CHEMICAL ENGINEERING TRANSACTIONS

VOL. 90, 2022

A publication of AIDIC
The Italian Association
of Chemical Engineering
Online at www.cetjournal.it

Guest Editors: Aleš Bernatík, Bruno Fabiano
Copyright © 2022, AIDIC Servizi S.r.l.
ISBN 978-88-95608-88-4; **ISSN** 2283-9216

DOI: 10.3303/CET2290050

Random Failures of Mechanical Components in Safety Instrumented Systems

Gregor Schmitt-Paukszat[a,*], Dirk Hablawetz[b]

[a] Bayer AG, Kaiser-Wilhelm-Allee, 51368 Leverkusen, Germany
[b] BASF SE, GET/EI - L440, Carl-Bosch-Strasse 38, 67056 Ludwigshafen am Rhein, Germany
gregor.schmitt-paukszat@bayer.com

For safety instrumented systems, only random failures shall be taken into account in the calculation of the probability of failure on demand (PFD). Finding sound random failure rates – especially for mechanical components - can be quite challenging due to a lacking statistical basis.

In the new VDI/VDE 2180-4 (2021) “Functional safety in the process industry” it is specifically discussed, how mechanical components shall be considered in PFD calculations. In principle, it is explained that for purely mechanical safety devices without an instrumented component, e.g. pressure relieve valves, burst disks, flame arresters, manually operated valves, random failure rates are negligible assuming a correct equipment selection, design, construction, installation, maintenance etc. This also applies to mechanical components within safety instrumented systems. In the case of components that show a failure behavior similar to safety valves, they are not taken into account in the PFD calculation.

Supporting the approach of VDI/VDE 2180-4, the NAMUR working group (WG) 4.5 Functional Safety has evaluated failure reports of valves of different companies. In addition, the first failure rates for valves have been derived from the failure database NAMUR.smart based on a period of about three reporting years. The data acquisition allows a differentiated estimation of failure rates for random failures delivering practical failure rates for valves.

1. The new VDI/VDE 2180-4 and its corresponding NAMUR WG Practice Paper

The VDI/VDE 2180 series forms the basis for engineering safety instrumented functions in the process industry. It is widely used for process control technology (PCT) functions as part of safety systems in Europe. Since VDI/VDE 2180 Part 1 to 3 (2019) usually reference electrical equipment, special attention is given in VDI/VDE 2180 Part 4 (2021) to purely mechanical safety components.

One aspect of engineering safety instrumented functions is proving the availability of the safety function by calculating the probability of failure on demand (PFD). For the PFD calculation failure rates of all components in the safety critical path of the safety function are needed. Failure rates for non-electrical devices are difficult to determine due to lacking operating data.

VDI/VDE 2180-4 states that for purely mechanical safety devices without a PCT component, e.g., pressure relieve valves, rupture discs, flame arresters, manually operated fittings, the failure rates relevant for the PFD calculation with the correct device selection, design, construction, installation, maintenance etc. are so low that they are negligible. This also applies to mechanical components within PCT safety devices. Components that show a failure behavior similar to that of pressure relieve valves can therefore be neglected in the PFD calculation.

A NAMUR WG Practice Paper for applying VDI/VDE 2180-4 has been published in 2021 to proof that statement and determine the boundary conditions for most widely neglecting the failure rates of mechanical components in the PFD calculation. That paper supplements VDI/VDE 2180-4 with failure rates for valves based on real life failure data from different NAMUR companies.

The content of this article is mainly based on the NAMUR WG Practice Paper (2021).

Paper Received: 15 January 2022; Revised: 2 March 2022; Accepted: 5 May 2022
Please cite this article as: Schmitt-Paukszat G., Hablawetz D., 2022, Random failures of mechanical components in safety instrumented systems, Chemical Engineering Transactions, 90, 295-300 DOI:10.3303/CET2290050

2. Failure types in safety instrumented systems

Failures in safety instrumented systems are categorized into safe and dangerous failures. Safe failures (S) trigger the safety function without safety necessity which usually leads to a safe state of the corresponding system. Dangerous failures (D) inhibit the correct operation of the safety function – thus the safety function cannot be executed. Depending on whether the failures are detected or not, they can be categorized furthermore into detected (D) and undetected (U) failures leading to four categories: safe detected (SD), safe undetected (SU), dangerous detected (DD) and dangerous undetected (DU). Given some boundary conditions according to VDI/VDE 2180-3 (2019) the PFD calculation can be narrowed to focus on DU failures since only those contribute to the loss of availability of the safety function.

There can be different reasons for failures accidentally triggering or prohibiting the safety function. These reasons are categorized into the failure types random and systematic. Systematic failures are e.g., incorrect design or engineering of the safety function, incorrect maintenance. They can be avoided by changing procedures, increasing quality, etc. Random failures are evenly distributed over time and usually occur due to the deterioration of properties of the hardware and cannot be avoided but only corrected by replacing the faulty component (see VDI/VDE 2180-1, 2019). While diagnostics lead to a shift of DU failures to DD failures, residual DU failures are only found during proof testing or if an incident occurs due to a DU- failure (e.g., fishes swim with their belly up).

Avoiding and controlling failures is key in Functional Safety Management. From a high-level point of view, systematic failures are avoided by quality measures during design, engineering and maintenance of the safety system (e.g., using prior use equipment). Random failures cannot be avoided but only controlled by the selection of diverse and / or redundant equipment, Hardware Fault Tolerance (HFT) and the PFD calculation.

Therefore, the relevant fraction of DU failures originates from random failures. Systematic failures shall not be included in the PFD calculation since systematic failure do not occur evenly distributed in time which is a prerequisite for the PFD calculation.

Engineering safety instrumented functions requires a sound knowledge of possible failures in the corresponding application including (DU-) failure rates for all components in the safety critical path of the safety function. Although failure rates are well assessed for sensors and logic systems by manufacturers, there is only a volatile basis for actuators and valves.

From a VDI/VDE 2180-4 (2019) point of view, safety critical parts of actuators and valves are purely mechanical safety devices and should therefore have a negligible failure rate.

3. Failure modes of actuators and valves

The data of NAMUR.smart - a failure database for safety instrumented systems – has been analyzed and first results for the years 2017, 2018 and 2019 have been published in the NAMUR WG Practice Paper for applying VDI/VDE 2180-4 (2021).

The fault patterns on actuators and valves described below have occurred in real life. All failure modes are indicated without any assessment on which failures could lead to a dangerous state of the system. Both random and systematic failures are listed.

Standardized failure patterns are used in the "NAMUR.smart" database. The failure modes for the defective components "actuator" and "final element" (valves) are evaluated - that is, without electrical components:

- internal leakage
- aging / wear out
- mechanical blockage
- influence of product
- external leakage
- internal device fault (not caused by product)
- design error
- other random fault
- corrosion
- influence of environment
- frozen signal / stuck-at
- installation fault
- line break / short-circuit
- design flaw
- other systematic error engineering
- operator error

- mechanical damage
- measurement inaccuracy too high, signal drift (environmental influence / operation)
- incorrect test instructions
- other systematic failure maintenance

Figure 1 gives a rough overview of NAMUR.smart’s distribution of failure causes for the years 2017-2019. Only a small fraction of these failures contributes to the relevant DU-failure rates. From the failures modes mentioned above, only “aging / wear out“, “internal device fault (not caused by product) “ and “other random fault” are considered as random failures. This is a conservative approach, since using the equipment after its useful lifetime (“aging / wear out“) generally is a systematic failure.

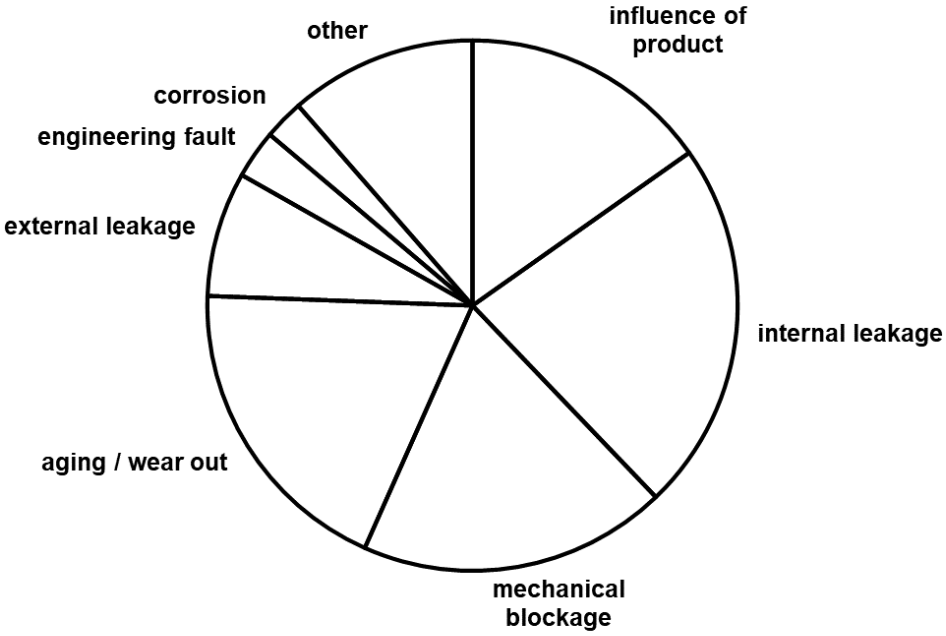

Figure 1: Failure modes for the defective components "actuator" and "final element" (valves) for the years 2017-2019

4. Failure rate estimation for actuators and valves

For a sound failure rate of actuators and valves, the corresponding components in the safety critical path need to be defined. A comparatively simple safety function for safeguarding against overfilling of a vessel serves as an example (see *Figure 2*). In case of a failure in the control loop L0001 and Y0001, level switch L0002 will close valve Y0002 and thus prevent too high level in the vessel and thus product entry into the exhaust pipe. The signal path of the safety function is shown in *Figure 3*.

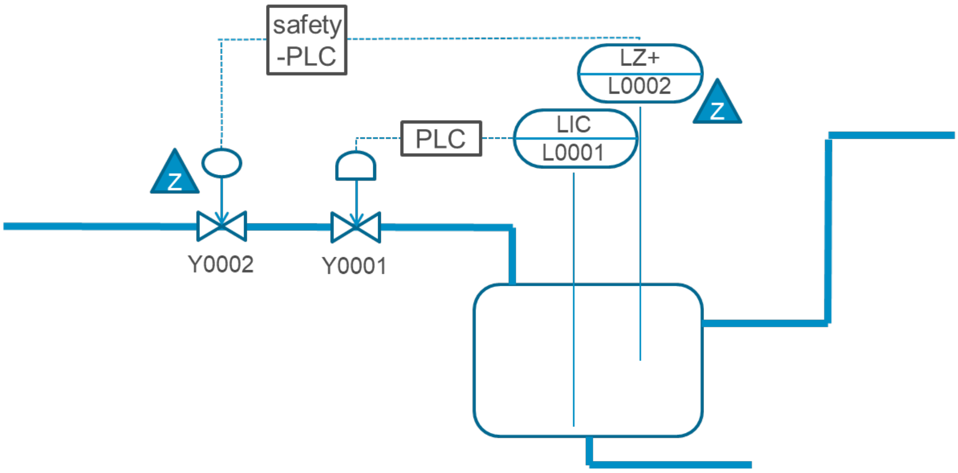

Figure 2: Typical safety function, safeguarding a vessel against overfilling (NAMUR WG Practice Paper, 2021)

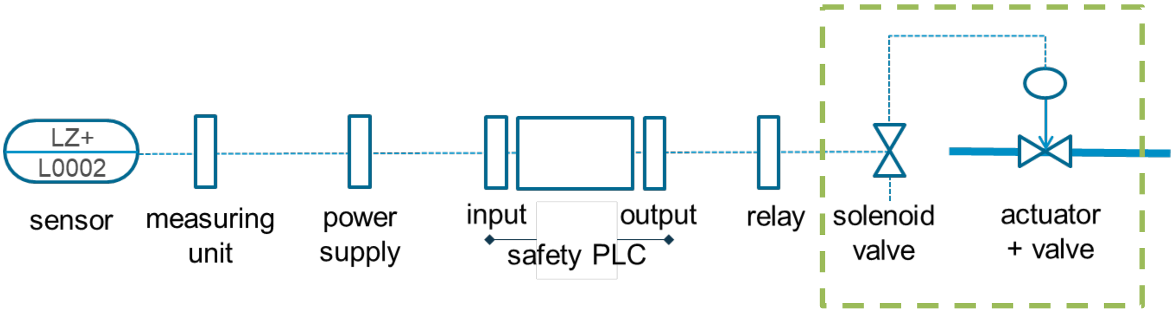

Figure 3: Signal path of the safety function and “extended valve” (NAMUR WG Practice Paper, 2021)

The estimation of failure rates based on user data (e.g., NAMUR.smart) typically includes electrical components when evaluating the final element subsystem, as shown by Hablawetz (2019). In *Figure 3* these are relays and the electrical part of the solenoid valve. The majority of the relevant random failures, however, is in the electrical components (see VDI/VDE 2180-4, 2021). This means that failure rates for mechanical components that are derived based on the failure rates of the whole final element subsystems in this database are too high.
For an objective comparison, it is necessary to define a generic "extended valve" (see *Figure 3*). This comprises all direct components of the valve including solenoid valve, switching contact, etc. According to NAMUR.smart, the components "attachment part", "actuator", "diagnostics", "final element" and "solenoid driver / isolator" are referred to as "extended valve". They all form the components of a valve. Failures in these components are conservatively added to the valve.

For calculating the failure rate λ the approach described in IEC 61511-2: 2019 (Section A.11.9.4, Note 2) is used.

$$\lambda = \frac{1}{2\,T_{op}} \chi^2_{\alpha,2n_x+2} \tag{1}$$

Here is $\chi^2_{\alpha,2n_x+2}$ the α-quantile of the chi-square distribution with degrees of freedom $n_x{}^* = 2n_x + 2$. α and T_{op} result from the previous specifications. n_x stands for the absolute failure numbers assigned to the individual failure types.
Since the database is inhomogeneous (different actuators from flap to control valve), the confidence limit is set to α= 90% - higher than specified in IEC 61511-1, 2017.

Table 1: Failure rates derived from NAMUR.smart (NAMUR WG Practice Paper, 2021)

Year	2017	2018	2019	total
Operating time	$425 \cdot 10^6$ h	$477 \cdot 10^6$ h	$569 \cdot 10^6$ h	$1.471 \cdot 10^6$ h
Number of all failures in the final element subsystem	374	446	572	1.392
Number of DU failures, extended valve	24	26	22	72
Number of DU failures of the actuator and valve, with-out systematic influences	2	6	6	14
λ_{total}	947 FIT	1.002 FIT	1.072 FIT	~1.000 FIT
$\lambda_{DU,\ ext.V}$	75 FIT	72 FIT	52 FIT	< 100 FIT
$\lambda_{DU,\ mech}$	13 FIT	22 FIT	19 FIT	< 25 FIT

In the literature, failure rates of typically 1,000 FIT can be found for actuators and valves. In these assessments, no distinction is made between the types of failures, but all failures are included in the assessment.

To check the plausibility, the failure rate for all failures (random + systematic) within the data record NAMUR.smart is calculated as λ_{total}. This also leads to a failure rate of approximately 1,000 FIT. This result is plausible.

By classifying the failure data according to failure types in NAMUR.smart, the data records can be limited to the DU failures relevant for the PFD calculation. This results in a failure rate $\lambda_{DU,\ ext.V}$ of less than 100 FIT for the extended valve ("attachment part", "actuator", "diagnostics", "final element" and "solenoid driver / isolator").

The failure rate $\lambda_{DU,\ ext.V}$ = 100 FIT matches results for failure rates from different users discussed in NAMUR WG Practice Paper for applying VDI/VDE 2180-4 (2021).

In NAMUR.smart, failure modes for aging and wear out are also assigned to the failure type “random”. Operating components beyond their useful lifetime is systematically incorrect and not a random failure.

In order to make an exclusive assessment of random failures, the failure rate $\lambda_{DU,\ mech}$ is assessed for the actuator plus valve without the failure mode “aging / wear out”. The failure rate of $\lambda_{DU,\ mech}$ = 25 FIT therefore refers exclusively to the mechanical body.

5. Impact of random failures for extended valve in PFD calculation

The small fraction of random failures for the extended valve raises the question whether the failure rate can be neglected in the PFD calculation.

A calculation of the probability of failure on demand according to VDI/VDE 2180-3 (2019), assuming a proof test coverage of 100%, annual proof test and single-channel structure (1oo1) and applying the assessed failure rate for the extended valve $\lambda_{DU,\ ext.V}$ = 100 FIT reveals a contribution of 5 % to the SIL2 band – so it is less than 5% of 10^{-2}.

Assuming a proof test coverage of 90%, an annual proof test, 10 years mission time and a single-channel structure (1oo1), the same failure rate contributes less than 9% of the SIL2 band.

Of course, the contribution to the PFD strongly depends on the complete safety instrumented system. Assuming the boundary conditions of the PFD are chosen to leave some space to the upper end of the SIL band in the calculation, the failure rates for the valve can be neglected.

6. Conclusion

The NAMUR WG Practice Paper for the application of VDI/VDE 2180-4 (2021) clearly proofs that for actuators and valves the fraction of random failures is little compared to the total number of failures. Most of the failures have a systematic reason.

Therefore, users need to focus on eliminating systematic failures rather than discussing the impact of actuators and valves on the PFD calculation. The latter is indeed negligible.

Systematic failures cannot be compensated by PFD calculation. Systematic failures can be avoided by using trained and qualified personnel, implementing prior use devices for safety instrumented systems, using the same type of devices in safety functions and control functions for a sound basis of experience and testing whether the devices are really suitable for the application or not, protecting the equipment against environmental influences and considering all process conditions during engineering (see VDI/VDE 2180-1, 2019).Focus on systematically correct engineering and design for safety functions!

Nomenclature

α – confidence limit
n_x – absolute failure numbers
$n_x{}^*$ - degrees of freedom
T_{op} – operating time, h
χ^2 – Chi-square distribution
$\widetilde{\lambda_x}$ – average failure rate
λ_{total} – failure rate for all failure modes, FIT
$\lambda_{DU, ext.V}$ – failure rate for extended valve, FIT
$\lambda_{DU, mech}$ – failure rate for mechanical part of actuator and valve, FIT

D – dangerous
S – safe
DU – dangerous undetected
DD – dangerous detected
PCT – Process Control Technology
PFD – Probability of Failure on Demand
HFT – Hardware Fault Tolerance
SIL – Safety integrity Level
WG – Working Group

Acknowledgments

Special thanks go to the sub team NAMUR.smart of the NAMUR working group 4.5 “Functional Safety” authoring the NAMUR WG Practice Paper for the application of VDI/VDE 2180-4 (2021) for assessing the field data: Dominic de Kerf (CARGILL), Matko Dijkman (BASF), Helge Essig (Bilfinger), Holger Haas (Covestro), Frank Höbel (Currenta), Marco Knödler (YNCORIS), Michael Lemke (CABB), Harry Siebert (BASF), Bernd Trompeta (INEOS), Hayriye Yazici (Bayer) plus the two authors of this article.

References

IEC 61511-1, 2017, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements, Ed. 2.1

IEC 61511-2, 2016, Functional safety – Safety instrumented systems for the process industry sector –Part 2: Guidelines for the application of IEC 61511-1: 2016

Hablawetz, D., 2019, What impacts the performance of safety instrumented systems? Experience based on field data of NAMUR.smart (in German), NAMUR general meeting 2019

NA106, 2018, Flexible proof testing of field devices in safety instrumented systems, NAMUR worksheet, edition 2018-09-06

NAMUR WG Practice Paper, 2021, Application of VDI/VDE 2180-4, Status 2021-07-22 (in German) <www.namur.net/fileadmin/media_www/Dokumente/AK-PRAXIS_4.5_VDI2180-4_DE.pdf> accessed 18.11.2021

VDI/VDE 2180-1, 2019, Functional safety in the process industry- Introduction, terms, conception

VDI/VDE 2180-3, 2019, Functional safety in the process industry - Verification of probability of failure on demand (PFD)

VDI/VDE 2180-4, 2021, Functional safety in the process industry - mechanical components in safety instrumented systems