TÜV AUSTRIA

AKADEMIE

Martin Doktor | Michael Struckl (Editoren)

Layer-of-Protection-Analyse (LOPA) zur risikobasierenden Bewertung von Szenarien

Guideline zur Anwendung für prozessbedingte Störungen bei der Sicherheitsanalyse von technischen Anlagen

TÜV AUSTRIA Fachverlag

Layer-of-Protection-Analyse (LOPA) zur risikobasierenden Bewertung von Szenarien

Guideline zur Anwendung für prozessbedingte Störungen bei der Sicherheitsanalyse von technischen Anlagen

3. Auflage 2022
ISBN 978-3-903255-49-4

Editoren der 1. und 2. Auflage: DI Dr. Reinhard Preiss, TÜV AUSTRIA,
und DI Dr. Michael Struckl, BMDW i. R.

Editoren der 3. Auflage: DI Dr. Martin Doktor, Leiter Competence Center Anlagensicherheit,
TÜV AUSTRIA, und DI Dr. Michael Struckl, BMDW i. R.

Medieninhaber:
TÜV AUSTRIA AKADEMIE GMBH
Leitung: Mag. (FH) Christian Bayer, DI (FH) Andreas Dvorak, MSc
2345 Brunn am Gebirge, TÜV AUSTRIA-Platz 1
+43 5 0454-8000
akademie@tuv.at | www.tuv-akademie.at

Produktionsleitung: Mag. Judith Martiska
Layout und Grafiken: Markus Rothbauer, office@druckwelten.at & lucdesign
Herstellung: druckwelten.at, 1180 Wien
Cover: © Onypix -– Fotolia

Inhalt

1. Einleitung

Die Unabhängigkeit von Schutzebenen untereinander und vom auslösenden Ereignis ist eine der Grundforderungen der Layer-of-Protection-Analyse (LOPA). Insbesondere in Fällen, wo der Auslöser eine Fehlfunktion des Prozessleitsystems ist, kommt es immer wieder zu Diskussionen, ob bzw. in welchen Fällen eine Maßnahme über das Prozessleitsystem auch als unabhängige Schutzebene gezählt werden kann. Gestützt auf eine aktualisierte Veröffentlichung von CCPS[1] erschien es deshalb auch notwendig, diesen Leitfaden in der dritten Auflage überarbeiten.

Seit etwa 30 Jahren findet in Österreich die technische Risikoanalyse[2] bei industriellen Betriebsanlagen Anwendung. Die dabei gemachten Erfahrungen, Entwicklungen in relevanten Fachbereichen, die sich verändernden gesetzlichen Vorgaben und die zunehmende internationale Vernetzung der Unternehmen lassen eine Überarbeitung der bisher im Bereich der technischen Risikoanalysen angewendeten Methoden gerechtfertigt scheinen.

Die so genannte Layer-of-Protection-Analyse (LOPA) stellt ein quantitatives Verfahren zur Bewertung von prozesstechnisch bedingten Einzelszenarien dar, welches vor allem in Unternehmen mit internationaler Ausrichtung in zunehmender Weise zum Einsatz kommt. Ein besonderes Element stellt dabei die in Teilbereichen mögliche Quantifizierung des Risikos und die darauf aufbauende Darstellung der Analyseresultate dar.

Zu diesem Zweck war es erforderlich, Festlegungen hinsichtlich der Zulässigkeit bestimmter Risikoniveaus zu treffen. Die Autoren legen Wert auf die Feststellung, dass damit kein Präjudiz für entsprechende Annahmen außerhalb des hier beschriebenen Anwendungsbereiches geschaffen werden soll.

„Objektive“ Sicherheit eines technischen Systems resultiert aus dem Vorhandensein von Schutzeinrichtungen und dem Fehlen von Gefahrenquellen. Durch die Festlegung von Schutzmaßnahmen und Regeln der Technik erfolgt eine nähere Bestimmung eines „Sicherheitsgrades“, aber dadurch auch indirekt eine Beschreibung eines „Grenzrisikos“.

Das Grenzrisiko ergibt sich dabei als Kompromiss der Ansicht verschiedener Interessensgruppen auf der Grundlage von Erfahrungen und rückblickenden oder vorausschauenden Untersuchungen hinsichtlich positiver und negativer Folgen, Aufwand und Wirksamkeit von Schutzmaßnahmen. Das Resultat dieses Kompromisses kann in einer deterministischen oder probabilistischen Betrachtung münden.

1 Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis (Center of Chemical Process Safety, 2015)

2 Unter dem Begriff „Risikoanalyse“ wird innerhalb dieses Leitfadens auch die Beurteilung der Tolerierbarkeit des verbleibenden Restrisikos miteingeschlossen.

Die Deterministik beansprucht, dass zukünftige Ereignisse oder Entwicklungen durch Vorbedingungen und Einflussfaktoren eindeutig festzulegen sind. Es wird das Vorhandensein von (Natur-)Gesetzen angenommen, die jedwedes System vollständig bestimmen.

Im Gegensatz dazu geht die Probabilistik davon aus, dass ein zukünftiger Zustand nur mit einer bestimmten (Eintritts-)Wahrscheinlichkeit vorausgesagt werden kann. Es wird dadurch versucht, das reale Geschehen genauer abzubilden und die daraus resultierenden Schlussfolgerungen zu objektivieren.

Naturwissenschaft und Technik folgten in ihrer Entwicklung ursprünglich einem rein deterministischen Prinzip. Das ist insofern verständlich, als die zur Verfügung stehenden Mittel bei komplexen Sachverhalten eine radikale Vereinfachung erforderlich machten. Die in der Realität als Variable auftretenden Zustände wurden zu fixen Größen umdefiniert und Zufallsparameter (insbesondere sehr seltene Ereignisse) vernachlässigt. Die dadurch bedingten Unsicherheiten wurden (und werden) durch fixe Sicherheitszuschläge berücksichtigt.

In Österreich und Deutschland existiert ein vorwiegend deterministisches System der Sicherheitsbeurteilung, das durch eine Vielzahl von untergesetzlichen Standards (Normen, Richtlinien usw.) gekennzeichnet ist. In diesem System gilt bei Nachweis der Einhaltung der anzuwendenden Normen quasi eine „Sicherheitsvermutung“: Es wird davon ausgegangen, dass der dokumentierte Stand der Technik ausreicht, dem Kriterium der Vermeidung von Gefährdungen zu entsprechen.

Nur bei Nichteinhaltung von Normen, Richtlinien usw. tritt eine Beweislastumkehr ein. Anders formuliert: Durch den im Rahmen der Formulierung der Normen, Vorschriften usw. erfolgten Interessensausgleich wurde ein „zu akzeptierendes Risiko“ bestimmt, das bei Einhaltung eben dieser Normen bzw. Vorschriften zwangsläufig nicht überschritten wird.

Das bedeutet aber nicht, dass es kein „Restrisiko“ jenseits des durch die Regeln der Technik definierten Sicherheitsniveaus gäbe. Durch eine systematische Risikoanalyse kann eine Reduzierung dieses Restrisikos erreicht werden, da dabei eine gesamthafte Betrachtung angestellt wird, während die „klassische Sicherheitstechnik“ sektoral ausgerichtet ist. Durch diese Vorgangsweise werden außerdem jene Fälle, für die keine normativen bzw. in Regelwerken angeführten Lösungen verfügbar sind, ebenfalls einer Betrachtung hinsichtlich notwendiger Risikoreduktion unterworfen.

Die dabei eingesetzten Methoden sind zwar „systematisch“ in dem Sinn, dass sie einem vorher festgelegten Schema folgen, sie sind allerdings primär immer noch qualitativ-deterministisch. Dies bedeutet, dass die Aussage nach wie vor auf ein Sachverständigenurteil (oder eine Summe solcher) aufgebaut ist. Unter Anwendung eines systematischen Untersuchungsrasters kombiniert dabei ein Sachverständiger (oder eine Sachverständigengruppe) den Sachverhalt mit seinen persönlichen Fachkenntnissen und Erfahrungen sowie fallbezogenen Annahmen. Das daraus resultierende Urteil enthält daher subjektive Werturteile und Unsicherheiten. Schlussfolgerungen sind, da auf groben unbestimmten Begriffen aufgebaut (*„… hohe Wahrscheinlichkeit …“, „… hinreichend sicher …“* usw.), angreifbar.

Die spezielle Bedeutung quantitativer bzw. probabilistischer Analysemethoden liegt darin, bei großen Gefahrenpotenzialen als vertiefende Erkenntnisquelle zu wirken und derart Defizite bei der vorangehenden deterministischen Betrachtung bzw. Maßnahmenbemessung zu identifizieren. Ferner sind die Ergebnisse, da nicht als unbestimmtes qualitatives Urteil formuliert, eindeutig umrissen und somit besser argumentierbar.