TÜV AUSTRIA

Background

Procedure

Examples from Industry

Reinhard Preiss | Michael Struckl

Layer of Protection Analysis (LOPA) for Risk-Based Evaluation of Scenarios

Application guideline for the analysis of process-based scenarios for risk assessment of technical installations in the process industry

Edition **TÜV AUSTRIA**

TÜV AUSTRIA

Reinhard Preiss | Michael Struckl

Layer of Protection Analysis (LOPA) for Risk-Based Evaluation of Scenarios

Application guideline for the analysis of process-based scenarios for risk assessment of technical installations in the process industry

Edition **TÜV AUSTRIA**

Editorial information

Layer Of Protection Analysis (LOPA)
for Risk-Based Evaluation of Scenarios

Application guideline for the analysis of process-based scenarios
for risk assessment of technical installations in the process industry

1st Edition 2014

Cretated by the Austrian Working group "Semi-quantitative risk analysis"

Participants:

Dipl.-Ing. Hans-Jürgen Essl, Process Safety, Borealis Agrolinz Melamin, Linz
Dipl.-Ing. Dr. Friedrich Fröschl, VTU Engineering GmbH, Graz
Dipl.-Ing. Helmut Lengerer, Head Technical Safety, Sandoz GmbH
Dipl.-Ing. Michael Lutz, Process Safety, OMV refinery Schwechat
Dipl.-Ing. Dr. Marian Goriup, Process Safety, Borealis Polyolefine GmbH, Schwechat
Dipl.-Ing. Dr. Horst Hartl, Dpt. for Process Safety, TÜV AUSTRIA
Dipl.-Ing. Edith Moshammer, Magistrat Linz, Umwelt- und Technik-Center
Dipl.-Ing. Alfred Moser, Magistrat Linz, Umwelt- und Technik-Center
Dipl.-Ing. Dr. Reinhard Preiss, Head of Dpt. for Process Safety, TÜV AUSTRIA
Ing. Georg Sagerer, Department FLS, Lenzing AG
Dipl.-Ing. Ernst Simon, Leiter der Stabsstelle Großanlagenverfahren, Stmk. Landesregierung
Dipl.-Ing. Bernd Stöckl, Dep. Quality-Safety-Environment, LINDE GAS GmbH
Dipl.-Ing. Dr. Michael Struckl, BMWFJ, Abt. I/2 bzw. Ref. I/2a
Dipl.-Ing. Dr. Ulrike Weingerl, Process Safety, OMV AG
Dipl.-Ing. Ropert Wieser, Technical Safety, Sandoz GmbH

Editors: Dipl.-Ing. Dr. Reinhard Preiss, Dipl.-Ing. Dr. Michael Struckl

Published by

TÜV AUSTRIA Academy GmbH
1100 Vienna, Gutheil-Schoder-Gasse 7a
Tel.: +43 (1) 617 52 50–0
Fax: +43 (1) 617 52 50–8145
E-Mail: academy@tuv.at
www.tuv-academy.at

ISBN: 978-3-901942-49-5

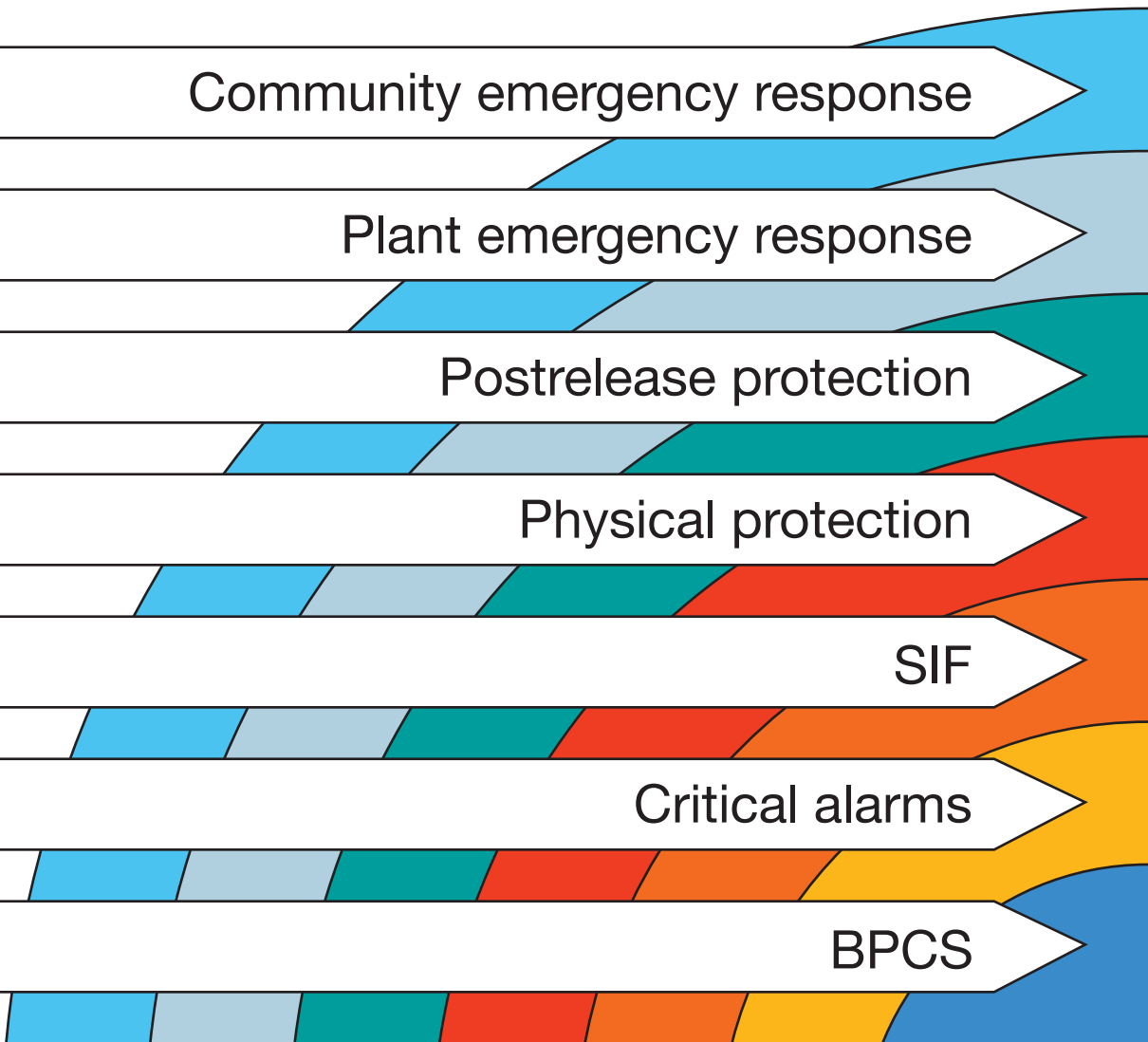
printed in Austria

Content

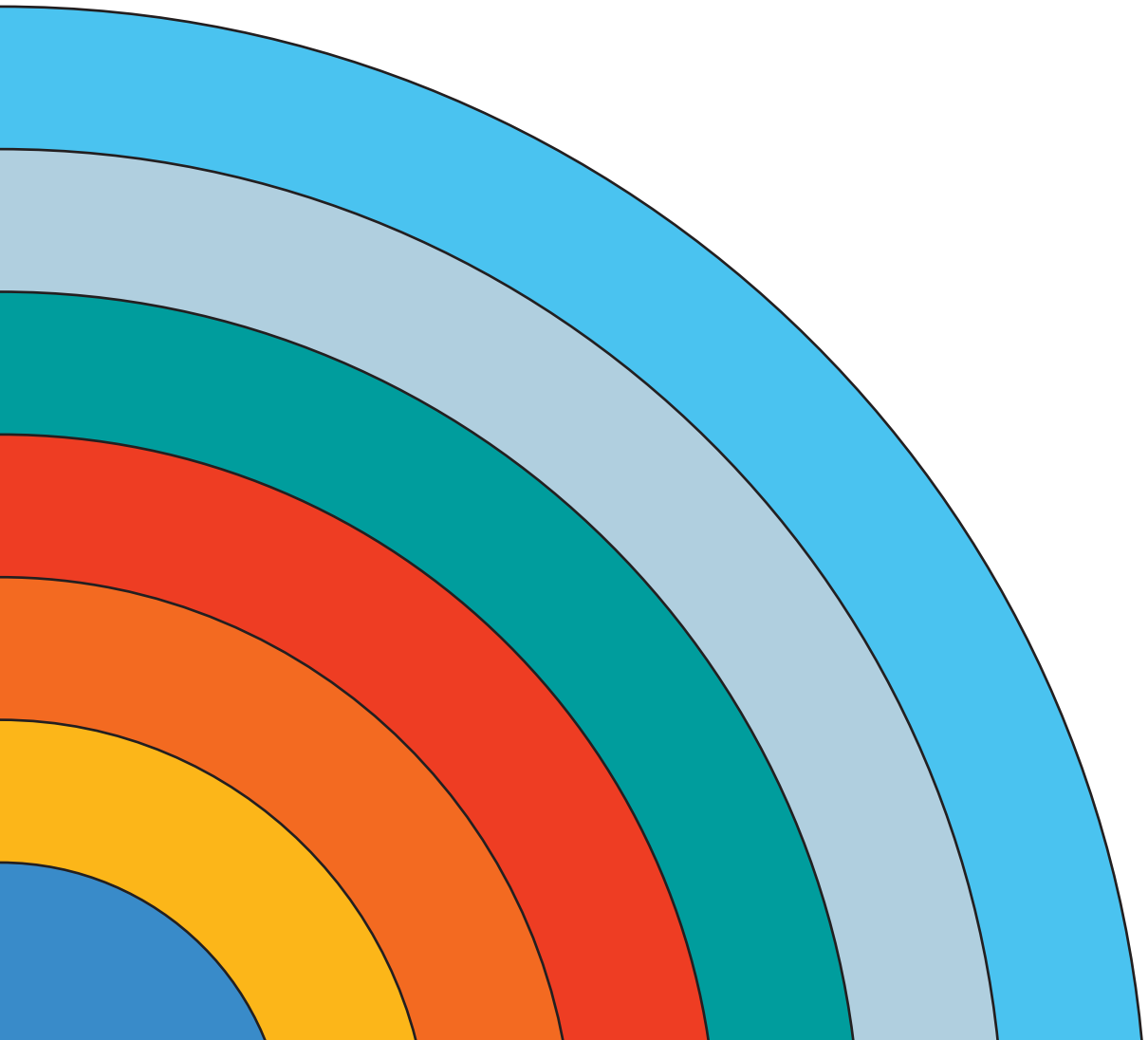
The Editors

Reinhard Preiss was heading the Process Safety Division in TÜV AUSTRIA for 7 years, now he is responsible for international business development within TÜV AUSTRIA group. He is giving lectures at several universities in Austria on technical risk management and process safety. He is author of the book “Methoden der Risikoanalyse in der Technik”.

Michael Struckl is heading the Industrial Technology Division at the Austrian Federal Ministry for Economics. Within this he is responsible for technical matters on legislation for machine safety, industrial accident prevention & industrial emission issues. From 2003 to 2005 Dr. Struckl was appointed as Austrian Expert to the EC JRC in Ispra, Italy, where he was involved in establishing guideline papers concerning major accident hazard issues.


Community emergency response
Plant emergency response
Postrelease protection
Physical protection
SIF
Critical alarms
BPCS

I. Preface



I. Preface

Since approximately 25 years technical risk analysis[1] methods are in use in Austria for industrial installations. The experiences made during this time, developments in relevant fields of application, changes of legal framework and new influences by international networking of companies justify a review of the methods in use so far. The so-called Layer-of-Protection Analysis (LOPA) is a quantitative approach for the evaluation of single accident scenarios in the process industry, which is applied increasingly in multinational companies. A particular element in this respect is the possible quantification of the risk for parts of the application and a documentation of the results of the analysis that is based on this quantification. For this purpose it was necessary to define levels of tolerability for certain risk values. The authors want to emphasize that this shall not constitute a precedent for respective assumptions outside of the field of application described here.

"Objective" safety of a technical system results from the presence of protective measures and the absence of hazard sources. By defining the protective measures and the State-of-the-Art a given level of safety is assigned, thus implicitly describing a "tolerable" or "acceptable" risk. A tolerable or acceptable risk[2] hereby results from a compromise of opinions of different stakeholder groups on the basis of experience, retrospective and prospective analysis of potential positive and negative effects, efficiency and expenses of safety measures. The outcome of this compromise may be a deterministic or probabilistic consideration.

The deterministic approach claims to specify future events and developments by preconditions and influencing factors. It assumes the presence of laws of nature and science which define each system totally. On the contrary the probabilistic approach assumes that a future state can only be predicted with a certain level of likelihood, thus trying to describe the real occurrence and making the resulting conclusions more objective.

Science and technology originally followed in their development a pure deterministic approach. This is understandable, because the available means required a stringent simplification of complex issues. Occurrences and events that appeared in reality as a variable state were re-defined in fixed values and stochastic parameters ignored, especially when it

1 *According to ISO 31.000 "risk analysis" is a process to understand the nature, sources and causes of identified risks and to estimate their level; for the purpose of this guideline the term also comprises the evaluation of the tolerability of the residual risk*

2 *There are many different forms of distinction between these two terms which are sometimes used as synonyms, especially in German technical language. The most acknowledged description of the two terms defines "acceptable" as the more likely risk level which may have a set borderline, whereas "tolerable" stands for a more unlikely area of risk where further reduction measures are still subject to consideration.*

concerned events with a very low likelihood[3]. The resulting uncertainty were (and are) considered by taking into account fixed additional values of safety.

In Austria and Germany a predominantly deterministic approach to safety evaluation exists which is characterized by a huge number of standards below the legal level. In this system there is a "presumption of safety" if all the relevant standards are in place and there is evidence for that: it is assumed that the documented State-of-the-Art of technology is sufficient to fulfil the criterion of avoidance of hazards. Only in case that the relevant standards, norms etc. were not followed there is a reverse burden of proof. In other words: by phrasing the norms, standards etc. a reconciliation of interests took place and created an "acceptable risk" which is not exceeded if these standards are followed.

This does not necessarily mean that there is no remaining residual risk beyond this level of safety defined by this State-of-the-Art. By means of a systematic risk analysis this remaining risk may be reduced, because this type of risk analysis usually is an integrated one whereas the classic safety technology is application-field-oriented. By performing this procedure, also cases for those no norms or solutions in existing rules are available are considered and evaluated with a view on risk reduction.

The methods in use until now for this purpose are systematic ones in the sense of following a pre-defined scheme but still they are primarily qualitative-deterministic. This means that their conclusion is based on expert judgement. By using a systematic scheme an expert (or a group of experts) combines the issue with personal opinion, experience and assumptions relevant for the case. The resulting conclusion therefore contains subjective judgements and uncertainty elements; conclusions are, as they contain vague terms ("high likelihood", "sufficient safety" etc.), vulnerable.

The specific relevance of quantitative and probabilistic methods lies in the potential to serve as an additional tool of evaluation for high hazard potentials and thus identifying leaks and deficits in the preceding deterministic evaluation and assessment of safety measures. Furthermore the outcomes are, because they are not phrased with vague judgment terms, clearly defined and therefore better defendable.

---

3 In English technical language the terms "likelihood" and "probability" (resp. "likely" and "probable") often are used in a different context, sometimes they are practically as synonyms. "Probability" stands for a value representing a result of a verifiable calculation (e.g. by the number of data), whereas "likelihood" expresses a more generic assumption. Taking into account the fact that there is no distinction in German between the two terms and that a exact knowledge of underlying data for quantitaive conclusion is rarely the case, this publication uses the expression "likelihood" only.

II. Scope and Range of Application

II. Scope and Range of Application

The range of application of the LOPA method described in this publication may be defined as follows:

LOPA is applied for the assessment of preventive safety measures in process installations by usage of a single accident scenario approach. Thus, LOPA is not applied for the integrated assessment of measures to find out or mitigate the individual or group risk figures which result from cumulative risks of several accident scenarios relevant for persons or groups of persons. LOPA therefore is not suitable for emergency planning or land-use planning. Furthermore the method is not appropriate for the assessment of classical occupational safety measures.

Although LOPA is aimed at a single-scenario evaluation, nevertheless a risk reduction for single scenarios will trigger a reduction of the overall individual risk, too – although it might not be quantified within LOPA as such –, if the acceptable risk value for the single scenario amounts only to some extent of the acceptable cumulative risk.

LOPA may be used for the classification of safety instrumented systems – alternatively to the risk graph method according to EN 61511–3[4], Annex D and E – but the basic range of application must be seen wider, which means in general for the evaluation of the appropriateness of protective measures with respect to safety of accident scenarios in process industry with a high loss potential.

The application of quantitative procedures of risk assessment requires the definition of reference values for acceptability or tolerability of residual risks. Therefore the authors discussed respective limit values for harm (expressed by dead or hurt persons, divided into on-site/workforce or off-site/public) or damage to the environment with a connection to a given industrial establishment; the resulting compromise was summarized by the working group from a technical viewpoint. The limit values for acceptance or tolerability indicated shall be used only in combination with the LOPA application as risk limit values for the assessment of single accident scenarios of process installations.

4 *EN 61511-3: Functional safety – Safety instrumented systems for the process industry sector, Part 3: Guidance for the determination of the required safety integrity level, issue 07/2005*

The LOPA analysis method was described for the first time in a CCPS publication[5] with an identical name and was then mentioned in standards EN 61511–3 annex F and 61508-5[6] annex F. The practical implementation of the method is not defined.

In the present guideline an application of LOPA is explained which is close to its practical implementation; for that purpose the individual necessary parameters are described in detail and – as far as meaningful – are standardized in order to achieve consistent results.

The practical application of the method is demonstrated in 8 practical examples and the result is – as far as feasible – compared with risk graph assessments for the same example.

5 *Layer of Protection Analysis; Center for Chemical Process Safety (CCPS), AIChE 2001*
6 *EN 61508-5: Functional safety of electrical/electronical/programmable electronic safety related systems, Part 5: Examples for methods for the determination of safety integrity levels; issue 05/2010*

III. Risk Acceptance and Tolerance Limit Values