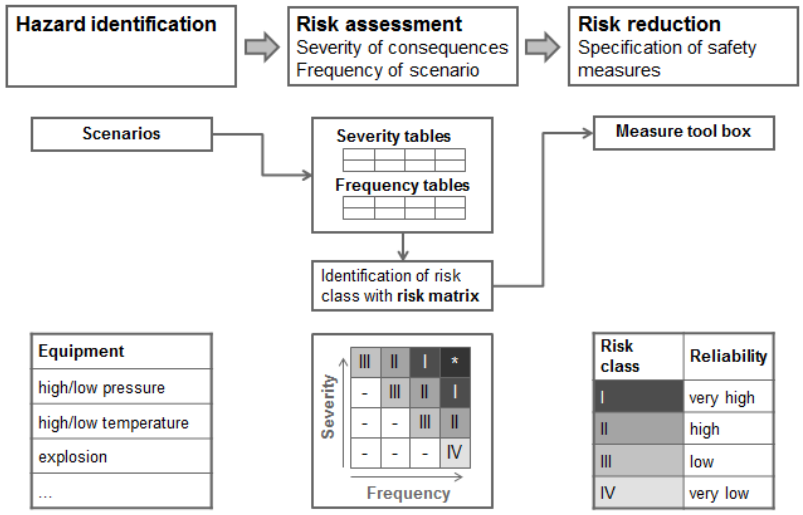

Figure 1: Assessment of risk and workflow of prevention concept.

The risk matrix is usually designed so that at the highest frequency of occurrence and the greatest damage the highest risk is reported. This usually describes a condition with a danger to life or physical condition of individual persons or a significant environmental hazard. However, the duty of care of the operator of a plant requires a risk reduction to a generally accepted level. In general, the reliability of technical devices for risk reduction is aligned to the level of risk. Reaching the required given specific risk reduction by means of process and control technology is described in great detail in the DIN EN 61508 as a generic framework standard and special in the DIN EN 61511 for safety devices in the process industry. This field of safety technology is now commonly referred to as "functional safety". The emphasis is, inter alia, on the prevention and control of systematic and random errors which have an impact on the safety function. For purely

Please cite this article as: Duenger U., 2016, The use of pressure relief systems as single-channel, highly reliable safety devices, Chemical Engineering Transactions, 48, 565-570 DOI:10.3303/CET1648095

mechanical safety devices such as rupture discs or relief valves, there is currently no such normatively defined requirement for proof of reliability.
Industrial Safety Regulation and the Pressure Equipment Directive contain requirements on the safeguard of pressure equipment. The requirements of these regulations with respect to pressure relief are generally satisfied when a pressure device is protected with at least one self-acting pressure relief device, such as a rupture disc or a safety valve. This installation thus represents a single-channel safety device. According to IEC 61511 risk reduction measures using process and control must be installed redundant, i.e. with two channels, for risks exceeding a certain level.
Since in accordance with DIN EN 61508 and DIN EN 61511 multi-channel redundant protective devices are required for very high assessed risk, the question was quickly asked whether this procedure is to be transferred to pressure-relief devices. It also applies to devices such as rupture discs or relief valves that they are influenced by systematic or random errors and they are used to protect risks of varying heights.
The aim of this work is to show that random errors in a safety valve mainly cause a failure on the safe side and the safety function will be preserved. Systematic errors that occur in all components of a pressure relief system and affect the safety function can be prevented by the consistent application of a procedure that is described in this work.
These statements can be used in the context of functional safety to evaluate the safety integrity of safety valves in semi-quantitative form. The applicable technical standard of the Framework Standard DIN EN 61508-2 is used here because there is currently no suitable sector standard for mechanical safety devices. This standard describes the basic concepts underlying the functional safety in a generic way and is therefore applicable in principle also for novel applications.
When assessing the safety function of a safety valve it is important that a safety valve or a rupture disk in general is not mounted directly on the tank but is usually connected by a pipeline, the so-called inlet line. Also on the downstream side, to fulfill the requirements of the rules for a safe disposal of blown materials, usually a pipeline, the so-called discharge line, is connected. Both the inlet and discharge line may adversely affect the safe function of the actual pressure relief device. The question of the reliability of a pressure relief device must therefore necessarily relate to the entire chain of components. In the simplest case, the pressure relief system consists of the inlet line, the pressure relief device itself and the blow-off line.

2. Fault analysis of a pressure relief system

In order to clarify whether a pressure relief system can be classified as highly reliable, first needs to be asked in what way systematic or random errors may affect the reliability of a pressure relief system.

2.1 Systematic errors

Such errors are classified as systematic errors that occur due to human error both in planning and during installation in the field. The systematic errors also include those errors that may arise from plant operation such as blocking of the inlet or discharge line, or sticking or corrosion of the valve seat.
It is known that a chain is only as strong as its weakest link. In a figurative sense, a pressure relief system can be seen as "chain", ranging from the design case to the safe disposal. This suggests that all chain links must be equally strong. In relation to our topic, they should have "the same reliability on demand". Table 1 lists possible systematic errors of the "chain links" and the consequences which can be derived therefrom in case of demand.

2.2 Random errors

Here errors are named random errors when they occur unexpectedly due to a structural inhomogeneity and in their effect can result in the loss of component function.
For the inlet and discharge line no random error can be identified in practical operation. Thus, the question for random errors of the above-defined pressure relief system is reduced to the pressure relief device itself.
For a safety valve are hereafter, starting from the function and component description, exemplified the possible random errors and their impact on demand. The safety function of a safety valve is to release a cross section at a predetermined pressure, so that in the end energy can flow from the pressure chamber of a device, and thus the pressure in the apparatus is kept at a safe level. This level is usually determined by the closing pressure of the safety valve. This safety function is achieved with very few components. Thus, a purely mechanically operating safety valve consists essentially of a housing made by casting on which the flanges of the inlet and outflow and the position for the valve seat are already integrated. Further components are the bonnet, the valve seat and the valve disk, the stem including adjusting nut and the valve spring.
Table 2 shows possible random errors on the components of a safety valve and the effects derived therefrom. Basically, every error leads individually or in combination to premature (at lower pressure) or spontaneous opening of the safety valve. That means that a safety valve is a component with fail safe behavior.

Table 1: Systematic errors of a pressure relief system

Chain link	Systematic error	Consequence
Design: - Filling level - Rate of heat production - Temperature - Substance property data	- Incomplete - Wrong	- False dimensioning - Pressure relief valve too small
Inlet line	- Diameter to small - too long - Blocked	- too high pressure loss - Insufficient or no functioning of the pressure relief valve
Pressure relief valve	- False dimensioning - False set pressure - False type - False material	- too high pressure loss - Insufficient or no functioning of the pressure relief valve
Discharge line	- Diameter too small - too long - Blocked	- too high pressure loss - Insufficient or no functioning of the pressure relief valve
Safe disposal	- Generates too high back pressure - Inappropriate for the substance - Outlet at false position	- too high pressure loss - Insufficient or no functioning of the pressure relief valve - (Release of products) - (Physical injuries)

Table 2: Random errors of a pressure relief valve

Part	Random error	Consequence
Housing	- Breaking due to undiscovered cavities in combination with superposed vibration	- Depressurizing by spontaneous relief
Bonnet	- Breaking due to undiscovered cavities in combination with superposed vibration	- Bonnet breaking leads to loss of preload, premature opening, possibly spontaneous relief
Valve seat, valve disk	- No random errors identified	- n/a
Valve stem (spindle)	- Fatigue fracture due to material errors and superposed vibration	- Loss of preload, premature opening, possibly spontaneous relief
Spring	- Fatigue fracture due to material errors and superposed vibration	- Loss of preload, premature opening, possibly spontaneous relief

3. Avoiding systematic errors

In accordance with DIN EN 61508 systematic errors are preferred to avoid (rather than to identify and resolve them at the installed system). For this purpose also "Good Engineering Practices" are applied in addition to the concept of the safety management system (see Section 3.1).

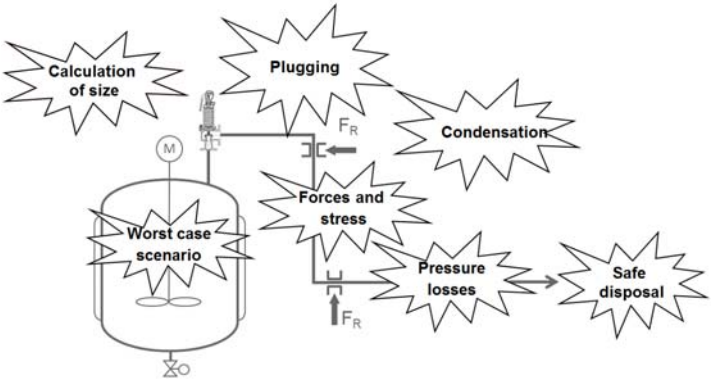

Figure 2: Challenges of pressure relief systems

Fig. 2 illustrates strikingly, the most important boundary conditions and issues for attention in the design of a complete pressure relief system. These points must be considered as a minimum requirement when designing a pressure relief system and are addressed by our procedure for the avoidance of systematic errors.
The key points are: Define the design case (worst case scenario), check whether two-phase flow occurs, check that pressure losses of the inlet and discharge line are adequate, consider solidification of product in the inlet and discharge line, safeguard the discharge of condensate (when applicable), check the reaction forces to the supports, ensure safe disposal of the relieved fluids, document the results.

3.1 Safety Management System

Based on the idea of the safety lifecycle of a safety device generally three management areas can be identified in order to avoid systematic errors in the above mentioned critical issues, see Figure 3. These areas ensure independently the safe functioning of the safety device and they are: Planning and execution, initial testing prior to commissioning and recurrent testing and inspection of the safety device during its lifetime. In the following basic contents are described for the three mentioned areas. These may need to be adapted to the task to be solved in the specific case.
Table 2 shows possible random errors on the components of a safety valve and the effects derived therefrom. Basically, every error leads individually or in combination with another to premature (at lower pressure) or spontaneous opening of the safety valve. The occurrence of one or more random errors in a safety valve so leads to a failure on the safe side (unwanted pressure reduction), i.e. a safety valve is a component with fail safe behavior.

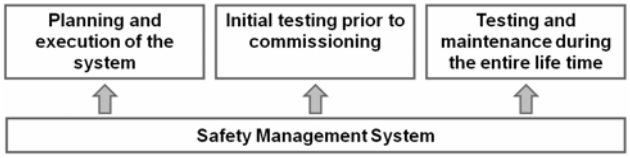

Figure 3: Safety Management System

Planning and execution
Starting point of every planning for a depressurization system is to determine the design case for the pressure relief device. For a reliable design finding out the design case in an interdisciplinary team is almost mandatory. In addition to the specialists responsible for the design, the operators, the technical support departments and possibly the TÜV should be involved. This ensures that the design case is evaluated and confirmed in terms of a redundant control by the team members. The team should also be questioning whether changes in technical equipment, such as control valves or pumps, lead to a change in the request to the pressure relief device. If this is the case, these devices are classified as safety-relevant and it is organizationally ensured that before a change of this technical equipment, the safe functioning of the pressure relief device is reviewed in view of the planned change.
An essential part of the overall design of the pressure relief system is the calculation of the discharge cross-section. For a pure gas or vapor flow the cross section calculation can be applied, for example, according to AD 2000 A1 (bursting discs) or according to AD2000-A2 (safety valves). By defining the discharge cross-section the discharged mass flow is determined, and thus all the information are given to calculate the downstream components such as separators, discharge line or a possibly required disposal system for the blown-out substances.
When calculating the discharge cross-section a possibly occurring two-phase flow consisting of the present liquid in the tank and its associated vapor or gas must be considered. The assessment of whether there is a two-phase flow due to the thermo-hydraulic processes during depressurization from the headspace of a container can be accomplished by means of the relevant literature, see Fischer 1992. If two-phase flow can occur during the depressurization, then a two-phase flow model must be used to calculate the discharge cross-section, for example, DIN ISO 4126 Part 10.
If a safety valve is used as a pressure-relief device, besides the design of the cross section also dynamic effects with the possibility of affecting the safe operation of the valve, have to be considered. Here in particular, the dynamic pressure losses in the inflow and discharge pipe of the safety valve have to be mentioned. For both pressure losses limits are specified in the literature, e.g. DIN AD2000-A2 or complete catalogue of LESER. Compliance with these pressure-loss limits must be checked.
At high set pressures and / or large and long discharge lines large forces can act on the fixed and loose bearings of the pipeline. This can lead to an overloading of standard pipe supports. As a result, the safe

functioning of the pressure relief device may be affected. For large pipes the sufficient dimensioning of fixed and loose bearings must be checked.
Inflow and discharge line can possibly blocked by substances that "freeze" at ambient conditions. In this way the safe function of the safety valve can be compromised. In such a case, usually the inlet and discharge line are trace-heated. For the purposes of the consideration of a pressure relief system as a chain in which all the members contribute to the same extent for safe function, the trace heating is included in the overall concept and must have adequate reliability.
The safe function of the pressure relief device, whose task is to prevent the bursting of a pressurized apparatus on demand, can also be affected by a disposal system downstream the discharge line which can influence the pressure. In the context of pressure loss calculation of the outlet line, therefore, the dynamic and static pressure losses of the individual components of the pressure relief system are taken into account from the outlet flange of the safety valve to the final outflow to atmosphere.
An according the above points planned pressure relief system, being tested according to the principle of redundancy, can be classified as a highly reliable safety device.
Initial testing prior to commissioning
Safety valves and bursting discs as conventional pressure relief devices are subject of strict production conditions or they are tested by the manufacturer prior to putting on the market. An independent testing by the end user does not take place normally.
During the approval for commissioning of the entire pressure relief system at Bayer and Covestro an internal procedure ensures that the engineered installation is checked on site. Here, in addition to the control of the correct installation position, the correct diameter and right set pressure of the pressure relief device and the piping of the inlet and blow-off line is checked. If deviations are found in the installed lengths, possibly carried out a re-calculation of the pressure loss or the deviations must be corrected.
Recurrent testing and inspection
Safety valves have to be regularly checked according to the applicable rules and regulations. Usually therefore the valves are detached on site and checked in a specialist workshop. The maximum intervals for the examination are specified in the regulations. Depending on the operational requirement of the safety valve, it can be necessary to shorten the inspection intervals, for example, for polymerizing products. The top priority here is to recognize deviations leading to adverse effects on the safe operation early enough.
During the valve test also a check of the inlet and outlet line with regard to free flow (no blocking) is done.

4. Assessment of random errors

For random errors DIN EN 61508 provides a quantitative criterion to evaluate the influence of this in principle unavoidable error type on the safety device. Here following requirements must be complied with:
• The minimum required level of redundancy of the device, and
• the maximum permissible probability of failure on demand (Probability of Failure on Demand, PFD, a probabilistic criterion).
Both criteria depend on the desired quality of the device. DIN EN 61508 uses four "grades" so-called "Safety Integrity Levels" (SIL): SIL1, SIL2, SIL3 and SIL4. From SIL1 to SIL4 the safety-related availability increases, so that for example SIL3 is capable to compensate for relatively higher risks and SIL1 is not. For both criteria quantitative statements on the frequency of random errors are required, as well as their classification into "safe" and "dangerous" fault (see Section 2.2). Specifically, the determination of the so-called "Safe Failure Fraction" (SFF) is required, which is the proportion of secure random errors based on the total amount of random errors.
In this context, studies were carried out on safety valves operating in the moderate pressure range which here means pressures below 100 bar, and mainly safeguard specific unit operations such as cleaning by boiling or securing of pipeline-bound energy, such as steam or nitrogen. The assessment of the probability of failure on demand is done for both newly delivered safety valves as well as valves, which were subject to a periodic inspection, by measurement of the pressure setting. A deviation of more than 10% of the nominal value was defined as failure on demand.
In the period from 2011 to 2013 regardless of the prior testing at the safety valve manufacturer valves have been randomly taken at the BAYER Subgroups out of the supplied safety valve batches and tested in the presence of a TÜV employee in a specialist workshop. The results showed that the measured set pressure does not exceed the set tolerance limits of the nominal set pressure of ± 3%.
In the period 2011-2013 1,000 safety valves from different manufacturers and different sizes were immediately checked after delivery from the operation, without cleaning. Valves contaminated with toxic or corrosive substances were excluded. From the total amount of the safety valves only one valve could be identified in which the measured set pressure was 20% above the set value. For all remaining valves, the maximum

upward deviation was below 10%. The plurality of valves showed a downward deviation, but with none of the valves opened below 10% of the nominal operating pressure.
Comparing the results of measurements with Table 2 of the EN 61508-2 and using the analytical examination of mechanical failure of a safety valve, a DIN safe failure fraction of SFF above 99 per cent can be noted for the examined safety valves.

Table 2: Maximum safety integrity level for a safety function according to DIN EN 61508-2

Safe failure fraction	Hardware fault tolerance		
of an element	0	1	2
< 60 %	Not allowed	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

In the normally single-channel (non-redundant) installation and thus a hardware fault tolerance of 0 the maximum achievable quality level is SIL3.
The activation of a safety valve is an extremely a rare event in practice, because operational measures are upstream in the holistic security concept. The reliable determination of the above-mentioned PFD value for a safety valve, based on real values for actual failures on demand is not possible. This is due to the small number of failures on demand and that in individual cases, the question of whether the safety valve has failed because of undetected dangerous faults in its components or for example has failed due to contamination, is not to clarify.
No failure rates can be analytically determined as the components of a safety valve in principle are subject only to static loads. Fracture mechanics methods for the determination of a component failure can therefore not be applied.
If we define failure on demand as a "non-opening" then our results show that none of the measured safety valves had failed on demand. This is consistent with the analysis of internal incidents at Bayer, where it has come despite the use of a safety valve to exceed the permissible tank pressure. The conducted incident analyses revealed that the cause of the excessive pressure was not a failure of the safety valve.
We therefore consider the use of safety valves in the mentioned field of application as a highly reliable safety device for consistent.

5. Summary

Starting from the discussion of the random and systematic errors that can occur on a pressure relief system, an evaluation of the impact of these errors on the pressure relief device was carried out according to DIN EN 61508-2. Random error could not be identified for the inlet and discharge line. Random errors at the actual pressure relief device (rupture disc or safety valve) lead to a failure of these devices to the secure side exclusively (Fail Safe behavior). Own measurements on approximately 1,000 safety valves revealed that a failure on demand (PFD) would not have occurred. It could be shown that, by introducing a management system that covers the entire life cycle of a pressure relief system, systematic errors can be prevented in the planning and construction of the entire system, at the inspection prior to commissioning and during the periodic inspection by applying the so-called four-eye principle. In strict compliance with this method, a pressure relief system can thus be classified as highly reliable.

Reference

DIN EN 61511 Functional safety - Safety instrumented systems for the process industry
DIN EN 61508-2 Functional safety of electrical / electronic / programmable electronic systems - Part 2: Requirements for safety-related electrical / electronic / programmable electronic systems (IEC 61508-2:2010)
VDMA Guideline Functional Safety Safety Integrity Level – SIL
EU Industrial Safety Regulation (BetriebsSichV), BGBL, 01.06.2015
EU Pressure Equipment Directive (Druckgeräte Richtlinie), BGBL, 2014
DIN AD2000-A1 (burst disks), Beuth, 10-2006
DIN AD2000-A2 (pressure relief valves), Beuth, 04-2015
H.G. Fisher et al. Emergency Design Systems Using DIERS Technology, AIChE, 1992
ISO DIN 4126-Part 10, Genf, 2010
Co. LESER, Complete catalogue, 2004